CEU
Escuela Internacional
de Doctorado

Universidad CEU San Pablo

CEINDO – CEU Escuela Internacional de Doctorado

PROGRAMA en Derecho y Economía

El interés legítimo en el tratamiento de datos personales masivos

TESIS DOCTORAL

Presentada por:

Elena Gil González

Dirigida por:

José Luís Piñar Mañas

Alberto Díaz-Romeral Gómez

MADRID

2020

Si continúas leyendo esta página aceptas el uso de tus datos personales a perpetuidad con finalidades que incluyen, pero no se limitan a la personalización del contenido de los siguientes agradecimientos y muestras de gratitud. Asimismo, manifiestas expresamente tu renuncia a la retirada de dicho consentimiento y el ejercicio de cualquier derecho o acción.

AGRADECIMIENTOS

En la esfera académica, es muy frecuente utilizar metáforas con las que uno pretende describir cómo ha sido su proceso de estudio y creación.

Para mí, este ha sido un largo camino. En realidad, una tesis doctoral se parece mucho al Camino de Santiago. Ésta es mi metáfora. Para aquellos que no lo han vivido, puede parecer un camino más. Tampoco será para tanto, podrán pensar. Aquellos que hayan llegado al final conocen bien que el paso a paso trae más traspiés que para los que íbamos preparados, pero también recompensas más profundas de las que se pueden explicar.

El Camino es largo y en ocasiones tortuoso, está lleno de subidas, bajadas, lugares, personas y experiencias. He podido atravesar todas ellas gracias a muchas personas, pero en especial, a mis acompañantes principales. En primer lugar, mis directores de tesis y más que ello, maestros, José Luís Piñar y Alberto Díaz-Romeral. Como dirían ellos, hemos llegado al Monte do Gozo. También guardo un agradecimiento especial a mi familia, a mi pareja David y amigos, que habéis vivido cada etapa conmigo.

Pero una tesis doctoral tiene factores únicos. Aquí el Camino lo crea cada uno. Surgen posibles desviaciones, hay que tomar decisiones, hay que superar muchas dudas. No se trata de ser inteligente, se trata de ser resiliente, tener gran capacidad de motivación y sentir pasión con lo que haces.

A atesorar esta pasión me han ayudado mis compañeros de Secuoya Group, a los que he convertido en mi familia jurídica. Gracias a Jorge García, Jeimy Poveda, Ángel Benito, Esther Botella, Jorge Morell, Darío López, Luís Gervás, Francisco Adán, Manuela Battaglini, Eleazar García y los anónimos. También al equipo de Écija, y en especial a Daniel López y Alonso Hurtado de quienes me llevo un gran aprendizaje.

En este Camino he tenido la suerte de cruzarme con el equipo de la Cátedra Google, cuyo entusiasmo tanto me ha inspirado, y con el equipo del Instituto

de Derecho de la Información de la Universidad de Ámsterdam (IViR), que hicieron que mi tiempo allí fuera tan enriquecedor como *gezellig* desde la primera *bitterballen* hasta el último debate. Igualmente, por supuesto, tantos otros compañeros con los que he tenido largas conversaciones en este tiempo. A riesgo de dejar muchos nombres en el tintero -en cuyo caso alegaré estar cumpliendo el principio de minimización de datos-, debo destacar a Paul de Hert, Borja Adsuara, Javier Sempere, Eduard Blasi, Antonio Estella, Íñigo de Miguel y Paco González-Calero.

A todos vosotros, gracias por compartir conmigo las vistas en el Camino y las paradas de avituallamiento.

TABLA DE CONTENIDO

CAPÍTULO I. INTRODUCCIÓN

1. Antecedentes

En el tiempo en el que una persona tarda en leer este párrafo, se habrán enviado 200 millones de emails y se habrán realizado 4.5 millones de búsquedas en Google.[1] De hecho, estas magnitudes quedan constantemente desactualizadas y son tan grandes que nuestro cerebro es incapaz de cuantificarlas, de modo que nos simplifica la información hasta el punto en el que la una persona media solo retendrá en la memoria que se trata de "muchos datos".

Ciertamente, cada una de nuestras interacciones en el entorno digital genera datos, en un proceso bautizado como dataficación.[2] Los datos han pasado de ser un subproducto[3] a ser definidos como el nuevo petróleo de nuestra generación.[4] Aunque esta metáfora quizás no sea del todo acertada, sirve para mostrar la esencia de la creciente importancia que el tratamiento de datos tiene en todos los aspectos de nuestra sociedad. Por su parte, diversos acontecimientos imprevisibles, conocidos como cisnes negros,[5] se encargan de acentuar y acelerar estas tendencias. Tal es el caso de la expansión de la pandemia consecuencia del COVID-19, que, más allá de implicaciones sanitarias, en solo unos meses nos ha llevado a replantear de manera profunda la eficiencia del teletrabajo, las compras por internet o la educación en línea.

[1] FORO ECONÓMICO MUNDIAL (2019): *Why Big Data Keeps Getting Bigger*.

[2] NEIL CUKIER, Kenneth; MAYER-SCHÖENBERGER, Viktor (2013): "The Rise of Big data. How It's Changing the Way We Think About the World", en *Foreign Affairs* Vol. 92, No. 3.

[3] SCHNEIER, Bruce (2015): *Data and Goliath: The Hidden Battles to Capture Your Data and Control Your World*, WW Norton & Company.

[4] The Economist, The world's most valuable resource is no longer oil, but data, de 6 de mayo de 2017.

[5] TALEB, Nassim Nicholas (2007): The black swan: *The impact of the highly improbable*, Vol. 2, Penguin Random house.

Las organizaciones hacen uso de las tecnologías de la información y la comunicación para recopilar, acceder, utilizar e intercambiar datos, muchos de los cuales se pueden definir como personales, con el objetivo de mejorar sus procesos de toma de decisiones. Estos procesos son fuente de grandes beneficios empresariales y sociales. Por ejemplo, Uber analiza datos en tiempo real para monitorizar la oferta y demanda de conductores en una zona específica, realizar predicciones en función del clima o eventos como conciertos, y así ajustar sus precios.[6] Por su parte, el análisis de datos masivos es utilizado en Bangladesh como parte de su estrategia de detección y control de brotes de malaria, una enfermedad que causa miles de muertes anualmente, en su mayoría de niños.[7]

La otra cara de la moneda es la innegable existencia de riesgos derivados de las tecnologías de la información. Estos van desde la posible baja calidad del conjunto de los datos, la capacidad de gestionar silos centralizados de grandes volúmenes de datos, el impacto de la creación de perfiles. Tampoco debemos olvidar las nuevas dinámicas competitivas entre mercados analógicos y digitales o las barreras de entrada a mercados basados en la digitalización. Por otro lado, la capacidad de almacenamiento de datos, en constante crecimiento, ha provocado una tendencia a acumular y almacenar datos por defecto, un síndrome de Diógenes digital. Con esta información, las organizaciones persiguen predecir nuestro comportamiento, y más aún, influir en él y diseñarlo, en lo que ha dado lugar al denominado capitalismo de la vigilancia, basado que se produce en muchas ocasiones de manera no autorizada, unilateral, “glotona” y secreta.[8]

[6] FORBES, *Uber Charges More If They Think You're Willing To Pay More*, de 30 de marzo de 2019.

[7] BBC NEWS, *Big data ‘can stop malaria outbreaks before they start´*, de 10 de junio de 2019.

[8] ZUBOFF, Shoshana (2018): *The Age of Surveillance Capitalism. The Fight for a Human Future at the New Frontier of Power*, Londres, Profile Books.

Pero sin duda, uno de los mayores retos que las tecnologías de la información han creado se relaciona directamente con la protección de nuestros datos personales y nuestra privacidad.

Ya en 1969, Arthur R. Miller describía los cambios de patrones en el desarrollo y protección del derecho a la privacidad en Estados Unidos. Enunciaba que en el pasado, esta ha sido relativamente fácil de proteger debido a diferentes razones: "1) no se han reunido grandes cantidades de información sobre las personas y, por lo tanto, no se encontraban disponibles; 2) la información disponible se ha mantenido por lo general de manera descentralizada; 3) la información disponible ha sido de carácter relativamente superficial y a menudo se ha permitido que se atrofie hasta el punto de ser inútil; 4) el acceso a la información disponible ha sido difícil de asegurar; 5) en una sociedad de gran movilidad es difícil seguir el rastro de las personas; y 6) la mayoría de las personas no son capaces de interpretar e inferir información esclarecedora a partir de los datos disponibles. Pero una lectura rápida de los testimonios obtenidos por diversos subcomités del Congreso y una breve reflexión sobre las capacidades intrusivas de los nuevos dispositivos de vigilancia y las tecnologías de la información llevan a la conclusión de que estas salvaguardias tradicionales sobre la privacidad ya no son fidedignas".[9]

Al otro lado del Atlántico, en la Unión Europea el derecho a la privacidad y a la protección de datos personales terminaron por consagrarse en la Carta de los Derechos Fundamentales de la UE y en su Tratado de Funcionamiento.[10] Sin embargo, el alcance del uso de datos trasciende el Derecho y es también una cuestión económica decisiva. La evolución tecnológica ha amplificado el debate sobre la necesidad de que el

[9] CONGRESO Y SENADO DE ESTADOS UNIDOS, COMITÉ DE ASUNTOS JURÍDICOS, SUBCOMITÉ DE DERECHOS CONSTITUCIONALES (1969): *Privacy, the Census and Federal Questionnaires: Hearings Before the Subcommittee on Constitutional Rights of the Committee on the Judiciary, United States Senate, Ninety-first Congress, First Session, on S. 1791, to Secure Personal Privacy and to Protect the Constitutional Right of Individuals to Ignore Unwarranted Requests for Personal Information, April 24, 25, May 2, and July 1*.

[10] GONZÁLEZ FUSTER, Gloria (2014): *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, Vol. 16, 1ª ed., Springer International Publishing.

ecosistema comunitario trabaje en pro de una armonización regulatoria. En este sentido, desde el punto de vista jurídico, lo relevante de la aplicación de tecnologías de recolección, almacenamiento, análisis y aplicación masiva de datos es el hecho de que estos procesos utilizan datos personales y sirven de base para tomar decisiones que despliegan consecuencias en la vida de las personas, así como en el desarrollo de la economía y la sociedad digitales.

En la actualidad, la protección de datos personales en la UE se rige normativamente por el Reglamento General de Protección de Datos (RGPD),[11] cuyo objeto de protección es bicefálico. En primer lugar, pretende dar protección a los datos personales, aunque reconoce que no se trata de un derecho absoluto, "sino que debe considerarse en relación con su función en la sociedad y mantener el equilibrio con otros derechos fundamentales, con arreglo al principio de proporcionalidad".[12] Es decir, la concepción comunitaria del derecho a la protección de datos parte de la base de que no debemos vernos obligados a escoger entre este o la protección de otros derechos, sino que ambos se conjugan para encontrar un equilibrio.[13] Por otro lado, el RGPD destaca la necesidad de no obstruir, o incluso facilitar la libre circulación de los datos personales dentro de la Unión Europea[14] e indica, expresamente que "el buen funcionamiento del mercado interior exige que la libre circulación de los datos personales en la Unión no sea restringida ni prohibida por motivos relacionados con la protección de las personas físicas en lo que respecta al tratamiento de datos personales".[15]

[11] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

[12] Considerando 4 RGPD.

[13] TRONCOSO REIGADA, Antonio (2010*): La protección de datos personales: en busca del equilibrio*, Valencia, Tirant lo Blanch.

[14] Ver, por ejemplo, los considerandos 5, 9, 10 ó 13 RGPD.

[15] Considerando 13 RGPD.

No se trata de un objeto de protección novedoso, sino que la norma que le precedió, la Directiva 95/46, ya pretendía asegurar la libre circulación de datos personales, garantizando al mismo tiempo un alto nivel de protección de los derechos e intereses de las personas a las que se refieren dichos datos[16] y así ha sido reconocido por la jurisprudencia de TJUE.[17]

Parece pues que el marco normativo de protección de datos no tiene, ni nunca ha tenido, como objetivo otorgar un derecho absoluto a los individuos a permitir o a oponerse a determinados tratamientos de datos personales. Asimismo, la tensión entre la normativa de protección de datos, por un lado, y los retos de las tecnologías de análisis masivo de datos, por otro, pueden parecer en conflicto. No obstante, la norma asume la necesidad del tratamiento de datos personales en la sociedad digital, así como sus beneficios, delimitando aquellos tratamientos abusivos o injustificados. La aplicación de la interpretación jurídica, combinada con soluciones técnicas, puede facilitar la reconciliación entre ambas dicotomías.

Pues bien, la normativa de protección de datos ha confiado en el consentimiento de los sujetos como el instrumento principal para ejercer control sobre nuestra información.[18] Sin embargo, en entornos big data el consentimiento muestra ciertas limitaciones, nuevas y diferentes de aquellas otras que podría mostrar en entornos analógicos o entornos tecnológicamente menos complejos. Sin embargo, el tiempo y el paso de un mundo eminentemente analógico a uno cada día más digital cuya base está asentada en el tratamiento de cantidades crecientes de datos, ha sacado a la luz diversas limitaciones que el consentimiento muestra en la aplicación del cuerpo normativo de protección de datos. Ante esta situación,

[16] Considerando 3 Directiva 95/46.

[17] TJUE, asunto Lindqvist, apartado 96. Este asunto, además, permitió también que el TJUE contrastara la relación entre el derecho a la protección de datos con otros derechos, en concreto, con la libertad de expresión. RALLO LOMBARTE, Artemi (2017): "El Tribunal de Justicia de la Unión Europea como juez garante de la privacidad en internet", en Teoría y realidad constitucional, No. 39.

[18] KOSTA, Eleni (2013): *Consent in European Data Protection Law*, Martinus Nijhoff Publishers.

un grupo de voces -quizás hasta ahora mayoritario- defiende la necesidad del consentimiento como eje central de la norma, y ha centrado sus esfuerzos en idear fórmulas que lo refuercen. De hecho, tanto el legislador comunitario como las autoridades encargadas de interpretar las normas de protección de datos personales han actuado con el objeto de solventar dichos problemas. Dichos cambios son, con toda lógica, bienvenidos. Sin embargo, ¿está justificado la gran atención que recibe el consentimiento como instrumento jurídico? ¿Sería posible trasladar el foco hacia otras herramientas que nos ayuden a encontrar soluciones a los nuevos retos? Es posible que no sea necesario aferrarse al consentimiento como el salvoconducto único o más efectivo para proporcionar garantías y seguridad a las personas a la luz de las realidades tecnológicas presentes y futuras. En concreto, la norma reconoce también que el interés legítimo puede sostener la licitud de tratamientos de datos personales bajo determinadas circunstancias. Se trata de una figura relativamente inexplorada en la doctrina y en la práctica de la aplicación de la protección de datos personales, cuanto más, en entornos de tecnologías de datos masivos.

2. Preguntas de la investigación

Con base en todo lo anterior, este trabajo pretende dar respuesta a las siguientes preguntas:

> ¿Es el consentimiento como base de licitud un instrumento ampliamente efectivo para la protección de datos de carácter personal en entornos de utilización de tecnologías big data? ¿En su caso, puede el interés legítimo resolver las principales limitaciones del consentimiento?

Para responder a las cuestiones anteriores es necesario establecer primero una definición de tecnologías big data o de datos masivos. En segundo lugar, es necesario conocer cómo estas interoperan con el modelo de bases de licitud, en concreto, el consentimiento y el interés legítimo.

Tradicionalmente, el consentimiento ha dado respuesta a los objetivos finales de la normativa de protección de datos personales. La persona adquiere un medio directo para manifestar su aceptación o negativa a determinado tratamiento, y el responsable obtiene confirmación para proceder al tratamiento. Por su parte, el interés legítimo se ha dispuesto como una figura de carácter abierto, en ocasiones falto de concreción y especificidad. Esta indeterminación jurídica, unida a la concepción de que serviría para crear vacíos normativos que terminasen por fundar una apariencia de licitud respecto de prácticas en realidad obscuras, terminó por dar como consecuencia la escasa utilización de esta figura en la práctica. Sin embargo, a la luz del avance tecnológico, la adopción de tecnologías de tratamiento de datos masivos y el nuevo marco normativo dado por el RGPD, estas concepciones deben ser reexaminadas.

La recogida y análisis de datos, así como la posterior utilización del nuevo conocimiento generado para la toma de decisiones o la mejora continua de procesos puede generar consecuencias sobre el individuo, positivas, negativas o neutras, en función del contexto. Sin embargo, en muchas ocasiones, estos procesos se llevan a cabo sin el conocimiento de los individuos y de maneras opacas. La posible falta de transparencia unida a la rapidez de la evolución de la innovación tecnológica se opone al ritmo más pausado del desarrollo legislativo. Esta situación justifica la realización de un análisis profundo sobre qué retos plantean estas tecnologías, así como modos eficientes de hacerles frente.

La elección de estudiar la figura del interés legítimo (art. 6.1.f) RGPD) como posible alternativa al consentimiento se justifica en varias premisas. En primer lugar, en este trabajo pretendemos analizar el estado actual técnico-jurídico para elaborar una propuesta con aplicación práctica que trascienda las elaboraciones puramente teóricas. En segundo lugar, el proceso de creación del RGPD ha sido largo y complejo. Como consecuencia de ello, cualquier hipótesis que se necesite de un cambio normativo profundo se incardina en aquellas que no son de facto efectivas en el corto plazo y cuya aplicación práctica queda relegada en la actualidad. Por este motivo, el

estudio y análisis y este sentido queda fuera del ámbito de este trabajo. Así, por ejemplo, la reforma del marco normativo de protección de datos o la concepción de nuevos derechos no reconocidos por el RGPD no son opciones factibles a medio plazo. En atención a ello, el estudio de cualquier alternativa al consentimiento como base de licitud debe ser un instrumento ya existente en el cuerpo normativo de protección de datos personales.

Este trabajo está dividido en diferentes capítulos que sirven al objeto de construir el análisis en torno a la existencia o no de una base de licitud en entornos big data.

Así, la primera parte del trabajo examina la evolución histórica de la ciencia de datos y la compara con la paralela evolución del derecho a la protección de datos personales. Además de aportar información sobre el contexto que sirve de base para los siguientes capítulos, analizaremos cómo el desarrollo legislativo discurre con posterioridad al desarrollo tecnológico. Este hecho pone de manifiesto que, en aras de conseguir efectividad práctica, la búsqueda de instrumentos jurídicos que puedan servir al ejercicio diario de los responsables del tratamiento no puede depender de la creación de desarrollos normativos dilatados en el tiempo. A continuación, se analizan las tecnologías de tratamiento de datos masivos y se centra el marco tecnológico del trabajo, algo necesario debido a la falta de consenso sobre qué debe entenderse por big data.

A continuación, examinaremos la figura del consentimiento en tanto elemento de licitud de tratamientos de datos personales. El consentimiento es uno de los nodos centrales del sistema de garantías de las personas en lo que respecta al ejercicio de su capacidad de control de aquella información que se refiere a ellas. Las innovaciones tecnológicas de datos masivos crean un contexto que acentúa o crea debilidades en esta figura y que han sido objeto de análisis por parte de la doctrina en los últimos años. La respuesta mayoritaria a ello se ha centrado en investigar modos de reforzar el consentimiento, la forma de solicitarlo o sus criterios de validez y a ello se han dedicado ríos de tinta también en los últimos años por parte

de la doctrina. Esta ha sido también la posición asumida en el RGPD, que ha creado requisitos más estrictos para la solicitud, obtención, prueba y retirada del consentimiento. El capítulo dedicado al consentimiento explora esta discusión.

Tras sentar las bases anteriores, el resto del trabajo se centra en el estudio del interés legítimo como título de licitud alternativo al consentimiento. Se trata de un instrumento comparativamente utilizado en mucha menor medida. Asimismo, los tratamientos basados en interés legítimo han sido tradicionalmente reservados a entornos de escaso uso de tecnologías. De este modo, este capítulo explora el desarrollo de la figura en el RGPD, sus requisitos y su evolución en el cuerpo normativo de protección de datos español, que goza de peculiaridades. Asimismo, el capítulo cubre el ejercicio del derecho de oposición, intrínsecamente ligado al interés legítimo. Todo ello se estudia bajo el prisma de las tecnologías big data para determinar si esta podría ser una base adecuada a las nuevas realidades digitales, detectar sus fortalezas y debilidades. Subsiguientemente, se analizan en un capítulo específicamente dedicado los derechos de acceso, portabilidad y a no ser objeto de decisiones automatizadas. La lógica de la selección de estos derechos ha seguido los siguientes pasos. En primer lugar, se seleccionaron como objeto de estudio los dos derechos que cumplen la doble condición de generar mayor influencia en la capacidad de control de la persona en la sociedad digital basada en datos y que asimismo ostentan diferencias en función de si la base de licitud del tratamiento es el consentimiento o el interés legítimo. Esto es, los derechos de portabilidad y a no ser objeto de decisiones automatizadas. A continuación, la detección de ciertas limitaciones en torno al derecho de portabilidad condujo a identificar el derecho de acceso como una posible salvaguarda. Por último, los derechos de información y el principio de transparencia aparecen de manera trasversal a lo largo de toda la disertación.

Hasta este momento, los capítulos conducen a aclarar y determinar la forma en que el interés legítimo puede lograr su fundamento en la práctica y qué potenciales deficiencias pueden surgir.

La última parte de esta tesis recoge las conclusiones de todo el estudio anterior y propone un modelo de diferentes bases de licitud para diferentes fases del ciclo de vida de un dato cuando este se utiliza en conjunción con tecnologías de datos masivos. Finalmente, en una manifestación de las consecuencias que todo lo analizado puede tener en la práctica, se incluye como anexo la presentación de una guía de buenas prácticas para la aplicación del interés legítimo en entornos big data. Esta guía propone medidas para solventar las limitaciones encontradas a lo largo del estudio, tanto para los propios interesados como para los responsables del tratamiento.

En nuestra durante varias discusiones con otros juristas a lo largo del desarrollo de este trabajo, diversas de las críticas comúnmente vertidas contra el interés legítimo como base de licitud del tratamiento parten de la premisa de que su flexibilidad permite al responsable crear un falso velo de licitud sobre tratamientos que bajo otra base no lo serían.

Ello genera un debate en el que diferentes bases de licitud se comparan bajo prismas diferentes. Por un lado, por ejemplo, el consentimiento, la necesidad de ejecutar un contrato o la obligación legal, sobre los que se presume que deben respetar el principio de transparencia, los deberes de información, el principio de minimización de datos y de limitación de las finalidades. Esta apreciación se produce principalmente respecto del consentimiento.

Por otro lado, un concepto de interés legítimo en ocasiones desvirtuado y que se presenta como una base que otorga al responsable la oportunidad de incumplir esos mismos principios y obligaciones. Así por ejemplo, existe la percepción de que el interés legítimo daría lugar a prácticas no informadas o a tratamientos secundarios de manera incontrolada.

Es lo que podría resumirse como una comparación entre un consentimiento idealizado versus un interés legítimo demonizado. En dichas condiciones, la conclusión es apartarse del interés legítimo como base del tratamiento con carácter general, máxime cuando el tratamiento incluye elementos especialmente complejos como tecnologías de procesamiento de datos masivos, aprendizaje automático, etc.

En los próximos capítulos analizaremos estas cuestiones. En concreto, trataremos de arrojar luz sobre las posibles limitaciones y beneficios de las principales bases de legitimación que un responsable del tratamiento utiliza en el sector privado: el consentimiento, la ejecución contractual y el interés legítimo, con especial énfasis en el estudio del interés legítimo.

3. Metodología

En conjunto, el objetivo de esta disertación es de naturaleza explicativa y normativa,[19] desde una perspectiva interna.[20] Tiene por objeto analizar y describir limitaciones concretas que la utilización de tecnologías de datos masivos crea sobre el modelo del consentimiento, así como el estudio del interés legítimo en una búsqueda de alternativas que mitiguen las asimetrías entre los responsables y las personas. Por otro lado, el trabajo también pretende proponer orientaciones claras sobre el modo en que el interés legítimo puede ser interpretado y aplicado para conseguir un equilibro de intereses en entornos de alta complejidad tecnológica. Para lograr este objetivo normativo, se requiere una considerable investigación preliminar.[21][22] Todo ello se analiza en atención al estado actual del sistema legal en la UE.

[19] SCHWARTZ, Richard L. (1992): "Internal and external method in the study of law", en *Law and Philosophy*, No.11.

[20] ECKES, Christina (2013): "European Union Legal Methods. Moving away from integration", en Ulla Neergaard and Ruth Nielsen (eds.), *European Legal method - Towards a New European Legal Realism?*, DJOF Publishing.

[21] HUTCHINSON, Terry; DUNCAN, Nigel James (2012): "Defining and Describing What We Do: Doctrinal Legal Research", en *Deakin Law Review*, Vol. 17, No. 1.

[22] SIEMS, Mathias M. (2007): *Legal Originality*, Oxford Journal of Legal Studies, Vol. 28.

La primera parte del trabajo realiza una revisión histórica de algunos de los principales hitos en el perfeccionamiento de la ciencia de los datos, que se combina con un análisis paralelo de los hechos principales que marcaron la creación y desarrollo del derecho a la protección de datos personales. El esfuerzo principal de este capítulo se centra en describir dos procesos coetáneos y complejos, tecnológico y normativo, de manera sencilla, pero sin perder profundidad. La búsqueda de este equilibrio es necesaria para permitir sentar las bases generales que nos ayuden a comprender conceptos técnicos ajenos a la teoría jurídica, pero de esencial relevancia para poder interpretar sus consecuencias legales. El resultado inmediato de este análisis es la conceptualización de las tecnologías big data como un proceso compuesto de tres fases, y no como una única actividad. Se trata de las fases de recogida de datos, análisis y aplicación de dichos resultados. Esta división será seguida a lo largo del resto de la tesis y permitirá distinguir diferentes implicaciones jurídicas.

Para los siguientes capítulos se han utilizado fuentes primarias, tales como las propias normas y jurisprudencia, así como fuentes secundarias, como literatura académica y doctrinal.

El estudio del consentimiento y, de forma más breve, la necesidad para la ejecución contractual se basa en un análisis de estas figuras siempre en relación con aquellos tratamientos que hacen uso de tecnologías big data y que, por tanto, crean problemas específicos derivados de su complejidad e impredecibilidad. Debido a la gran cantidad de producción escrita, la revisión se ha centrado en la literatura académica, principalmente en relación con el consentimiento, que en los últimos años ha tratado precisamente el auge de las tecnologías de la información. El análisis persigue recopilar las críticas surgidas en torno a estas bases de licitud, así como identificar otras posibles limitaciones normativas. En consecuencia, se da respuesta a la cuestión de si las bases de licitud asentadas en la manifestación de la voluntad o aquiescencia del interesado son efectivas para garantizar un nivel adecuado de control y protección en entornos tecnológicamente complejos.

El estudio del interés legítimo y el derecho de oposición parte de una metodología similar. Adicionalmente, esta parte cuenta con un análisis jurisprudencial, así como el estudio de cómo se ha trasladado esta figura a la norma española. Este análisis persigue un triple objetivo. En primer lugar, determinar si el interés legítimo como título de licitud puede solventar las limitaciones identificadas respecto del consentimiento. En segundo lugar, identificar qué deficiencias o fuentes de posibles inconvenientes puede implicar. En tercer lugar, analizar si la utilización de esta base en ecosistemas de tecnologías de la sociedad de la información se alinea con el espíritu del RGPD. En este capítulo se da una respuesta preliminar a la cuestión de si el interés legítimo puede potencialmente servir de base alternativa al consentimiento. Para terminar de conceptualizar esta cuestión, en el siguiente capítulo se analizan los derechos de portabilidad, acceso y no ser objeto de decisiones automatizadas. Metodológicamente, se analiza la norma en búsqueda de lagunas.

Finalmente, el último capítulo se basará en evaluar la interrelación entre todos los conceptos jurídicos extraídos hasta el momento que aúna el conocimiento extraído sobre la existencia de lagunas jurídicas, las posibles limitaciones interpretativas y la existencia de alternativas. Ello da lugar a la especificación de recomendaciones de aplicación normativa y el desarrollo de una propuesta de guía de buenas prácticas, que se incluye como anexo. Por último, tras las conclusiones, la disertación aleja la vista de lo concreto que nos ha ocupado hasta este momento y finaliza con una serie de consideraciones finales de carácter más amplio que se extraen de todo lo analizado en el trabajo pero que lo trascienden.

Existe un aspecto relevante que ha caracterizado todo el estudio que se deriva de este trabajo. Durante el desarrollo de esta tesis ha tenido lugar un cambio normativo de gran calado, impulsado por la entrada en vigor y en aplicación del RGPD y la subsiguiente LOPDgdd. Estas normas han terminado por impulsar modificaciones, por ejemplo, en el régimen del consentimiento y sus requisitos de validez, los principios de transparencia y de responsabilidad proactiva, que sin duda influyen en las conclusiones.

A sensu contrario, el régimen del interés legítimo ha sido escasamente modificado, hecho del que también se desprenden conclusiones. En cualquier caso, el panorama tecnológico y normativo ha sufrido una profunda evolución precisamente durante el ciclo de este trabajo. Debido a esta novedad normativa, parte de la producción y el pensamiento jurídico se ha volcado en revisar el pensamiento sobre aquellos aspectos de la norma que presentan cambios más sustanciales, como puede ser el régimen del consentimiento, dejando en un segundo plano aquellos otros aspectos sobre los que no han tenido lugar tales modificaciones, como es el caso del interés legítimo.

4. Relevancia socio-científica

La tendencia actual hacia los servicios que se basan en el tratamiento de enormes cantidades de datos personales tiene como consecuencia el surgimiento de problemáticas y retos nuevos. En consecuencia, debemos analizar si las normas y el modo en que estas se aplican se encuentran óptimamente adaptados. Si bien es cierto que el estudio del big data como disciplina se encuentra en España en una fase de crecimiento en áreas como la informática o el marketing, resulta mucho más incipiente en el campo de las ciencias sociales y jurídicas, a pesar de su importancia.

La importancia de este trabajo radica en primer lugar en la realización de una explicación sencilla del proceso de evolución que dio como resultado las tecnologías de tratamiento masivo de datos, así como del estudio de mecanismos jurídicos que se adapten a las novedades que dichas tecnologías han creado. En un contexto marcado por la intensidad innovativa, se torna fundamental que los juristas realicen un esfuerzo por comprender y transmitir conceptos técnicos que serán la base de los tratamientos normativos presentes y futuros. Así, la conceptualización de las tecnologías big data como un proceso de tres fases facilita el estudio de las implicaciones legales de diferentes actividades, desde la recogida masiva de datos, la creación y observación de nuevo conocimiento a partir

del análisis de datos o la aplicación de estos a procesos de toma de decisiones.

Más importante, esta investigación viene a llenar el vacío creado por la escasez de estudios académicos en torno a la búsqueda de bases de licitud alternativas al consentimiento para aquellos procesos que conlleven un tratamiento de datos personales haciendo uso de tecnologías big data. Específicamente, este trabajo aborda la posibilidad de aplicar una herramienta normativa ya existente, el interés legítimo, de modos hasta ahora descartados en la práctica, a pesar de que nada en la redacción jurídica así lo decrete. En este sentido, constituye también una aportación la desmitificación de aquellas concepciones negativas que en la esfera jurídica se atribuyen al interés legítimo, así como la presentación de una propuesta de buenas prácticas que pretende tener aplicación práctica inmediata en el contexto digital actual.

Así, la tesis propuesta es coherente el objeto de protección de la norma, en la medida en que aporta un elevado grado de garantías que deben ser observadas por el responsable en favor de los interesados, al tiempo que permite flexibilizar el tratamiento de datos, su flujo y los tratamientos.

5. Alcance y delimitación de la investigación

Los procesos big data hacen uso de grandes cantidades de datos personales y no personales. Este trabajo centra su atención en aquellos procesos que hacen uso de datos personales, definidos en el art. 4 RGPD. En este sentido, los procesos big data utilizan, no solo datos personales de aquél que será objeto de una decisión, sino también de otras muchas personas. Los datos pasados de multitud de personas son la base para predecir comportamientos de otras.

Esta investigación está centrada territorialmente en la Unión Europea y por tanto las fuentes jurídicas y la doctrina consultada se refieren principalmente al Derecho comunitario. Para ello, el principal instrumento

jurídico de estudio será el Reglamento General de Protección de Datos,[23] la anterior Directiva de protección de datos, así como la jurisprudencia del Tribunal de Justifica de la Unión Europea. Además, para determinados aspectos, tomaremos como referencia la conocida como Directiva e-Privacy o de comunicaciones electrónicas,[24] que actualmente se encuentra en proceso de actualización en lo que será el futuro Reglamento e-Privacy. Esta decisión se justifica por el hecho de que los retos de la sociedad de la información y las tecnologías de datos masivos trascienden por naturaleza las fronteras nacionales. Asimismo, por el hecho de que el principal instrumento de protección de datos personales en la UE adquiera la forma de Reglamento. En efecto, la elección de un Reglamento como modo de ordenar esta rama del Derecho pretende lograr un alto grado de armonización entre los Estados miembros. Por este motivo, el estudio desde la perspectiva comunitaria cobra mayor sentido que el análisis del derecho nacional. Sin embargo, determinados aspectos de la investigación gozan de particularidades en Derecho español y son por tanto analizados también desde esta perspectiva. Para ello, las normas tomadas como referencia serán la Ley Orgánica de Protección de Datos y garantía de los derechos digitales,[25] así como la derogada Ley Orgánica de Protección de Datos.[26] Se trata, en concreto, de analizar algunos hechos específicos que pueden explicar la particular visión que en la práctica se ha dado en España a la figura del interés legítimo. Estas ayudarán a contextualizar el debate y pueden revelar por qué las propuestas y recomendaciones con las que

[23] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

[24] Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas).

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

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

cierra la disertación pueden resultar cuanto más novedosas dentro de nuestras fronteras.

Por su parte, el ámbito material de estudio se circunscribe al tratamiento de datos personales llevados a cabo en el sector privado o los usos comerciales de aquellos desarrollos que conllevan la aplicación de tecnologías big data. En el sector privado, las bases de legitimación generalmente aplicables son el consentimiento (art. 6.1.a) RGPD), la ejecución contractual (art. 6.1.b RGPD) y el interés legítimo (art. 6.1.f) RGPD). Este trabajo considera estas tres, aunque otorga un peso especialmente relevante al consentimiento y al interés legítimo. Por otro lado, el tratamiento de categorías especiales de datos requiere que el responsable identifique cumulativamente una base de licitud del art. 6 RGPD junto con una excepción de entre las establecidas en el art. 9 RGPD.[27] Las condiciones del art. 9 se encuentran fuera del ámbito de estudio de este trabajo.[28] Del mismo modo, el uso de datos personales por parte de las administraciones públicas o en relación con la investigación policial y criminal[29] no han sido parte del estudio.

Este estudio no pretende ignorar los evidentes beneficios que el uso de los avances tecnológicos aporta a nuestra vida. Pensemos, por ejemplo, en la facilidad de poder acceder a fuentes de información prácticamente ilimitadas a través de una simple búsqueda en internet, de la comodidad de poder almacenar nuestras fotografías en un servicio en la nube o de

[27] Véase, por todas, DATA PROTECTION COMMISSION, (2019): *Guidance Note: Legal Bases for Processing Personal Data*. Disponible en: https://www.dataprotection.ie/sites/default/files/uploads/2019-12/Guidance%20on%20Legal%20Bases_Dec19_1.pdf.

[28] Para ampliar sobre estos extremos, ver, entre otros, DE MIGUEL, Íñigo; MÉNDEZ GARCÍA, Miriam; ALFONSO FARNÓS, Iciar (2019): "La legitimación para el tratamiento de categorías especiales de datos con finalidades de investigación en el marco del Reglamento (UE) 2016/679 y de la Ley Orgánica 3/2018", en *Revista de Derecho y Genoma Humano*, No. Extraordinario, p. 205-231.

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

comunicarnos instantáneamente con personas que se encuentran al otro lado del mundo. En reflejo de ello, una parte importante de este trabajo se centra en analizar los intereses legítimos de las organizaciones y las vías para poder aplicarlos con carácter general. Sin embargo, el análisis jurídico de los derechos de las personas requiere un análisis crítico de la norma, la búsqueda de sus limitaciones y las posibles fuentes de impactos negativos. Por este motivo, gran parte de la atención se centra en aquellos aspectos nocivos inherentes a las tecnologías o la posibilidad de que un responsable actúe de manera poco ética o con menosprecio a la licitud haciendo uso de lagunas legales en búsqueda de un beneficio propio. Este trabajo no pretende presuponer que este sea el modo de actuación por defecto de la generalidad de responsables y organizaciones, sino simplemente apuntar su esfuerzo dirigido a detectar situaciones en las que esto pueda suceder.

Abordaremos problemas específicos a las tensiones entre las tecnologías de datos masivos y la regulación de las bases de licitud de las normas de protección de datos. Particularmente, el objetivo de este trabajo es encontrar oportunidades para interpretar y aplicar las normas existentes sin oprimir el desarrollo técnico y ofreciendo un nivel de garantías superior para las personas. En consecuencia, se propondrán soluciones que abarcarán desde el desarrollo de determinados conceptos por vía interpretativa hasta la creación de medios de autorregulación a través, por ejemplo, de códigos de conducta que suplan la lentitud del proceso legislativo ordinario. Para ello, esta tesis culmina con la creación de una guía de buenas prácticas que tiene en cuenta aquellos aspectos que han sido objeto de investigación.

A pesar de la delimitación del ámbito de estudio, este trabajo no ignora el hecho de que los retos que las tecnologías de datos masivos ponen de manifiesto en ámbitos que trascienden la privacidad, la intimidad o la protección de los datos personales. Una visión cegada por dirigir únicamente la atención sobre un espacio normativo limitado será nociva para la efectiva protección de los derechos de las personas, la creación de seguridad jurídica y el desarrollo tecnológico. Otras ramas del Derecho jugarán también un papel relevante a la hora de afrontar el desarrollo de

actividades que hacen uso intenso de las tecnologías de la información. Será, de hecho, la combinación de diversas áreas jurídicas el único modo de dar una respuesta completa a los retos jurídico-sociales del presente y del futuro. Sin embargo, la investigación durante el desarrollo de una tesis doctoral exige concreción en el ámbito de estudio.

Este trabajo no pretende ser la exposición final de las soluciones a los problemas que afronta el usuario en entornos digitales, y en concreto, en relación con la prestación de su consentimiento o la ponderación de intereses y derechos, sino únicamente paso más más en el camino hacia una conversación y un debate más amplio en torno a diferentes alternativas.

CAPÍTULO II. HISTORIA DE LA CIENCIA DE DATOS Y SU REGULACIÓN

> "Debe insistirse en la necesidad de considerar el derecho a la protección de datos como pieza clave del sistema democrático. Derecho que además es esencial para el desarrollo efectivo de otros derechos, como el de no discriminación, libertad de residencia y circulación, igualdad, derecho al trabajo, etc., y, en definitiva, para el respeto a la dignidad humana".[30]

1. Introducción

Desde incluso antes de que surgiera la escritura hasta las potentes bases de datos actuales, los seres humanos no han dejado de recopilar información. Así, diferentes culturas han desarrollado lo que podríamos considerar bases de datos que ayudaban a su sustento. En este desarrollo, la evolución hacia formas cada vez más sofisticadas de recopilar y almacenar la información han venido marcadas por la necesidad de hacer frente a cantidades de datos crecientes y las limitaciones que los sistemas de cada momento presentaban. Por ello mismo, el big data puede ser un concepto reciente en la historia de la humanidad, pero sus cimientos se retrotraen muy atrás en el tiempo.

El incremento en la recopilación de información estrechamente ligada a las personas comenzó con el tiempo a abrir debates doctrinales en torno a la necesidad de crear una esfera de protección frente a posibles abusos o prácticas que afectaran intereses individuales que, en última instancia, están ligados al desarrollo de la personalidad. Con ello, el desarrollo jurídico

[30] PIÑAR MAÑAS, José Luís (2009): "Seguridad, transparencia y protección de datos: el futuro de un necesario e incierto equilibrio. Documento de trabajo 147/2009", en Laboratorio de Alternativas, Centro de Estudios Políticos y Constitucionales, p. 58.

del derecho a la privacidad y la intimidad, en un primer momento, y de protección de datos personales, en un momento posterior, fueron tomando fuerza hasta ser considerados derechos fundamentales en la Unión Europea.

En la actualidad, el desarrollo de tecnologías que permiten la recogida y tratamiento de datos y la protección de los derechos y libertades personales están intrínsecamente ligadas.

En este capítulo analizaremos algunos de los principales hitos históricos del proceso que culminó con la llegada de las tecnologías big data y la protección jurídica de los datos personales. El objetivo, más que realizar un estudio detallado de cada paso histórico es comprender el camino recorrido analizando una selección de hechos concretos, que nos ayude a entender el contexto actual, sobre el que después se desarrollarán los siguientes capítulos.

2. La Antigüedad

Las técnicas de realización de cálculos, así como de almacenamiento de información y acceso a esta han ido evolucionando con la humanidad desde sus inicios. Los orígenes de las bases de datos se remontan a la Antigüedad.

Por ejemplo, el imperio inca desarrolló un instrumento muy simple, el quipu, que consistía en una larga cuerda gruesa de la que colgaban cuerdas secundarias de diferentes colores en las que se realizaban una serie de nudos, que representaban diferentes cifras. El quipu tenía numerosos usos, desde contabilizar la población de las ciudades hasta controlar el pago de impuestos.[31] También se cree que el quipu podía representar letras y vocablos y, de este modo, ser un instrumento para conservar y transmitir leyendas e hitos históricos del momento. De hecho, la complejidad del sistema de almacenamiento de información en los quipus hacía necesaria

[31] ASCHER, Marcia; ASCHER, Robert (2013): *Mathematics of the Incas: Code of the Quipu*, Courier Corporation, p.10.

la labor de los quipucamayos, expertos encargados de codificar y descodificar la información en los quipus, que se convirtieron en un elemento fundamental en la administración inca.[32] En consecuencia, puede considerarse al quipu como una forma primitiva de base de datos.

Otro artilugio aritmético desarrollado para realizar cálculos de forma sencilla a partir de una forma originaria de tabla fue el ábaco, que ya había sido utilizado en Babilonia hacia el año 2400 a.C. Posteriormente, en torno al año 150 a.C, los griegos fabricaron el llamado mecanismo de Anticitera,[33] el primer ordenador analógico de la historia, compuesto por un conjunto de engranajes de bronce, similar a un reloj. Su función era predecir eclipses y calcular la posición astronómica de los planetas, para elaborar el calendario y así poder determinar, entre otras cosas, la fecha de eventos como los Juegos de Olimpia. Tras la destrucción y desaparición de este avance, no volvió a existir un mecanismo de tanta complejidad hasta casi mil años más tarde.

3. Siglo XIX. Inicio del tratamiento automatizado de la información y concepto de privacidad

Los siglos pasaron desde aquellos desarrollos técnicos más arcaicos hasta llegar al siglo XIX.

El término inteligencia de negocio fue utilizado por primera vez en 1868 de un modo no relacionado con el uso o el avance tecnológico sino con mero uso de la información como estrategia para la toma de decisiones informadas. [34]

[32] PAREJA, Diego (1986) “Instrumentos prehispánicos de cálculo: el quipu y la yupana”, en *Revista Integración*, Vol. 4, No. 1, p-38-43.

[33] PALAZÓN, Javier (2014): “¿Un ordenador en la Antigua Grecia? El misterioso mecanismo de Anticitera”, en *Estratos*, No. 107, p. 53-54.

[34] MARIANI, Marcello; et al, (2018): “Business intelligence and big data in hospitality and tourism: a systematic literature review”, en *International Journal of Contemporary Hospitality Management*, Vol. 30, No. 12, p. 3515.

En este sentido, el término fue esgrimido para describir el motivo del gran éxito del banquero Sir Henry Furnese. Sir Henry obtenía gracias al análisis de información un conocimiento altamente detallado de los acontecimientos políticos y de mercado de su época; de hecho, antes que sus competidores, lo que le permitía tomar decisiones más informadas y de manera más temprana. “El nombre de Sir Henry Furnese figura extensamente entre los banqueros de la época que aportaron notoriedad a los financieros de su tiempo. A lo largo de Holanda, Flandes, Francia y Alemania, mantuvo un completo y perfecto estudio de inteligencia de negocio. Las noticias sobre las múltiples batallas combatidas le llegaban primero a él”. [35]

El concepto no se utilizó de nuevo en varias décadas. En este impasse, comenzaron las primeras actividades de tratamiento automatizado de la información basados en el uso de máquinas troqueladoras, cuyo origen se remontaba a la revolución industrial.

En efecto, el inicio del tratamiento automatizado de la información tiene sus raíces más directas en los telares de la industria textil francesa en 1725 y las décadas posteriores. Fue entonces cuando se comenzaron a utilizar tarjetas perforadas para controlar el movimiento de las agujas de los telares y los patrones que se creaban en las telas. Estas tarjetas perforadas eran unas simples láminas de cartulina con pequeños óvalos perforados que contenían información sobre el movimiento que debían seguir las agujas para crear cada diseño. De este modo, en función de la disposición de las tarjetas y de las perforaciones de cada una de ellas, el telar creaba diferentes patrones, y con ello se facilitó crear complejas trazas de forma sencilla.[36]

En este escenario, la tecnología continuó evolucionando y los datos que creaba el hombre fueron creciendo, llegando en ocasiones a suponer un problema para poder gestionarlos. El uso de las tarjetas perforadas se

[35] MILLER DEVENS, Richard (1868): *Cyclopaedia of Commercial and Business* Anecdotes, D. Appleton, p. 210. [Traducción propia].

[36] PIÑOL TORRENT, Francesca (2016): “De la tradición al diseño textil digital”, en *Primer Simposio de la Fundación Historia del diseño*, Barcelona, p. 5.

extendió entonces a otros ámbitos para permitir una gestión de datos más eficiente. Un ejemplo de ello fue la elaboración del censo de Estados Unidos.

En efecto, para elaborar el censo de población de Estados Unidos de 1880 fueron necesarios casi nueve años de trabajo, debido a la cantidad de datos que necesitaban ser analizados de forma manual. En ese momento, se calculó que para elaborar el censo electoral de 1890 serían necesarios diez años de trabajo; es decir, que el censo no estaría finalizado hasta que hubiera llegado el momento de realizar el siguiente.[37] Fue por ello que Hollerith se percató de que las preguntas contenidas en el cuestionario para elaborar el censo se podían responder con un simple "sí" o "no". Sobre esta base, creó una máquina tabuladora que permitía introducir toda la información en una tarjeta perforada del tamaño de un billete de dólar y formada por una tabla de diversas columnas, con la que se pudo gestionar esa gran cantidad de datos y reducir considerablemente el tiempo de creación del censo.

Se trataba de una simple tabla formada por columnas que contenían información como la dirección de la vivienda, el número de personas que la habitaban, la raza, si se trataba, por ejemplo, de un soldado o marine, viuda, prisionero de guerra, convicto, granjero, etc.

Este fue el inicio del tratamiento automatizado de la información y de las bases de datos tal y como se conocen en la actualidad. Hollerith, considerado por algunos el primer informático de la historia y el primero en llevar a cabo un tratamiento automatizado de la información, patentó su invención, y creó la empresa *Tabulating Machine Company* para explotar esta nueva máquina, que fue el germen de la empresa actual IBM (*International Business Machines Corporation*).

En paralelo con los primeros tratamientos automatizados de la información comenzó a surgir la preocupación por los posibles usos indebidos que de

[37] BABINIP, Nicolás (2003): “Las antecesoras de la computadora: la era de la tabuladora”, en *Revista de Historia de la Ciencia Saber y Tiempo*, Vol. 4, No. 16, p. 77.

ella se podrían hacer. El debate en torno a la libertad personal y el avance técnico dio como resultado el surgimiento de la construcción doctrinal del "derecho a ser dejado en paz" por Cooley en 1988[38] y al concepto de privacidad, que fue perfilado desde el punto de vista jurídico en 1890 por Samuel Warren y Louis Brandeis.[39]

4. Los años 50 y 60. Automatización del tratamiento de información y derecho al respeto a la vida privada.

Desde 1900, el sistema de tarjetas perforadas de Hollerith se convirtió en el primer medio de almacenamiento de datos y procesamiento automatizado. El tamaño de las tarjetas fue evolucionando e incorporando un cada vez mayor número de columnas y perforaciones, mediante los que se posibilitaba el tratamiento de un mayor volumen de datos. Para el año 1950, IBM ya había desarrollado esta tecnología y sus tarjetas se habían vuelto indispensables para el tratamiento de grandes volúmenes de datos numéricos, tanto por las empresas privadas como la Administración.[40] Este avance en la recolección y análisis de información fue acompañado por los avances en el almacenamiento de la información, uno de cuyos hitos fue la creación del disco duro, también por IBM en la misma época.

Con la llegada del siglo XX, el tratamiento de datos, y concretamente de datos personales, comenzó a crecer en intensidad, creando así conciencia de los riesgos que dicho tratamiento abría. De hecho, la máquina tabuladora de Hollerith está ligada a uno de los momentos más oscuros en el uso de los datos personales, pues fue utilizada durante el régimen del holocausto nazi en su ímpetu por sistematizar información como el origen

[38] COOLEY, Thomas McIntyre (1888): *A Treatise on the Law of Torts or the Wrongs which Arise Independent of Contract*, 2ª ed., Chicago, Callaghan & Co.

[39] D. WARREN, Samuel; BRANDEIS, Louis D. (1890): "The right to privacy", en *Harvard Law Review*, p. 193-220.

[40] BABINIP, Nicolás (2003): "Las antecesoras de la computadora: la era de la tabuladora", en *Revista de Historia de la Ciencia Saber y Tiempo*, Vol. 4, No. 16, p. 79.

racial, edad u ocupación de la población; información sobre la cual se tomaban decisiones posteriores acerca del destino de cada persona.[41]

Así fue como en 1950 se firma la conocida como Convención Europea de Derechos Humanos, cuyo artículo 8 proclama el derecho al respeto a la vida privada y familiar. Este derecho protege una esfera de intimidad del domicilio, así como la inviolabilidad de la correspondencia. La correspondencia, que en aquel momento se realizaba mayoritariamente en papel, fue evolucionando con el tiempo hasta los actuales medios digitales como el correo electrónico, o mensajes de aplicaciones móviles. El art. 8 de la Convención es así el precursor de la normativa presente sobre confidencialidad de comunicaciones electrónicas. Es reseñable que el término "privacidad" no es expresamente utilizado en la redacción del art. 8 de la Convención y, de hecho, hasta casi dos décadas después no se comenzó a hacer referencia a este precepto como un derecho general a la privacidad.

Con el paso de los años, la literatura vuelve a mostrar de nuevo el uso del término "inteligencia de negocio" en una publicación del ingeniero Hans Peter Luhn en 1958.[42] Mientras en la primera aparición de este término, como comentábamos, el concepto no hacía referencia al uso de tecnologías, sino únicamente a la toma de decisiones informadas, la definición aquí utilizada ya se refería al uso de tecnologías de la información. Este cambio acerca el término un paso más a su concepción actual. El artículo resaltaba la creación de cada vez más información en las organizaciones, lo que había creado barreras y divisiones entre diferentes almacenes de información que conllevaban que la información no fuera conocida antes de la toma de decisiones. En este contexto, la mejora en la automatización en el tratamiento de la información tenía grandes beneficios

[41] LUEBKE, David Martin; MILTON, Sybil (1994): "Locating the Victim: An Overview of Census-Taking, Tabulation Technology and Persecution in Nazi Germany", en *16 IEEE Annals of the History of Computing*, No. 3, p-25-39.

[42] LUHN, Hans Peter (1958): "A business intelligence system", en *IBM Journal of research and development*, Vol. 2, No. 4, p. 314-319.

potenciales. Sin embargo, la automatización conllevaba mayor complejidad del sistema. Por este motivo, la gestión de los datos debía encomendarse a personas especializadas en la realización de búsquedas en las llamadas "librerías" de datos.

Es decir, parece que el concepto de inteligencia de negocio se refería ya a tratamientos de la información que suponían el uso de tecnologías con la finalidad de conocer la información disponible, ordenarla y poder hacerla accesible a las personas relevantes para la toma de decisiones en la organización. Así, esta noción estaba aún lejos de la noción actual de inteligencia de negocio. El artículo de Luhn trata de describir una idea de tecnología aún no desarrollada, sino que se encontraba por crear pero que, sin embargo, parece introducir términos que serían desarrollados en años posteriores como las bases de datos, los lenguajes de consulta o *queries* o la importancia del uso de metadatos en la gestión de la información.

También se ponían expresamente de manifiesto las mayores dificultades en el tratamiento de la información del momento: la dificultad de gestionar volúmenes de información creciente, y la necesidad de recurrir a profesionales especializados para poder extraer información concreta de las librerías, con la dificultad que eso entrañaba para el usuario final de la información.

A partir de la década de 1960 se comenzó a utilizar el término "base de datos", que podemos definir como una colección de información ordenada, de manera tal que pueda ser fácilmente accesible y manejable. Más concretamente, fue el Diccionario de inglés de Oxford el que, en 1962, utilizó el término base de datos en un sentido técnico por primera vez.[43]

Las primeras bases de datos eran relativamente "planas", lo que implica que se trataba básicamente de un conjunto de filas y columnas. Un ejemplo de estas bases de datos planas eran aquellas tablas creadas por Hollerith

[43] OXFORD ENGLISH DICTIONARY, Words from the 1960s; HAIGH, Thomas (2009): "How Data Got its Base: Information Storage Software in the 1950s and 1960s", en *IEEE Annals of the History of Computing*, Vol. 31, No. 3, p. 17.

para realizar el censo electoral de Estados Unidos. Otro ejemplo puede ser una guía telefónica, compuesta por un listado de nombres y números de teléfono. El uso de las tarjetas perforadas fue poco a poco cayendo en desuso y sustituyéndose por medios más modernos de almacenamiento y procesamiento de datos como el CD-ROM, cuya tecnología se basa de hecho en un principio similar al de las tarjetas. Esto propició que a partir de la segunda mitad de los años 60 la computación comenzó a ganar importancia.

Con la memoria reciente del uso de datos personales por parte del régimen nazi, a finales de los años 60 se comenzó a configurar una noción jurídica de privacidad entendida como el ejercicio de control propio sobre la información,[44] mientras que en Estados Unidos comenzaba a debatirse la necesidad de proteger este concepto mediante legislación.

5. Los años 70. Simplificación del análisis de datos y primeras normas nacionales.

5.1. Tecnología: bases de datos relacionales y lenguaje SQL

En las décadas siguientes la creación de información se encontraba en pleno auge en todos los sectores, desde el científico hasta los negocios, y su magnitud había alcanzado un nivel preocupante para ser almacenada. Acceder a la información era una tarea muy compleja llevada a cabo solo por expertos, lo que la convertía en una labor que exigía demasiado tiempo y recursos.

Esto propició que en 1970 el matemático de IBM Research Lab, Edgar F. Codd, molesto por las dificultades que creaban los sistemas de búsqueda en las bases de datos hasta la fecha, desarrollara un nuevo modelo de base de datos, denominado "relacional", cuyas bases recogió en su artículo “Un

[44] GONZÁLEZ FUSTER, Gloria (2014): *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, Vol. 16, 1ª ed., Springer International Publishing, p. 48.

modelo relacional de datos para grandes bancos de datos compartidos".[45] Se trata de un sistema que organiza la información de manera jerárquica y que permite acceder a la información almacenada en grandes bases de datos mediante un método de índice simple. Esto significa que cualquier persona podía utilizar las bases de datos, aun sin saber cómo estaba estructurada la información dentro de dicha base de datos. Todavía hoy en día la mayor parte de las transacciones de datos rutinarias, como acceder a nuestras cuentas bancarias o reservar un viaje a través de internet, utilizan estructuras basadas en la base de datos relacional, y es previsible que esto continúe siendo así en las próximas décadas.

La explicación del modelo relacional realizada por Edgar F. Codd parte de conceptos matemáticos como los de relación, modelos binarios, proyección, permutación, etc., y de la demostración matemática de la eficiencia de su modelo. Los conceptos matemáticos que subyacen bajo este modelo exceden nuestro ámbito de estudio, de modo que nos centraremos en presentar las nociones básicas más necesarias.

Baste decir que Codd demostró que este sistema, basado en la rama de las matemáticas conocida como "cálculo de tuplas",[46] posibilitaba realizar todas las operaciones que permitían las bases de datos tradicionales. Al mismo tiempo, la base de datos relacional permitía crear un medio de acceso simple a toda la información relativa a un registro. Recordemos que el principal problema de las bases de datos hasta el momento era la dificultad que tenían los usuarios no expertos para acceder a dicha información, de modo que la creación de un medio sencillo de explotar los datos tuvo un enorme impacto.

[45] CODD, Edgar F. (1970): "A relational model of data for large shared data banks", en *Communications of the ACM*, Vol. 13, No. 6, p. 377-387.

[46] Una tupla es una secuencia ordenada de valores que se agrupan de forma que funcionan como un único valor. Cada uno de los datos que conforman una tupla es conocida como tuple. Así, en el campo del cálculo relacional, las tuplas proporcionan la base para formular la definición de la relación con la que se crea una base de datos relacional.

En términos sencillos, el modelo relacional consiste en organizar los datos en tablas (también denominadas relaciones), que se componen de columnas o atributos. Hasta aquí, el concepto es idéntico al que describíamos para las bases de datos planas de las décadas anteriores. La contribución radica en que, mientras en la base plana cada dato se introduce una única vez en una única tabla, el modelo relacional permite asociar o relacionar diversas tablas a través de algún campo común, para que un mismo dato aparezca en diversas tablas al mismo tiempo. Así, modificando los datos en una de las tablas, se pueden modificar de manera automática todas las demás tablas asociadas a ella. Esto es, el modelo relacional permite, no solo crear la base de datos, sino operar dentro de ella.

Esto es posible gracias a aquellos campos que actúan como identificadores únicos o "llaves", que singularizan un registro de forma inequívoca dentro de la base de datos. De este modo, una base de datos puede contener tablas cuyas columnas tengan el mismo nombre o encabezado, pero cuyos registros puedan diferenciarse debido a dichos identificadores únicos. Por medio de estas llaves también se pueden re-asociar datos de diferentes tablas relacionados entre sí, y esto constituye una característica nueva respecto a los sistemas previos de organización de bases de datos. Estas llaves o identificadores únicos son también un concepto fundamental para proteger la privacidad de los individuos a los que se refieren los registros, en la medida en que permiten identificar de forma directa a quién pertenece la información, así como una la cadena de datos asociados entre sí.

En conclusión, el modelo relacional permitía que un usuario de la base de datos pudiera introducir información o buscarla en función de las relaciones que se hubiesen creado entre los datos, las tablas, y las llaves. Además, estas bases de datos permiten realizar consultas que necesitan múltiples tablas u operaciones antes de devolver un resultado, como agregar datos de diferentes tablas. En otras palabras, el modelo de bases de datos relacionales supuso una explosión en la utilización de información y sus

beneficios, pero también potenció los riesgos del uso indebido de los datos y del acceso a información cada vez más rica sobre una persona.

Fue también en el seno del IBM Research Lab donde, en 1975, se diseñó un nuevo lenguaje de consulta estructurado para acceder a las bases de datos relacionales, conocido por sus siglas en inglés SQL ("*structured query language*" o lenguaje de consultas estructurado), cuya utilización sigue ampliamente extendida hoy en día. Este lenguaje permite, de forma sencilla, efectuar consultas en bases de datos cada vez más grandes, realizar cambios u operaciones en ellas. En este momento, el uso de los ordenadores personales en las empresas se encontraba en auge y se fundaron sociedades como Oracle o SAP. A finales de esta década, fue precisamente Oracle quien comenzó a comercializar paquetes basados este nuevo lenguaje SQL, lo que le permitió alcanzar un gran dominio del mercado.

En este punto es útil detenerse para comprender estos conceptos para obtener un mejor juicio acerca del potencial de estos avances tecnológicos y de su consiguiente riesgo para la esfera privada de una persona.

Una "*query*" es una petición de información que se realiza a una base de datos, o, con otras palabras, una consulta. De este modo, el "*structured query language*" o SQL es un lenguaje utilizado para realizar consultas a las bases de datos. Una consulta SQL se asemeja a una frase en inglés a través de la que el usuario describe lo que quiere obtener y de dónde. Su uso es relativamente sencillo, incluso para los no expertos. Está reconocido como el lenguaje estándar para comunicarse con bases de datos relacionales, y actualmente es el lenguaje más utilizado para lanzar consultas a bases de datos, utilizado por programas tan extendidos como Microsoft Access, que no es más que un sistema de gestión de bases de datos.

Veamos un corto ejemplo ilustrativo.

Ejemplo: Base de datos relacional

Un paciente puede acudir al médico muchas veces en la vida. En cada visita que realiza el paciente le puede atender un médico distinto por padecer una patología diferente. A su vez, un mismo médico atiende a numerosos pacientes. De este modo, la base de datos de un hospital o centro médico se puede establecer una relación entre los pacientes y los médicos mediante la tabla "Visitas".

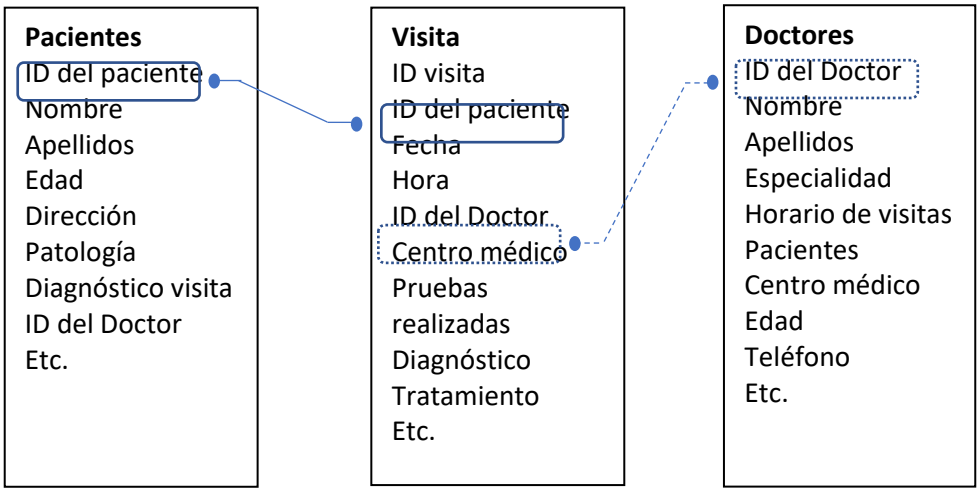

Gráfico 1: Tabla de datos relacional. Fuente: Elaboración propia

Los campos que relacionan las diferentes tablas son los de identificador o ID del paciente e identificador o ID del doctor. Estos campos tienen su origen en su tabla correspondiente, en la que fueron creados (tabla "Pacientes" o tabla "Doctores"), pero esos mismos datos se podrán ver en la tabla "Visitas" gracias a las relaciones que se han creado. De esa forma, los datos de una visita concreta procederán en parte de las tablas "Médicos" y "Pacientes" y en parte serán datos propios de visitas, tales como la fecha o las pruebas realizadas. Asimismo, para acceder a la información, un usuario no especializado en la gestión de bases de datos (enfermera, médico, personal administrativo, etc.) puede simplemente introducir los datos del paciente sobre el que quiere

conocer información. El proceso informático que se ejecuta en el ordenador conlleva realizar una consulta o *query* en lenguaje SQL.

Una sentencia SQL permite numerosas operaciones como, por ejemplo, seleccionar todos los pacientes atendidos por un médico específico, ordenar las visitas por fecha y hora, o filtrar los pacientes por edad. De este modo, si quisiéramos seleccionar aquellos pacientes con una edad superior a 45 años, la *query* que a ejecutar sería algo tan sencillo como:

```
SELECT Código_del_paciente FROM Pacientes WHERE
Edad > 45
```

Para cargar los datos de una visita concreta, la base de datos necesita ejecutar asociaciones y cargar datos provenientes de diferentes tablas antes de devolver el resultado por el que se le pregunta, que puede ser, por ejemplo, el historial de visitas del paciente número 8652174. Este proceso precisa, por tanto, de una base de datos relacional.

5.2. Derecho: las primeras normas nacionales

En esencia, la década de los 70 consagró la tendencia de los años anteriores por la que la adopción de la tecnología creció, lo que permitía no solo generar, recoger y almacenar cada vez mayor cantidad de información, sino, sobre todo, de someterla a tratamiento.[47]

A partir de ello se abrieron infinidad de nuevas posibilidades sobre el uso de información. No es de extrañar por tanto que, en paralelo a todo ello, la década de 1970 fue un punto de inflexión en el desarrollo legislativo en torno al tratamiento de datos personales, y más concretamente, el tratamiento automatizado de dichos datos.[48]

[47] PIÑAR MAÑAS, José Luís (2005): "El derecho fundamental a la protección de datos personales. Algunos retos de presente y futuro", en Asamblea: revista parlamentaria de la Asamblea de Madrid, No. 13, págs. 21-46.

[48] GONZÁLEZ FUSTER, Gloria (2014): *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, Vol. 16, 1ª ed., Springer International Publishing, p. 55.

HESSE. La norma de protección de datos del estado alemán de Hesse de 1970 es considerada el primer instrumento legislativo[49] de protección de los datos personales en Europa,[50] cuyo alcance era el uso de datos personales por parte del sector público e incidía en que cualquier uso de estos debía estar legitimado. Comprendiendo el camino previo recorrido y la experiencia de los horrores del régimen nazista se comprende que la primera norma de protección de datos fuera alemana y estuviera directamente dirigida a limitar el tratamiento de datos por parte de las autoridades públicas. De hecho, desde ese momento, Alemania ha sido uno de los grandes influyentes en los subsecuentes desarrollos legislativos en materia de protección de datos personales.[51]

SUECIA. Poco después, en 1973, Suecia se convertía en el primer país en publicar una norma de protección de datos de alcance nacional, cuyo ámbito de aplicación cubría el tratamiento de datos por parte del sector público y privado, y se refería expresamente al uso de técnicas de computación.[52] De nuevo, ello se entiende gracias a que en dicho momento Suecia ya poseía repositorios que permitían un tratamiento automatizado de los datos de sus ciudadanos, un desarrollo técnico al que se quiso imponer sanas autolimitaciones con el objetivo de proteger los derechos y libertades de los individuos.

ALEMANIA. Tras la experiencia de Hesse, a la que siguieron otros estados alemanes, finalmente Alemania promulgó su primera norma federal de

[49] Al otro lado del Atlántico, se desarrollaron las normas estadounidenses Fair Credit Reporting Act de 1970 o la Privacy Act de 1974. HONDIUS, Frits (1975): *Emerging Data Protection in Europe*, North-Holland, p. 6.

[50] KOSTA, Eleni (2013): *Consent in European Data Protection Law*, Martinus Nijhoff Publishers, p. 13.

[51] Son numerosos los ejemplos a este respecto. Desde la consolidación del consentimiento como base de legitimación para el tratamiento de datos personales (ver más abajo en este epígrafe), pasando por el desarrollo de la noción de autodeterminación informativa, que tanta importancia sigue cobrando aún en la actualidad, hasta, más recientemente, la innegable influencia alemana en la inclusión de la figura de Delegado de Protección de Datos en el Reglamento General de Protección de Datos.

[52] KOSTA, Eleni (2013): *Consent in European Data Protection Law*, Martinus Nijhoff Publishers, p. 35-36.

protección de datos personales en 1977, donde destacó la importancia concedida al consentimiento. La norma establecía la prohibición del tratamiento de datos personales salvo que se cumpliera alguna de las dos excepciones previstas: que existiera autorización legal o consentimiento del individuo. Así, la norma parece partir de una aproximación restrictiva al tratamiento de datos personales, si bien adquiere una gran flexibilidad al abrirlo a la voluntad del individuo a través de la prestación del consentimiento.[53]

FRANCIA. A finales de la década, concretamente en 1978, Francia también promulgó su primera normal nacional ad hoc en la materia. Destaca de ella la alusión a los riesgos derivados del uso de la informática. Asimismo, la norma menciona la necesaria protección de las libertades de los individuos (sin referirse expresamente los datos personales) y muestra preocupación por el impacto que el uso de la informática pudiera tener sobre la dignidad de la persona al reducir el significado de una persona a números procesados de manera automatizada. Por último, también destaca que esta fue la primera norma en otorgarle gran importancia a la creación de un elenco de derechos para los individuos.[54]

Otros Estados miembros promulgaron también sus leyes de protección de datos a finales de la década de los 70. Sin embargo, la norma francesa puede considerarse entre las últimas normativas pioneras en materia de protección de datos.[55]

La década se cierra con la Resolución del Parlamento Europeo de 1979 sobre la tutela de los derechos del individuo frente al creciente progreso técnico en el sector de la informática.

[53] GONZÁLEZ FUSTER, Gloria (2014): *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, Vol. 16, 1ª ed., Springer International Publishing, p. 60.

[54] GONZÁLEZ FUSTER, Gloria (2014): *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, Vol. 16, 1ª ed., Springer International Publishing, p. 70.

[55] AUSLOOS, Jeff (2018): *The Right to Erasure in EU Data Protection Law*, Oxford University Press.

En conclusión, si los años 60 supusieron la explosión de la computación, a pesar de que la dificultad de explotar las bases de datos hacía que la labor quedara restringida únicamente a especialistas, los años 70 supusieron el auge de la informática a nivel de usuario final por la facilidad de realizar consultas y obtener información en las bases de datos. En consonancia con este contexto, la década de los 70 trajo consigo la consolidación legislativa de la protección de datos personales. Por un lado, estas normas mantuvieron desde el inicio una mirada al pasado y a la memoria de los abusos que las tecnologías habían permitido en décadas anteriores. Por otro lado, las normas fueron posando también una mirada al futuro y a la prevención de posibles riesgos que el desarrollo pudiera atraer. Asimismo, destaca que, si bien en un primer momento únicamente se reguló la protección de datos como un límite frente al poder público, pronto se constató que los agentes privados también debían ser limitados.

6. Los años 80

6.1. Tecnología: agilización de consultas complejas

Estrechamente ligado a las bases de datos relacionales se encuentran los llamados sistemas gestores de bases de datos (DBMS por sus siglas en inglés o “database management system”), surgidos en la década de los 70, pero no popularizados hasta los años 80. Se trata de programas informáticos que interactúa con el usuario y múltiples bases de datos, de las que cada una puede estar a su vez compuesta por múltiples tablas. Este gestor permite crear una base de datos, gestionarla, almacenar, buscar y modificar datos, así como realizar *queries* de forma sencilla y estructurada, de modo que cualquier usuario puede realizar operaciones complejas sin necesidad de tener conocimientos técnicos avanzados.[56] Asimismo, también permiten dar acceso a los datos para los que cada

[56] GRAD, Burton; BERGIN, Thomas J. (2009): “History of Database Management Systems”, en *IEEE Annals of the History of Computing*, Vol. 31, No. 3, p. 3-5.

usuario haya sido autorizado.[57] Estos sistemas gestores de bases de datos permiten, además, estructurar las relaciones entre las diferentes tablas y elementos de las bases de datos.

En sus inicios, los gestores de bases de datos eran costosos y difíciles de utilizar[58] de modo que no fue hasta los años 1980 cuando comenzaron a ganar mayor popularidad, debido auge de la comercialización de los ya aludidos modelos de bases de datos relacionales, que facilitaban y flexibilizaban el uso de las bases de datos. Este fue precisamente uno de los factores que contribuyeron al establecimiento de grandes bases de datos compartidas entre departamentos dentro de una organización o entre sistemas diferentes.[59]

Volviendo al ejemplo anterior, si utilizamos la *query* "SELECT Código_del_paciente FROM Pacientes WHERE Edad > 45" para realizar una consulta sobre nuestra base de datos, obtendremos una lista completa de pacientes cuya edad supera los 45 años. Esta operación arroja un resultado rápido y de manera sencilla. De hecho, recordemos que la sencillez en la realización de consultas era una de las mayores ventajas de los sistemas relacionales. Sin embargo, esta simplicidad también puede resultar en inconvenientes. Imaginemos que en queremos analizar información en una gran base de datos, como puede ser la de un conjunto de hospitales, donde hay miles de médicos, decenas de miles de pacientes y millones de visitas. En ese caso, los resultados de la consulta serán una larga lista de pacientes que cumplen la condición de edad mayor de 45 años. Entre tantos resultados, nuestra capacidad analítica queda limitada, no somos capaces de darle más valor a ese resultado de datos.

---

[57] HAIGH, Thomas (2009): "How Data Got its Base: Information Storage Software in the 1950s and 1960s", en *IEEE Annals of the History of Computing*, Vol. 31, No. 3, p. 7.

[58] BERGIN, Thomas J.; HAIGH, Thomas (2009): "The Commercialization of Database Management Systems, 1969–1983", en *IEEE Annals of the History of Computing*, Vol. 31, No. 3, p. 32.

[59] BERGIN, Thomas J.; HAIGH, Thomas (2009): "The Commercialization of Database Management Systems, 1969–1983", en *IEEE Annals of the History of Computing*, Vol. 31, No. 3, p. 38.

De modo similar, imaginemos que deseamos realizar consultas más complejas como "¿Cuántos pacientes de más de 45 años han sido diagnosticados de gripe en el Centro de salud con código U508E en el último mes?". Esta consulta podría hacerse mediante *queries* SQL, pero sería compleja y lenta debido a que sería necesario recurrir a varias operaciones subsecuentes a partir de datos de diversas tablas, uniones y múltiples operaciones.

Este problema puede solucionarse ordenando las tablas y sus relaciones de manera diferente, creando una base de datos multidimensional. Para ello, se agregan tablas y se crean cubos de resultados, de manera que obtener los mismos resultados requiere un poder de computación mucho menor.[60] De este modo, el modelo de organización en cubos, que parten de bases de datos multidimensionales, no es sino una evolución de las bases de datos de dos dimensiones, típicas, por ejemplo, de las hojas de cálculo. Esta técnica se denomina OLAP ("*online analytical processing*") o procesamiento analítico en línea y permite agilizar la consulta de cantidades de datos cada vez mayores.

En realidad, los cubos representan resultados de *queries* pre-calculados y almacenados. Es decir, cada parte del cubo es un resultado de una consulta específica realizada sobre el esquema de estrella que contiene todas las dimensiones, medidas y jerarquías elegidas. Puesto que están pre-calculados, el modelo OLAP consume más capacidad de memoria del sistema, pero permite acceder a resultados complejos de forma inmediata.[61] Por ejemplo, con un modelo OLAP podríamos analizar todos los pacientes del sistema en función del diagnóstico que recibieron, el médico que les atendió, la fecha de visita o el centro al que acudieron. De forma similar, también se pueden analizar las ventas de una organización

[60] HAMEL, Lutz; HALL, Tyler (2005): "A brief tutorial on Database Queries, Data Mining, and OLAP" en *The Encyclopedia of Data Warehousing and Mining*, Vol. 401, p. 8.

[61] JENSEN, Michael R.; MOLLER, Thomas H.; PEDERSEN, Torben B. (2001): "Specifying OLAP cubes on XML data", en *Journal of Intelligent Information Systems*, Vol. 17, No. 2-3, p. 256.

por mes, por tienda, por producto, por vendedor, etc. Es decir, el modelo permite observar múltiples variables desde múltiples perspectivas.

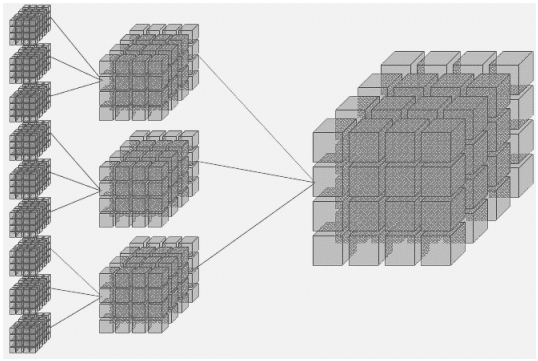

Gráfico 2: Cubo OLAP. Fuente: https://apandre.wordpress.com/data/datacube/.

Sobre los cubos también se pueden llevar a cabo operaciones de aumento o disminución para cambiar la granularidad de los datos que son examinados. En términos sencillos, sería algo similar a realizar *zoom* sobre la información de modo que pudiéramos ver el mismo dato con mayor o menor precisión. Por ejemplo, para examinar el número de ventas por unidad de tiempo, el cubo tendría los resultados pre-calculados en función de medidas jerárquicas diferentes: horas, días, mes, trimestre o año. Si la unidad que queremos observar es el punto de venta o tienda, estas podrían mostrarse por tienda específica, por código postal, por región, país o continente. De este modo, los modelos OLAP permiten analizar la base de datos de manera interactiva. Sin un modelo OLAP, obtener estas medidas sería lento ya que habría que realizar una *query* para cada una de las consultas deseadas. De este modo, multitud de consultas se encuentran calculadas y organizadas de manera sencilla y accesible. Esto supone una gran mejora en la capacidad de examinar los datos disponibles que ayuda a la toma de decisiones.

El problema de los modelos OLAP es que obligan a pre-seleccionar qué datos y consultas queremos construir, de modo que sacrifica en gran medida la flexibilidad. Asimismo, requiere encontrar un equilibrio entre el

número de datos y dimensiones que se incluyen en el cubo. Demasiados datos pueden resultar inmanejables para el usuario del sistema, pero pocos datos resultarían irrelevantes para obtener información de valor. Además, los modelos OLAP más utilizados únicamente analizan datos numéricos estructurados, pero no son válidos para otros formatos de datos más complejos como el texto.[62]

En conclusión, los modelos OLAP permiten reorganizar una base de datos relacional de un modo que permite que un número amplio pero limitado de consultas sea pre-calculado para analizar los datos de manera eficiente e interactiva sin necesidad de realizar consultas que serían complejas y conllevarían un consiguiente coste de tiempo.

6.2. Derecho: internacionalización de la protección de datos

Si tal y como veíamos la década de los 70 marcó el inicio de las primeras legislaciones sobre protección de datos en diferentes Estados europeos, los años 80 supusieron "un respaldo definitivo"[63] a la consolidación de la protección de los datos personales a nivel trasfronterizo, al tiempo que trajeron un cambio de mentalidad muy relevante. Dos hechos concretos marcaron un hito en esta senda.

6.2.1. Directrices de la OCDE

En primer lugar, la Organización para la Cooperación y el Desarrollo Económicos (OCDE) publicó en 1980 sus Directrices sobre protección de la privacidad y flujos transfronterizos de datos personales,[64] sobre las que un grupo de expertos creado con este fin ya llevaba años trabajando. Este documento ya muestra una clara diferencia con los textos anteriores, por

[62] RAVAT, Franck; TESTE, Olivier; TOURNIER, Ronan (2007): "OLAP aggregation function for textual data warehouse", en *ICEIS*, Vol. 1, p. 1.

[63] PIÑAR MAÑAS, José Luís (2005): "El derecho fundamental a la protección de datos personales. Algunos retos de presente y futuro", en *Asamblea: revista parlamentaria de la Asamblea de Madrid*, No. 13, págs. 21-46.

[64] ORGANIZACIÓN PARA LA COOPERACIÓN Y EL DESARROLLO ECONÓMICOS (1980): *Directrices sobre protección de la privacidad y flujos transfronterizos de datos personales* de 23 de septiembre.

cuanto, además de la protección de los derechos individuales, defiende los beneficios de la libre circulación de datos personales. Es decir, parece que por primera vez un texto de carácter jurídico reconoce el valor socioeconómico de la utilización de los datos en el comercio internacional sin renunciar al interés común de la protección del individuo.

En la memoria que acompaña Las Directrices, el grupo destaca expresamente cuestiones que en los años anteriores se habían ido haciendo palpables: la obligación de que aquellos que van a hacer uso de los datos personales informen apropiadamente al público general, la importancia de los derechos de los individuos y, muy especialmente, los problemas legales de los procesos automáticos de datos. Ya en los 80 se mostraba preocupación por la cada vez mayor adopción de los ordenadores y la capacidad de almacenar, comparar, enlazar, seleccionar y acceder a los datos personales. Resulta incluso gracioso leer cómo el grupo mencionaba uso “ubicuo” de los ordenadores, pues en ese momento pocos podrían haber imaginado que tan solo unos años después prácticamente cualquier persona de cualquier región del mundo tendría un ordenador en el bolsillo y siguiéramos refiriéndonos, con algo más de motivo, a la ubicuidad, no solo de los ordenadores, si no ya de sensores. Y a pesar de ello, parece seguro que dentro de unos pocos años lo que hoy consideramos tan generalizado habrá quedado minimizado frente a la adopción tecnológica que nos espera.

Las Directrices aportaron un conjunto de principios básicos relativos a las actividades para tratar datos y de estos, nos detendremos a examinar el principio séptimo.

El apartado 7, titulado Principio de limitación de la recogida indica:

> “7. Debería haber límites a la recogida de datos personales y cualquiera de esos datos debería ser obtenido por medios legales y honestos y, en su caso, con el conocimiento o consentimiento del sujeto de los datos” (énfasis añadido).

Lo primero que llama la atención es la referencia al consentimiento del individuo como límite básico. Así, parece que tanto las normas nacionales desarrolladas en los años 70 como los principios que se consolidaban en los años 80 giraban sobre la importancia otorgada a la voluntad de la persona. Sin embargo, es necesario realizar más apreciaciones.

En primer lugar, debe recalcarse expresamente el uso de la partícula "o", que demuestra que, si bien el consentimiento se menciona como una garantía básica para los individuos, no tuvo nunca un carácter de unicidad. De hecho, el propio grupo de expertos detalla que "El conocimiento o consentimiento del sujeto de los datos es una regla fundamental, siendo el conocimiento el requisito mínimo. Por otra parte, no siempre se puede imponer el consentimiento, y ello por razones prácticas".[65] En el mismo sentido debe interpretarse la referencia a que el individuo debe conocer o consentir "en su caso". Es decir, determinadas situaciones podrían justificar que el sujeto no debiera conocer o consentir que sus datos están siendo objeto de tratamiento.

Por su parte, las directrices también incluyen como principio décimo la limitación de uso. Este principio implica que los datos personales no podrán utilizarse para fines diferentes de aquellos que se hayan previamente especificados. Esta regla general cuenta sin embargo con dos excepciones: el consentimiento del sujeto o la obligación de una norma legal.

6.2.2. *Convenio Nº 108*

En 1981, tan solo un año más tarde que las Directrices de la OCDE, el Consejo de Europa publicó el Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, más comúnmente conocido como Convenio 108.[66] Se trata por fin del

[65] Memoria explicativa de las Directrices, apartado 52.

[66] CONSEJO DE EUROPA (1981): Convenio 108, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal.

primer documento jurídicamente vinculante a nivel internacional que utiliza el término “protección de datos”.[67]

El origen de este documento puede verse en la constatación de que el art. 8 de la Convención Europea de Derechos Humanos de 1950 parecía no ser suficiente para garantizar la protección de los individuos frente al desarrollo tecnológico, pues, por ejemplo, únicamente era aplicable a las autoridades públicas, mientras que el tratamiento de datos por parte de entes privados no estaba sujeto a escrutinio.[68] Es decir, este Convenio refleja ya la perspectiva de la época por la que informática y protección del individuo eran intereses en conflicto.

Este documento no contiene una manifestación sobre la necesidad de encontrar un equilibrio entre el valor económico del flujo de los datos y la defensa de los individuos, sino que su finalidad primordial es únicamente la protección de los derechos y libertades fundamentales de la persona (art. 1).[69]

Por otro lado, el Convenio alude al principio de licitud y lealtad aunque sin desarrollarlo. Esto es, no contiene especificaciones sobre cuáles puedan ser las bases que legitimen el tratamiento de datos personales ni realiza mención al consentimiento, sino que se limita a dejar la cuestión abierta.

El Convenio 108 ha continuado siendo un instrumento de enorme influencia hasta nuestros días, aunque los desarrollos tecnológicos, sociales y legislativos de las décadas posteriores culminaron con la publicación de una versión renovada del Convenio en 2018.[70]

---

[67] GONZÁLEZ FUSTER, Gloria (2014): *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, Vol. 16, 1ª ed., Springer International Publishing, p. 254.

[68] AUSLOOS, Jeff (2018): *The Right to Erasure in EU Data Protection Law*, Oxford University Press.

[69] AUSLOOS, Jeff (2018): *The Right to Erasure in EU Data Protection Law*, Oxford University Press.

[70]CONSEJO DE EUROPA (2018): *“Convenio 108” modernizado de 17 de 2018 para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal*.

7. Los años 90

7.1. Tecnología: inteligencia de negocio y minería de datos

A finales de los años 80 y principios de los 90, el modelo relacional de bases de datos y el lenguaje estandarizado SQL desarrollado para este modelo relacional dominaban los sistemas gestores de bases de datos.

El siguiente paso en la ciencia de los datos fue la expansión de las técnicas de inteligencia empresarial o *business intelligence* (BI). Si bien este concepto había surgido unas décadas atrás, es a partir de este momento cuando se comienzan a desarrollar definiciones más cercanas al concepto actual del término. Tamar Gilad y Benjamin Gilad definían la inteligencia de negocio como una "revolución silenciosa" que estaba tomando fuerza en multitud de compañías a lo largo de Estados Unidos, a pesar de que su importancia aún no había sido vista en las escuelas de negocios.[71] Comprendían la inteligencia de negocio como el proceso de institucionalizar las actividades de inteligencia en las organizaciones, y lo definían como un compendio de cinco actividades: la recogida de los datos, la evaluación de su validez o confiabilidad, el análisis, el almacenamiento de los datos y la inteligencia y la difusión.[72]

En 1989 Howard Dresner propuso una definición de inteligencia empresarial como "los conceptos y métodos usados para mejorar la toma de decisiones de negocio mediante el uso de sistemas basados en datos reales".[73]

En otras palabras, la inteligencia de negocio se concreta ya como el conjunto de actividades que persiguen organizar y explotar los datos brutos

[71] GILAD, Tamar; GILAD, Benjamin (1986): "SMR Forum, Business Intelligence – The quiet revolution", en *Sloan Management Review*, Vol. 27, No. 4, p. 53.

[72] Esta diferenciación de la inteligencia de negocio es enormemente interesante, por cuanto este trabajo realiza una definición de las tecnologías big data como un proceso de varias fases, con similitudes con las que aquí se señalan.

[73] POWER, Daniel J. (2007): *A brief history of decision Support Systems*, Vol. 4.1, DSS Resources.

o históricos de la empresa para tomar mejores decisiones y aumentar la competitividad de la organización.[74]

La fuente de la inteligencia de negocio son los datos que la empresa genera en sus actividades diarias (datos transaccionales u operacionales), que conforman una "mina" o "yacimiento" de datos, y que normalmente están almacenados en las grandes bases de datos corporativas,[75] los denominados *datawarehouses* o *datamarts*. El término *datawarehouse* o almacén de datos, fue acuñado en la década de los 1970 para referirse a servidores localizados *in situ*, en las instalaciones de la organización. De este modo, el almacenamiento de datos en un único lugar, el *datawarehouse,* ayudó a reducir drásticamente el tiempo requerido para acceder a la información en comparación con el almacenamiento de datos en múltiples sistemas o que funcionan como silos inconexos en la organización.

Gracias a la creación de estos repositorios únicos, el crecimiento de la cantidad de datos disponible en esta década hizo necesario apoyarse en herramientas informáticas y métodos automatizados más potente para analizar estas minas de datos y extraer la inteligencia contenida en ellos. Estas técnicas son las que constituyen la denominada minería de datos (o *data mining* en inglés). Se trata de técnicas derivadas de la estadística y la computación encaminadas a analizar grandes cantidades de datos de manera automática o semiautomática para descubrir conocimientos ocultos en los datos.[76] Estos conocimientos pueden ser patrones de comportamiento, tendencias en los datos, registros poco usuales o

[74] EVELSON, Boris; NICHOLSON, Norman, (2008): *Topic overview: business intelligence*, Forrester.

[75] El adjetivo “grande” utilizado en diversas ocasiones a lo largo del capítulo es subjetivo, flexible y variante en función de la capacidad media general de almacenamiento de cada período histórico. A modo de ejemplo, en la actualidad no se debate que los teléfonos móviles modernos tienen mayor capacidad de almacenamiento que los primeros almacenes de datos. En la actualidad, los almacenes de datos han evolucionado y se gestionan, en un número creciente de casos, desde la nube (a través de internet).

[76] HAND, David J. (2007): “Principles of data mining”, en *Drug Safety*, Vol. 30, No. 7, p. 621.

anómalos, etc., que no se pueden detectar mediante la explotación tradicional de los datos porque las relaciones son demasiado complejas o porque hay demasiado volumen de datos que analizar. Con ello se consigue hacer una radiografía de los datos que permita saber de forma detallada lo que ocurre en la organización.

Un famoso mito de descubrimiento de asociaciones en los datos a través del uso de la minería de datos es la historia de las cervezas y los pañales.[77] Gracias al análisis de los tickets de compra de los clientes en sus establecimientos, una cadena de venta minorista en supermercados observó que los viernes por la tarde se vendían un mayor número de paquetes de pañales y de cerveza de forma conjunta, una combinación de artículos que no parece obvia.

La minería de datos permitió analizar la combinación de productos que los clientes compraban cada día de la semana. El proceso sería algo similar a analizar los siguientes datos:

PRODUCTOS EN LA CESTA DE LA COMPRA
{**Cerveza**, pan, **pañales**}
{**Cerveza**, refresco, **pañales**, leche}
{**Cerveza**, pan, **pañales**, tomates}
Etc.

→

Regla de asociación descubierta:
{**cerveza**} - {**pañales**}

Gráfico 3: Proceso de minería de datos. Fuente: Elaboración propia.

Está analítica permitió descubrir un patrón de comportamiento muy difícilmente observable a simple vista entre las grandes cantidades de

[77] GORUNESCU, Florin (2011): *Data Mining: Concepts, models and techniques*, Springer Science & Business Media.

información y comprobar que dicho patrón se repetía en todos sus establecimientos. El motivo de ello era que esos días había más padres de familia jóvenes que hacían la compra, que pasaban el fin de semana en casa con la familia y viendo la televisión tomando una cerveza. Este conocimiento permitió adaptar el orden de los productos en el supermercado y así, en lugar de colocar la cerveza junto a otros refrescos, colocarla junto a los pañales, producto con el que tenía una mayor relación de consumo. El aumento de las ventas de ambos productos confirmó el hallazgo de esta asociación de productos, que de otra forma no se habría descubierto.

De este modo, ¿qué diferencia hay entre realizar una consulta o *query* a una base de datos y hacer minería de datos? Es cierto que son conceptos cercanos, y muy relacionados, pero en todo caso presentan diferencias sustanciales.[78]

Lanzar una *query* o consulta contra una base de datos permite rescatar datos contenidos en la base de datos relacional que cumplan con los criterios de búsqueda. Esto puede ser, como en nuestro ejemplo anterior, recuperar los datos de todos aquellos pacientes mayores de 45 años. También podría ser obtener todos los clientes de nuestro supermercado que en el último mes hayan realizado un gasto mayor de 100 € en una sola compra ordenados de mayor a menor volumen de gasto. De este modo, la consulta actúa como un filtro que se aplica a los datos.

Sin embargo, si partimos de una base de datos con una gran cantidad de entradas, los resultados que se obtienen al realizar estas consultas pueden ser muy numerosos, de modo que la cantidad de resultados es excesiva para poder operar con ella. Los resultados obtenidos no nos permiten conocer muchos más detalles que el hecho de que tenemos un elevado número de pacientes mayores de 45 años, o de que una gran cantidad de clientes realizan compras de más de 100 €. En este caso, el insumo del

[78] HAMEL, Lutz; HALL, Tyler (2005): “A brief tutorial on Database Queries, Data Mining, and OLAP” en *The Encyclopedia of Data Warehousing and Mining*, Vol. 401, p. 5.

sistema es la consulta o especificaciones, lo que requiere tener una idea previa de qué tipo de conocimiento se desea encontrar, y el resultado son los datos filtrados que cumplen con dichas especificaciones.

La minería de datos, por su parte, implica un análisis de datos más profundo. El insumo es la base de datos en su conjunto, sin necesidad de tener una idea preconcebida que implique insertar un filtro, y el resultado es un modelo o patrón de comportamiento de las variables, cuyo conocimiento es más valioso que el conjunto de los datos en bruto, pues el modelo ayuda a comprender y otorgar significado a los datos.[79] Por ejemplo, el resultado de ejecutar técnicas de minería de datos sobre nuestra base de datos podría mostrarnos que los pacientes de más de 45 años acuden al médico especialista una media de dos veces al año, o que el perfil más probable de cliente que gasta más de 100 € en cada compra es hombre y residente en un determinado código postal. Este conocimiento es enormemente valioso en una organización, y permite obtener reglas de negocio que agrupen cientos o incluso miles de entradas de nuestra base de datos bajo una simple premisa.

En conclusión, los conceptos de *query* y minería de datos son diferentes. La diferencia reside en que, al realizar una *query,* el resultado obtenido es un listado de los datos que cumplen la condición de la consulta, es decir, una parte de la totalidad de datos brutos que teníamos originariamente, pero en todo caso los datos obtenidos no han sido modificados, sino que siguen en bruto. Por su parte, la minería de datos no devuelve los datos brutos que cumplen ciertas características, sino que devuelve un modelo o patrón de comportamiento que se ha detectado en los datos[80] y por lo tanto genera nuevo conocimiento.

Estos datos sí son comprensibles y ayudan a la toma de decisiones informadas, porque crean un contexto y dan sentido a miles de entradas

[79] BERRY, Michael J. A.; LINOFF, Gordon S. (2004): *Data Mining Techniques: For Marketing, Sales, and Customer Relationship Management*, John Wiley & Sons.

[80] HAMEL, Lutz; HALL, Tyler (2005): “A brief tutorial on Database Queries, Data Mining, and OLAP” en *The Encyclopedia of Data Warehousing and Mining*, Vol. 401, p. 5.

de una o varias bases de datos. Es decir, mientras realizando *queries* obtenemos como resultado los mismos datos brutos filtrados, realizando minería de datos, el resultado es un modelo de los datos.[81]

Por otro lado, tradicionalmente se ha considerado que la minería de datos implica realizar un tratamiento secundario de datos que fueron recogidos para otra finalidad.[82] Por ejemplo, en nuestro ejemplo de las relaciones entre las ventas de cerveza y pañales en un supermercado, los datos se recogieron inicialmente para realizar el cobro de la cesta de la compra de los clientes, y solo en un momento posterior se analizaron en búsqueda de posibles correlaciones y patrones.

Decidir cuándo un patrón de comportamiento es relevante o interesante para el objeto de estudio o la toma de decisiones dependerá del contexto. En este sentido, el conocimiento experto ayudará a poder comprender qué están describiendo los datos. Para esto es necesario saber si las correlaciones se deben a una causa real o a mera coincidencia.

Sin embargo, en entornos cada vez más complejos que analizan más cantidad de datos, también un ojo experto puede quedar sobrepasado por el modelo. Aquí se torna especialmente complicado poder determinar si las relaciones encontradas en los datos tienen significatividad.

Por otro lado, la década de los noventa trajo consigo los inicios de la "World Wide Web", o internet tal y como lo conocemos en la actualidad,[83] aunque esta tecnología no se popularizó hasta 1995. Gracias a internet, cualquier persona puede acceder a la red y a datos cargados por otras personas, o cargar sus propios datos.

---

[81] HAMEL, Lutz; HALL, Tyler (2005): "A brief tutorial on Database Queries, Data Mining, and OLAP" en *The Encyclopedia of Data Warehousing and Mining*, Vol. 401, p. 7.

[82] HAND, David J. (2007): "Principles of data mining", en *Drug Safety*, Vol. 30, No. 7, p. 621.

[83] En realidad, la creación de internet puede retrotraerse a las décadas previas durante la Guerra Fría, con las primeras conexiones entre ordenadores de una red descentralizada hasta la creación de los protocolos utilizados por el Departamento de Defensa de Estados Unidos en los años 80.

Una vez más, la gran cantidad de información disponible creó un problema de gestión de los datos, así como un aumento del coste de almacenamiento. Efectivamente, muchas empresas veían como cada vez era más difícil acceder a los datos que necesitaban para responder a sus consultas, y cuando los empleados de una organización necesitaban acceder a la información debían recurrir al departamento informático o de sistemas, debido a la dificultad de gestionar el acceso a tanta información.

Así fue como en 1997, los investigadores de la NASA Michael Cox y David Ellsworth utilizaron por primera vez el término "big data" en un artículo científico. En este se afirmaba que el ritmo de crecimiento de los datos comenzaba a ser un problema para los sistemas informáticos.[84]

En su artículo, los autores diferenciaban entre dos perspectivas del big data: las compilaciones o repertorios y los objetos ("*big data collections*" y "*big data objects*").

En primer lugar, Cox y Ellsworth definen big data como compilación como compendio o unión de diversas cosas. En estos términos, big data implica la agregación de múltiples ficheros de datos, provenientes de fuentes múltiples, distribuidas en diversas localizaciones físicas y en diferentes tipos de bases de datos o repositorios. La cantidad de los datos excedería la capacidad de almacenamiento de modo que los datos se particionan, de forma que cada partición es fácilmente manejable.[85] Sin embargo, el manejo de la base de datos big data seguiría siendo compleja. Así por ejemplo, para poder obtener utilidad de los datos, un científico de datos debe consultar bases de datos diversas, cada una de las cuales requiere accesos diferenciados.

---

[84] COX, Michael; ELLSWORTH, David (1997): "Managing Big Data for Scientific Visualization", en *ACM Siggraph*, Vol. 97, p. 21-38.

[85] En concreto, los autores ilustran la importancia del concepto como unión o agregado mediando el eso gran cantidad de adjetivos precedidos por el prefijo "multi": *"[B]ig data collections are aggregates of many data sets. Typically the data sets are multi-source, are often multi-disciplinary, are generally distributed among multiple physical sites, and are often multi-database (that is, they are stored in disparate types of data repositories)*". COX, Michael; ELLSWORTH, David (1997): "Managing Big Data for Scientific Visualization", en *ACM Siggraph*, Vol. 97, p. 22.

En segundo lugar, Cox y Ellsworth definen objetos big data como aquellos conjuntos de datos demasiado grandes para ser tratados mediante algoritmos, software o a través de equipos tradicionalmente disponibles. En concreto, el tamaño de los datos debería ser mayor que los más grandes equipos disponibles en el mercado (o incluso, añaden, que los superordenadores más potentes de la época). Incluso conjuntos de datos pequeños serían sustancialmente mayores que aquellos capaces de ser manejados por los equipos a los que un ingeniero o científico "típico" tendrían acceso.[86] Todo ello provocaba claros problemas para la gestión de los datos.

Ese mismo año, Cox y Ellsworth desarrollaron en mayor profundidad los problemas que generaba el big data sobre la visualización de datos derivado de las dificultades del almacenamiento de dicho volumen de datos. El artículo comienza reconociendo que la visualización de datos supone un gran reto para los sistemas de computación debido a que los ficheros de datos son cada vez más grandes, creando dificultades para el almacenamiento de datos, ya sea en la memoria, disco local o incluso en remoto. "Llamamos a esto el problema del big data". [87]

En este momento, ya se podían discernir algunas de las características que definían el big data: gran volumen, fuentes y tipos de bases de datos diversas, localizaciones variadas, dificultad de visualización. De entre ellas, resalta notablemente la importancia dada al gran volumen o cantidad de datos. Una vez más, la creciente complejidad de la gestión de los datos hacía que fuera necesaria la ayuda de expertos en tecnologías de la información para poder extraer información relevante de los datos primarios. Del mismo modo, una vez más, el foco comenzó a ser puesto en modos de hacer la tecnología más accesible a los usuarios finales de la

[86] COX, Michael; ELLSWORTH, David (1997): "Managing Big Data for Scientific Visualization", en *ACM Siggraph*, Vol. 97, p.23.

[87] COX, Michael; ELLSWORTH, David (1997): "Application-controlled demand paging for out-of-core visualization", en *Proceedings of the 8th Visualization '97 Conference, IEEE*, p. 235-244.

información, un proceso que no obstante nunca es rápido. La conectividad que trajo el desarrollo de internet y la mayor fuerza competitiva de los actores de mercado hacía cada vez más necesario poder reducir el tiempo de la toma de decisiones. Esto desencadenó en la cada vez mayor urgencia para disponer de la información en tiempo (cuasi) real.

7.2. Derecho

En paralelo a esta evolución tecnológica, la década de los 90 fue crucial en el desarrollo del derecho de protección de datos personales en el continente europeo. Los Estados miembros habían continuado promulgando leyes nacionales, lo que con el tiempo creó un mosaico de regulaciones diferentes que llevó a la comprensión de que el desarrollo del mercado interior comunitario se vería beneficiado de mayor homogeneidad.

7.2.1. *Ley Orgánica de Regulación del Tratamiento Automatizado de Datos (LORTAD)*

Uno de los Estados miembros que promulgó su norma nacional de protección de datos personales fue España, que por medio de Ley Orgánica de regulación del tratamiento automatizado de datos de carácter personal (LORTAD),[88] en 1992 se propuso “limitar el uso de la informática y otras técnicas y medios de tratamiento automatizado de los datos de carácter personal para garantizar el honor, la intimidad personal y familiar de las personas físicas y el pleno ejercicio de sus derechos”. La norma, en coherencia con el art. 18.4 de la Constitución (1978) refleja una vez más la tensión entre el desarrollo técnico y la protección del individuo. Por otro lado, la norma española sienta las bases de uno de los modelos europeos que mayores garantías ofrece a las personas.[89]

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

[89] PIÑAR MAÑAS, José Luís; GIL, Álvaro Canales (2011): *Legislación de protección de datos*, 2ª ed., Madrid, Iustel, p. 39.

La ley fue actualizada de nuevo a través de Ley Orgánica en 1999[90] para adaptarse a lo dispuesto en la primera Directiva europea de protección de datos, que comentamos en las próximas líneas.

7.2.2. *Directiva de Protección de Datos*

Ya desde 1990 la Comisión Europea inició el procedimiento legislativo que condujo a la promulgación de la Directiva de protección de datos en 1995.[91] Esta nació con dos objetivos principales. En primer lugar, garantizar la protección de las libertades y de los derechos fundamentales de las personas físicas, y, en particular, del derecho a la intimidad, en lo que respecta al tratamiento de los datos personales.[92] En segundo lugar, la libre circulación de datos personales entre los Estados miembros. Ello comienza a reflejar cómo en la construcción del debate en torno a la protección de los datos personales el funcionamiento de la economía, la globalización y el valor económico de los flujos de datos se convierten en factores a tomar en consideración.[93] En efecto, el desarrollo del mercado único europeo hacía necesaria la circulación de datos en el área. En palabras de Gloria González Fuster, la inclusión de ambos objetivos en el primer artículo de la Directiva refuerza la importancia de ambos, pero también su carácter de valores rivales.[94]

---

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

[91] 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.

[92] Aunque el nexo legal directo del derecho a la protección de datos sea el derecho a la privacidad y la intimidad de las personas, Piñar Mañas recuerdo que surge también de la propia dignidad de la persona, de lo que se deriva su importancia trascendental. PIÑAR MAÑAS, José Luís (2005): "El derecho fundamental a la protección de datos personales. Algunos retos de presente y futuro", en Asamblea: revista parlamentaria de la Asamblea de Madrid, No. 13, págs. 21-46.

[93] PIÑAR MAÑAS, José Luís (2005): "El derecho fundamental a la protección de datos personales. Algunos retos de presente y futuro", en *Asamblea: revista parlamentaria de la Asamblea de Madrid*, No. 13, págs. 21-46.

[94] GONZÁLEZ FUSTER, Gloria (2014): *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, Vol. 16, 1ª ed., Springer International Publishing, p. 130.

Sin embargo, la intención de conseguir un equilibrio entre ambos objetivos muestra la idea subyacente de que es posible considerar las tecnologías de una manera más positiva, aceptando la importancia de la informática en la sociedad. La tecnología no ha de ser vista únicamente como un riesgo para los derechos del individuo y por ello, los beneficios que puedan originarse del tratamiento de los datos y su circulación son también considerados.

La regulación a través de la figura de Directiva tenía como objetivo hacer que el nivel de protección de los derechos y libertades de las personas fuera equivalente entre los Estados miembros, en vista de las grandes diferencias existentes hasta ese momento entre las legislaciones nacionales de cada uno de ellos. Dicho objetivo armonizador se reflejó en la creación de principios y normas que debían servir de marco para el posterior desarrollo de normas nacionales. De hecho, esta armonización y mutua garantía de que los datos de los ciudadanos de cualquier Estado miembro gozarían del mismo nivel protección en el resto de Estados fue la premisa sobre la que se aceptó el principio de libre circulación de datos personales y la flexibilización de las limitaciones previas a las transferencias de datos entre Estados miembros. Gracias a ello, la evolución de la economía digital y el desarrollo tecnológico de las décadas posteriores pudo realizarse en un entorno de confianza mutua.

Entre los aspectos a resaltar de la Directiva se encuentra el foco en los derechos de los interesados. Asimismo, la Directiva incluye, junto con el consentimiento, un listado cerrado de bases de legitimación del tratamiento. Es decir, la Directiva recoge el testigo de documentos previos que ya introducían expresamente la importancia del consentimiento y de la expresión de la voluntad del individuo. Pero recordemos, como ya vimos en epígrafes anteriores, el consentimiento no se reflejaba como el único medio por el que se podría legitimar el tratamiento de datos personales de un individuo. De este modo, el art. 7 de la Directiva establece que el tratamiento será legítimo cuando exista alguna de las bases allí expresadas, entre las que se cuentan el consentimiento inequívoco del

interesado, la necesidad para la celebración o ejecución de un contrato con este, el cumplimiento de una obligación legal o la realización de un interés legítimo de una persona siempre que no prevalezcan los intereses o los derechos y libertades del interesado.

La Directiva tuvo realmente un papel relevante en la inspiración de las normas nacionales de protección de datos que fueron promulgando los Estados miembros en los siguientes años. A este mismo fin servían las opiniones y directrices sobre multitud de temas publicadas a lo largo de los años por el llamado Grupo de Trabajo del Artículo 29,[95] órgano consultivo creado por la Directiva y formado por representantes de las autoridades de control de cada Estado miembro, el Supervisor Europeo de Protección de Datos y la Comisión Europea.

Si bien es cierto que la Directiva creó un marco común de normas de protección de datos, el tiempo demostró que la elección de la figura de la Directiva no terminó por cristalizar en el nivel de homogeneidad deseado. En la práctica, los responsables del tratamiento se vieron ante la tesitura de cumplir con 28 normas nacionales diferentes. Este mosaico creó, con el paso de los años, inseguridad jurídica, fragmentación y costes, al tiempo que creaba niveles de protección diferentes para los interesados.

A modo ejemplificativo, Viviane Reding señalaba[96] el caso pasado de una empresa multinacional que había instaurado un sistema virtual de cartografía que permitía recabar imágenes de edificios públicos y privados, así como tomar fotografías de los viandantes sin su conocimiento. En un Estado miembro, esta práctica se consideró contraria a la normativa de protección de datos personales cuando las fotografías no desenfocaban a la persona (es decir, cuando la cara del interesado era nítida y constituía

[95] AUSLOOS, Jeff (2018): *The Right to Erasure in EU Data Protection Law*, Oxford University Press.

[96] REDING, Viviane (2012): "Protección de la privacidad en un mundo conectado. Un marco europeo de protección de datos para el siglo XXI", en Jorge Pérez y Enrique Badía (coords), *El debate de la privacidad y seguridad en la red: regulación y mercados,* Ariel/Telefónica, Madrid.

.

un dato personal), mientras que en otro Estado miembro la práctica no se consideró contraria a Derecho.

En todo caso, la Directiva de protección de datos fue un paso necesario, aunque no suficiente hacia una mayor homogeneización.

8. El inicio de los años 2000

8.1. Tecnología

Tras la irrupción de tecnologías que comenzaban a regirse bajo la definición amplia de big data, Doug Laney propuso en 2001 una definición de big data a partir de tres atributos, las llamadas “tres uves”: volumen, variedad y velocidad.[97] Laney defendía que el almacenamiento de datos en silos separados dificultaba la coherencia interna de los datos para todos los miembros de una organización, que no tenían acceso a una versión unificada de la realidad, sino a diferentes versiones de la misma realidad. En este artículo, Laney sugiere que volumen, velocidad y variedad son las tres dimensiones del reto de la gestión de los datos.

Más adelante nos pararemos a analizar cada una de estas "uves" de forma detallada para obtener una mejor comprensión de lo que son las tecnologías big data, haciendo en este momento una mera aproximación de lo expuesto por Laney.

El volumen hace referencia a la cantidad de datos que se procesan, y al hecho de que, por ejemplo, se haya convertido en normal hablar de terabytes o petabytes. La digitalización aumenta la cantidad de datos disponibles de cada transacción, aumentando de este modo la cantidad total de datos recopilados. Por otro lado, en la medida en que la información se convierte en un activo cada vez más valioso, las organizaciones son más reacias a su eliminación.

[97] LANEY, Doug (2001): *3D Data Management: Controlling Data Volume, Velocity and Variety*, META Group research note, Vol. 6, No. 70, p.1.

La velocidad se refiere a la capacidad de procesar los datos de forma rápida, en tiempo real o casi real, frente al llamando procesamiento en *batch* o por lotes. La digitalización también ha incrementado la velocidad de recogida de datos y de respuesta respecto de los nuevos datos.

Por último, la variedad se refiere a la diversidad de orígenes de los datos. Si bien en décadas anteriores los datos debían tener un formato de tabla para ser analizados (es decir, ser datos estructurados), las tecnologías big data permiten procesar datos no estructurados o datos provenientes de fuentes muy diversas, lo que provoca que tengan estructuras diferentes.[98] Precisamente la variedad de los datos es, según Laney, el mayor escollo para la gestión de los datos. La gran diversidad de formatos de los datos, la combinación de datos con diferentes estructuras o, incluso la cada vez mayor cantidad de datos no estructurados, así como la inconsistencia semántica crean retos. Esto es relevante porque, de hecho, el 43% de las organizaciones manifiestan tener más de seis localizaciones de almacenamiento de datos.[99]

Es anecdótico señalar que, a pesar de que el concepto de big data parece intuirse en su artículo, no se menciona explícitamente en ningún momento.

De este modo, si bien es cierto que no existe una definición única y concreta de lo que se entiende por big data, sí parece haber consenso en que “las tres uves” son las características comúnmente aceptadas para definir el big data.

Un ejemplo de ello es la definición de big data aportada por Gartner: “Big data son activos de información de gran volumen, gran velocidad y gran variedad que requieren formas de tratamiento eficientes e innovadoras para

[98] Los datos no estructurados son aquellos que no cuentan con una estructura determinada o que no encajan bien en modelos relacionales. Este tipo de datos son especialmente difíciles de almacenar y analizar, ya que no responden a la organización tradicional de filas y columnas, que es la forma más básica en la que se encuentran los datos estructurados. Además, en muchas ocasiones, es necesario que el procesamiento de este tipo de datos complejos se haga con altas tasas de disponibilidad y rapidez.

[99] ZHENG, Jack G (2018): *Business intelligence and analytics: a comprehensive overview*.

mejorar el conocimiento y la toma de decisiones".[100] En modo similar, la TechAmerica Foundations's Federal Big Data Commission define big data como "un término que describe grandes volúmenes de información a gran velocidad, compleja y variable que requiere de técnicas y tecnologías avanzadas para permitir la recogida, almacenamiento, distribución, gestión y análisis de la información".[101]

Es decir, parece haber una aceptación general de que el concepto identifica cantidades masivas de datos, tanto estructurados como no estructurados, tan grande y complejo que necesita de una rapidez de procesamiento tal que las tecnologías, software y bases de datos tradicionales no pueden gestionar. Sin embargo, estas dimensiones son relativas, y no existe una medida de a partir de qué volumen, velocidad o variedad se habla de big data. El límite dependerá del contexto y podrá evolucionar con el tiempo.[102]

Estas "uves" se han ido completando posteriormente con otras. Ejemplo de ello es la dimensión de "valor" [103] o la "visualización".[104]

8.2. Derecho

El intenso desarrollo normativo de los años previos continuó en el inicio de la década de los 2000, en paralelo a un rápido desarrollo tecnológico que creaba nuevas realidades cuyas amenazas necesitaban de unas reglas de juego comunes y adaptadas al desarrollo de los conceptos jurídicos de privacidad y protección de datos personales.

---

[100] GARTNER, *IT Glosary*. Disponible en: https://www.gartner.com/it-glossary/big-data/.

[101] MILLS, Steve; et al (2012): "Demystifying Big Data. A Practical Guide To Transforming The Business of Government", en *TechAmerica Foundation's Federal Big Data Commission*.

[102] GANDOMI, Amir; HAIDER, Murtaza (2015): "Beyond the hype: Big data concepts, methods, and analytics", en *International Journal of Information Management*, Vol. 35, No. 2, p. 137-144.

[103] GANTZ, John; REINSEL, David (2011): "Extracting Value from Chaos", en *IDC Review*, Vol. 1142, p.1-12.

[104] CHEN, Hsinchun; CHIANG, Roger HL; STOREY, Veda C. (2012): "Business Intelligence and Analytics: From Big Data to Big Impact", en *MIS quarterly*, Vol. 36, No 4, p. 1165-1188.

8.2.1. *Carta de Derechos Fundamentales de la Unión Europea*

A la luz de todos los avances vividos en los años previos, no extraña que el inicio de la década de los 2000 comenzara con una clara demostración de la creciente concienciación sobre la necesidad de proteger al individuo frente a posibles abusos en el tratamiento de sus datos personales. Es de este modo que en diciembre de 2000 se proclama la Carta de Derechos Fundamentales de la Unión Europea,[105] que eleva la protección de datos personales a la categoría de derecho fundamental en la Unión Europea, reconociendo su importancia como uno de los derechos más importantes de la sociedad actual[106] y marcando lo que se ha llegado a definir como un "giro copernicano"[107]. De hecho, tal y como el propio preámbulo de la Carta indica, esta tiene por objetivo "reforzar la protección de los derechos fundamentales a tenor de la evolución de la sociedad, del progreso social y de los avances científicos y tecnológicos".

Se trata de la primera vez un texto internacional de validez jurídica diferenciaba entre el derecho a la privacidad, recogido en el art. 7 de la Carta, y el derecho a la protección de datos personales, recogido en el art. 8. Si bien poco se conoce sobre la motivación específica que llevó a la inclusión de este derecho a la Carta,[108] la separación clara entre ambos derechos otorgaba a la protección de datos personales un carácter propio, ya no subordinado al derecho de privacidad.[109] Cobra sentido marcar esta diferencia, pues ciertamente el derecho a la protección de datos se

[105] Carta de los Derechos Fundamentales de la Unión Europea, de 18 de diciembre de 2000 (2000/C 364/01).

[106] PIÑAR MAÑAS, José Luís (2005): "El derecho fundamental a la protección de datos personales. Algunos retos de presente y futuro", en *Asamblea: revista parlamentaria de la Asamblea de Madrid*, No. 13, págs. 21-46.

[107] PIÑAR MAÑAS, José Luís (2005): "El derecho fundamental a la protección de datos personales. Algunos retos de presente y futuro", en *Asamblea: revista parlamentaria de la Asamblea de Madrid*, No. 13, págs. 21-46.

[108] GONZÁLEZ FUSTER, Gloria (2014): *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, Vol. 16, 1ª ed., Springer International Publishing, p. 206.

[109] GONZÁLEZ FUSTER, Gloria; GELLERT, Raphaël (2012): "The Fundamental Right of Data Protection in the European Union: In Search of an Uncharted Right", en *International Review of Law, Computers & Technology*, Vol. 46, p. 73-75.

despliega, no solo en la esfera privada de la persona, sino también en la pública.[110]

El art. 8 contiene en su párrafo primero la declaración del derecho a la protección de datos *per se*, cuando indica que "[t]oda persona tiene derecho a la protección de los datos de carácter personal que le conciernan". El artículo contiene dos párrafos más. Siguiendo la estela de los instrumentos jurídicos previos, el segundo párrafo reitera que los datos deban tratarse de modo leal, para fines concretos y "sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley". Una vez más, se destaca la importancia otorgada al consentimiento del usuario como medio de control en torno a sus datos personales, al tiempo que se reconoce que puedan existir otras bases que legitimen el tratamiento, que se dejan abiertas. Asimismo, se mencionan los derechos de acceso y rectificación. A continuación, el tercer párrafo reitera la importancia capital de la existencia de autoridades de control independiente. Por último, no puede olvidarse que se trata de un derecho no absoluto, y por tanto sujeto a limitaciones conforme al art. 52 de la Carta. Sin embargo, este artículo no solo destaca por lo que dice, sino por lo que omite: no hace referencia alguna a la informática ni a la necesidad de protegerse de ella.[111]

Es conclusión, el art. 8 de la Carta detalló los principios básicos que deben definir el derecho a la protección de datos personales, tomando como referencia los instrumentos jurídicos supranacionales existentes hasta el momento, entre los que se encontraba la Directiva de protección de datos

[110] RODOTÀ, Stefano (1999): *Repertorio di fine secolo*, 2.ª ed., Editori Laterza, Roma-Bari, pp. 201-202.

[111] PIÑAR MAÑAS, José Luís (2005): "El derecho fundamental a la protección de datos personales. Algunos retos de presente y futuro", en *Asamblea: revista parlamentaria de la Asamblea de Madrid*, No. 13, págs. 21-46.

de 1995[112] y diferenciando claramente este derecho de aquel de la privacidad.[113]

8.2.2. *Reglamento de Protección de Datos por las Instituciones Europeas*

Solo un año después de la proclamación de la Carta nació el Reglamento 45/2001[114] sobre protección de datos personales por parte de las instituciones y cuerpos de la Unión Europea, cuya finalidad era garantizar la libre circulación de datos al tiempo que la protección de los derechos individuales.

Esta norma desarrolla los arts. 7 y 8 de la Carta y, por tanto, puede decirse que nace con un doble objeto de protección. Por un lado, traslada los principios de la Directiva de protección de datos, aplicable a los agentes públicos y privados de los Estados miembros, a los organismos comunitarios. Por otro lado, también introduce obligaciones relacionadas con la protección de la privacidad y la confidencialidad de las comunicaciones, inspirada por la Directiva 97/66. La existencia de esta norma puede entenderse, en primer lugar, por las particularidades que presentan las instituciones europeas, que justificaban poder contar con una

---

[112] Explicaciones sobre la Carta de los Derechos Fundamentales, de 14 de diciembre de 2007 (2007/C 303/02).

[113] En España, el Tribunal Constitucional sigue la estela marcada por la Carta y, mediante las STC 290/2000 de 30 de noviembre, reconoce la existencia del derecho a la protección de datos personales como derecho autónomo que se desprende del art. 18.4 de la Constitución. La Sentencia introduce los elementos que configuran el contenido esencial del derecho a la protección de datos indicando que "consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso". Especialmente relevante es la mención al poder de disposición y control, que fue interpretado a nivel nacional como una suerte de reinado absoluto del consentimiento del interesado.

Para un análisis sobre la construcción y desarrollo del art. 18.4, desde el nacimiento del derecho a la privacidad y a la autodeterminación informativa, pasando por el derecho a la intimidad hasta la protección de datos personales, ver MARTÍNEZ MARTÍNEZ, Ricard (2004): *Una aproximación crítica a la autodeterminación informativa*, Madrid, Civitas.

[114] Reglamento (CE) 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos.

normativa propia. Una de las principales aportaciones del Reglamento fue la creación del Supervisor Europeo de Protección de Datos, autoridad de control independiente con funciones de supervisión, consulta y cooperación.

8.2.3. *Directiva de Comunicaciones Electrónicas*

La intensidad reguladora volvió a mostrar sus resultados en 2002, con el nacimiento de la Directiva sobre la privacidad y las comunicaciones electrónicas, comúnmente conocida como Directiva e-Privacy.[115] Esta norma, que venía a modificar a la anterior Directiva 97/66 sobre datos personales y a la protección de la intimidad en el sector de las telecomunicaciones, pretende garantizar el pleno respeto de los derechos enunciados en los artículos 7 y 8 de la Carta, en concreto, en lo que respecta al sector de las telecomunicaciones. La reforma de la norma en 2002 trae sentido en el hecho de que el avance tecnológico, por ejemplo, el rápido desarrollo de internet, las tecnologías móviles o el creciente uso de rastreadores como cookies había dejado ya desactualizada la Directiva anterior. Este progreso creaba nuevas situaciones y riesgos que debían ser regulados, con especial atención al uso de datos para el envío de comunicaciones electrónicas, la protección de la confidencialidad de las comunicaciones, la identificación de llamadas o la aparición en directorios públicos.

8.2.4. *Tribunal de Justicia de la Unión Europea*

De modo paralelo a la construcción y el desarrollo jurídico de los derechos de privacidad y de protección de datos personales, el Tribunal de Justicia de la Unión Europea (TJUE) ha jugado un papel cada vez más relevante su la interpretación. Ya desde antes de la existencia de la Directiva de protección de datos del año 1995, el TJUE había conocido de casos relativos al tratamiento de información personal, aunque sin la legitimidad

[115] Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas).

que hubiera dado la Directiva, el Tribunal no se refería expresamente a los derechos de privacidad o protección de datos. Desde la promulgación de la Directiva de protección de datos hasta la obligatoriedad de la Carta de Derechos Fundamentales,[116] sus decisiones pretendían definir los límites y alcance de este derecho de forma prudente.[117]

Con el tiempo, el Tribunal fue adquiriendo una postura más activa en la precisión del derecho de protección de datos y ha tomado decisiones de grandísima trascendencia, tales como[118] Digital Rights Ireland Ltd,[119] donde se declaró la invalidez de la Directiva de conservación de datos,[120] Google Spain,[121] por el que se aceptó la existencia del conocido como "derecho al olvido", o Maximillian Schrems v Data Protection Commissioner,[122] que supuso la invalidación del Acuerdo de Puerto Seguro en el que se basaban las transferencias internacionales de datos entre la Unión Europea y Estados Unidos para aquellas organizaciones adheridas.

En conclusión, parece claro que el desarrollo jurídico en la Unión Europea diferencia la existencia de dos derechos diferentes, aquel que se refiere a la protección de la vida privada de la persona y aquel que se refiere a la protección de los datos personales de la persona. A pesar de ello, no obstante, existen áreas de yuxtaposición entre ambos derechos que hacen

[116] La Carta de Derechos Fundamentales de la Unión Europea de 2000 únicamente fue jurídicamente vinculante a partir del año 2009.

[117] AUSLOOS, Jeff (2018): *The Right to Erasure in EU Data Protection Law*, Oxford University Press.

[118] AUSLOOS, Jeff (2018): *The Right to Erasure in EU Data Protection Law*, Oxford University Press.

[119] TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA (2014) Digital Rights Ireland Ltd, asuntos C-293/12 y C-594/12.

[120] Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006 sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE.

[121] TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA (2014): Asunto C-131/12, Google Spain SL, Google Inc v Agencia Española de Protección de Datos (AEPD), Mario Costeja González, de 13 de mayo, apartado 81

[122] TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA (2015): Asunto C-362/14 Maximillian Schrems v Data Protection Commissioner.

que no siempre sea una decisión directa el tipo de protección que un individuo obtendrá o, incluso, el texto normativo que deba ser de aplicación. Esto puede tener consecuencias tanto para los responsables, por cuanto, por ejemplo, las bases de legitimación permitidas por la norma Europa de protección de comunicaciones electrónicas (que desarrolla el art. 7 de la Carta, sobre la privacidad de la persona), son más restringidas que las bases de legitimación previstas en las normas de protección de datos personales (que desarrollan el art. 8 de la Carta, sobre protección de datos personales). Por consiguiente, el resultado y las garantías para el individuo podrán ser diferentes.

Esta situación se ve agudizada por el avance tecnológico y, en concreto, por la capacidad de recogida y análisis de datos que permiten. El enriquecimiento de datos que permiten las tecnologías actuales pone en entredicho incluso la capacidad para anonimizar datos, esto es, para hacer que un dato no sea considerado "personal" y que por tanto quede fuera del ámbito de protección de las normas sobre protección de datos. De este modo, un conjunto de datos que puedan afectar la vida de privada de una persona pero que, en principio, no permitan ser considerados personales, tales como un conjunto de metadatos, únicamente quedarían dentro del ámbito de aplicación de la normativa sobre comunicaciones electrónicas.

La Directiva de protección de datos define[123] dato personal como "toda información sobre una persona física identificada o identificable", siendo identificable aquella persona cuya identidad pueda determinarse, directa o indirectamente. Para determinar cuándo la persona es potencialmente identificable han de tomarse en consideración todos los medios que puedan ser razonablemente utilizados por el responsable. Es decir, la consideración de cuándo un dato puede ser considerado personal o no es un proceso dinámico que tiene en cuenta, no solo los esfuerzos en términos de tiempo y recursos que deben ser empleados por el responsable para

[123] Esta definición se ha mantenido sin alteraciones sustanciales en el RGPD, por lo que las conclusiones aquí vertidas continúan siendo válidas. Ver art. 2.a) y considerando 26 Directiva 95/46 en relación con el art. 4.1 y considerando 26 RGPD.

reidentificar un dato en el momento de la recolección, sino también el estado del arte de los medios tecnológicos en cada momento del tratamiento.

De este modo, la capacidad técnica de cruzar bases de datos a nivel masivo, detectar patrones y descubrir nueva información puede por terminar reidentificando a quien antes era anónimo. En dicho caso, las normas sobre protección de datos serán también de aplicación, en conjunto con las ya aplicables normas sobre comunicaciones electrónicas. En consecuencia, entran en juego normas con estándares diferentes y comienza la labor de dilucidar a qué parte de los datos o de las actividades de tratamiento que forman parte del proceso completo debe aplicarse cada cuerpo normativo. Una tarea desde luego no sencilla debido a la yuxtaposición de conceptos y ámbitos de protección a la que nos referíamos.

Pensemos por ejemplo en una persona sobre la que se realiza un escáner de cuerpo completo.[124] Consideremos que quien revisa las imágenes no tenga datos adicionales de la persona, sino únicamente pueda acceder a la imagen resultante del escáner, que muestra una silueta de la que no se puede extraer información adicional. En dicho caso, sería razonable asumir que la imagen es un dato anónimo con el que no se puede hacer identificable a ninguna persona en concreto. En dicho caso, el sujeto no podrá disponer de las garantías y limitaciones que son objeto de protección bajo el derecho de protección de datos. Sin embargo, en la medida en que el tratamiento de la imagen resultante del escáner puede afectar a la intimidad de una persona, el individuo gozará de protección bajo el derecho de privacidad. Si el paso del tiempo y la evolución de técnicas de análisis de datos evoluciona de forma tal que es razonablemente posible asociar la imagen del escáner con la persona de la que provenía sin esfuerzos desproporcionados, el dato deviene en personal y por tanto el individuo

[124] GELLERT, Raphaël; GUTWIRTH, Serge (2013): “The legal construction of privacy and data protection”, en *Computer Law & Security Review*, Vol. 29, No.5, p- 522-530.

adquiere su derecho a la protección de datos personales. Dependiendo incluso de la naturaleza de la información que adquiera carácter de dato personal, podríamos llegar incluso a poder estar ante datos relacionados con el estado de salud de la persona -categoría especial de datos personales, que son objeto de un mayor nivel de protección.

9. La segunda mitad de la década de los 2000 hasta la actualidad

9.1. Tecnología: el impulso de las tecnologías big data

En relación con el desarrollo de las tecnologías big data, a segunda mitad de la década de los 2000 fue relevante. En 2006, nace el entorno Hadoop, icono de las tecnologías big data. Hadoop es un proyecto de código abierto que funciona como un conjunto o ecosistema de herramientas que utilizan tecnologías diversas. Permite trabajar a gran velocidad con grandes volúmenes de datos, estructurados y no estructurados. Las tecnologías que componen Hadoop funcionan de forma flexible y escalable haciendo uso de internet y de la "nube". Microsoft define la nube en términos sencillos diciendo que se trata de la prestación de servicios de computación (desde servidores, almacenamiento, bases de datos, redes de comunicación, software, analítica e inteligencia entre otros) a través de internet. Así, a través del entorno Hadoop se pueden procesar grandes cantidades de información en paralelo, ya que la información es distribuida en multitud de servidores. Esto permite generar economías de escala, obtener un acceso flexible a los recursos y reducir costes.[125] De este modo, es posible que un gran número de usuarios utilicen al mismo tiempo las herramientas de consulta y análisis de datos para ejecutar tareas cada vez más complejas.

Aunque el funcionamiento de Hadoop es complejo, a los efectos que aquí nos ocupan podemos resumirlo en términos sencillos de la siguiente forma.

[125] MICROSOFT AZURE, *What is cloud computing? A beginners guide*.

Una de las principales funcionalidades es Hadoop es la permisividad del trabajo distribuido, esto es, fraccionar el trabajo en múltiples pequeños ordenadores o nodos. Para ello, Hadoop contiene dos sub-proyectos principales, MapReduce y Hadoop Distributed File System (HDFS).

El subproyecto MapReduce es un componente del ecosistema Hadoop que permite trabajar en paralelo con enormes cantidades de datos particionando la carga de trabajo en partes pequeñas, mediante el desarrollo del trabajo en dos pasos principales: map y reduce. El primer paso (la fase “map”) consiste en dividir los ficheros de origen, que generalmente contienen grandes cantidades de información compleja, en diferentes bloques, cada uno de los cuales se envía a un nodo. En función de las características del fichero, la memoria disponible en cada nodo y la tarea a ejecutar y la correspondiente necesidad de poder de computación, el sistema elige a qué nodo enviar qué parte de los ficheros. Este proceso permite trabajar con un grupo de ordenadores poco potentes por separado pero muy potentes cuando trabajan en sincronía, ya que cada nodo soporta solo una porción del trabajo. De este modo, cada tarea se desarrolla a través de multitud de nodos trabajando en paralelo, acelerando así la finalización de cada tarea. El segundo paso (la fase “reduce”) consiste en reducir o unificar los resultados de cada nodo en un único resultado final.

Estos nodos se encuentran en diferentes localizaciones físicas, dando lugar en ocasiones a problemas en la gestión de la localización de los datos, lo que puede llegar a suponer un problema por la existencia de transferencias internacionales de datos personales.

Por otro lado, Hadoop Distributed File System o HDFS es el modelo de ficheros distribuidos bajo el que funciona el ecosistema Hadoop. La cantidad de información, su complejidad y la necesidad de poder analizarla de forma rápida harían necesario el uso de superordenadores, que en la actualidad son escasos y poco económicos. Este problema se ha resuelto mediante el almacenamiento distribuido en grupos de máquinas o clúster,

que trabajan de manera coordinada como si en realidad se trataran de una sola máquina.

Para funcionar, un clúster necesita una infraestructura encargada de comunicarse con el usuario y de supervisar las tareas, lo cual se lleva a cabo a través de un sistema de nodos máster y nodos esclavos. [126] El nodo máster se sitúa en una posición jerárquica superior en la medida en que es el encargado de las funciones de control, de decidir qué nodo soportará cada parte de la tarea atendiendo a la disponibilidad de recursos, distribuir cada bloque de datos entre los diferentes nodos y servir de comunicación entre el usuario y cada uno de los demás nodos. Asimismo, el nodo máster memoriza en qué nodo se encuentra cada bloque de información y el orden en el que la información debe ordenarse. De este modo, el nodo máster únicamente necesita almacenar los metadatos necesarios para unificar la información, pero no la información en sí misma. Por su parte, los nodos esclavos son los que soportan el grueso del almacenamiento de los bloques de información y de las tareas.

El sistema de nodo máster y esclavos tiene muchas ventajas con respecto a otros modelos de funcionamiento. Por un lado, permite acceder a una gran capacidad de almacenamiento, que además es escalable, pues basta con añadir nuevos nodos al sistema para incrementar su límite. Por otro lado, la paralelización del trabajo permite ejecutar tareas complejas de forma más rápida. Por ejemplo, imaginemos que necesitamos leer un fichero de millones de entradas para después realizar una operación, que puede ser encontrar un dato concreto, ordenar los datos por orden ascendente, buscar una media, etc. Puesto que el fichero ha sido dividido en partes, que se han guardado en diferentes ordenadores o nodos, todos los ordenadores trabajan a la vez, cada uno sobre la parte del fichero que les ha sido asignado, acelerando la ejecución de la tarea. La paralelización del trabajo no es, sin embargo, una capacidad sencilla de conseguir. Por

[126] INUKOLLU, Venkata Narasimha; ARSI, Sailaja y RAVURI, Srinivasa Rao (2014): "Security issues associated with Big Data in cloud computing", en *International Journal of Network Security & Its Applications*, Vol. 6, No. 3.

ejemplo, no siempre es posible trasladar algoritmos a entornos de trabajo en paralelo.[127] Por último, las máquinas que pueden adoptar la posición de nodo pueden ser componentes de hardware ordinarios. De este modo, es posible obtener funcionalidades de gran potencia y complejidad sin necesidad de acudir a un equipo de alto rendimiento. Por poner una analogía, sería como crear un ejército de nodos comunes en lugar de un único super nodo.

En consecuencia, el conocimiento potencial que pueda extraerse de un análisis de datos realizado sobre la base de tecnologías big data como las que aporta el ecosistema Hadoop es más compleja y detallada que la mera obtención de patrones de comportamiento que se obtenía a través de las técnicas de minería de datos desarrolladas en décadas anteriores. Por ejemplo, el hallazgo de un patrón puede resultar en la generación de nuevo conocimiento que sirva de base para tratamientos analíticos posteriores de aprendizaje automático o de creación de modelos predictivos.

De este modo, la analítica de datos posibilita, por un lado, acceder a conocimiento implícito en el conjunto de datos que, sin embargo, no es observable a simple vista. El conjunto de tecnologías que permiten recoger datos a gran escala, analizarlos, utilizar métodos de aprendizaje computacional, minería de datos o herramientas de visualización de datos provoca un crecimiento incremental de la información de partida. En términos sencillos, permite comprender información existente pero no obvia y transformarla en conocimiento. Por otro lado, en otras ocasiones la analítica posibilita ir un paso más adelante y generar información nueva.

El modo de analizar esta información ha sufrido grandes avances en los últimos años. A principios de la década de los 2000, los procesos se basaban mayoritariamente en tratamientos por lotes (en *batch*). En este proceso, los sistemas de ficheros distribuidos y la computación en paralelo

[127] RUSITSCHKA, Sebnem; RAMÍREZ, Alejandro (2014): “Big Data Technologies and Infrastructures”, en *Proyecto Big data roadmap and cross-disciplinary community for addressing societal externalities*, Deliverable D1.4, 2014, p. 31.

permitían un tratamiento de los datos de manera más eficiente, en el sentido ya adelantado anteriormente. Así por ejemplo, cuando una organización programa tareas que son realizadas en horario nocturno o días no laborables es capaz de aprovechar una capacidad de computación que de otro modo estaría inutilizada en ese momento y destinarla a cargar y procesar los datos recogidos durante la jornada anterior.

Este proceso pudo evolucionar a la capacidad de recoger, almacenar y tratar esos datos en flujo continuo, es decir, de manera que la corriente de datos alimente a los sistemas de manera ininterrumpida. Para ello, las soluciones técnicas han debido adaptarse a la necesidad de funcionar de modo rápido, tolerante a fallos y alta disponibilidad. En los últimos años están cada vez más extendidas las herramientas que permiten, no solo que el procesamiento sea continuo, sino que el resultado de la analítica se obtenga en tiempo real o cuasi real.

En esencia, las tecnologías big data constituyen únicamente un paso más en la evolución de las ciencias de datos a lo largo de la historia.

Desde el punto de vista del sujeto de los datos, en años más recientes, la popularización de los dispositivos inteligentes como teléfonos, sensores y objetos cotidianos ha vuelto a cambiar la forma de generar, acceder y utilizar la información. Hoy en día los usuarios de etas tecnologías generan datos de manera continua, a través de acciones diarias como navegar y comprar por internet, realizando pagos a través del teléfono, generando contenido en redes sociales o portando ropa con sensores.

Por su parte, desde el punto de vista del usuario de los datos, en los últimos años están ganando auge herramientas que permiten que usuarios no expertos accedan a la información y conocimiento de la organización por sí mismos, sin necesidad de acudir en todo caso a los equipos de analistas. Ejemplos de estas herramientas son Tableau o Qlik. De hecho, según Forbes, las tecnologías que permiten al propio usuario acceder a la

información por sí mismo fueron catalogadas entre las iniciativas más importantes de 2018.[128]

9.2. Derecho: necesidad de actualización

El momento actual no es el único en el que se han producido desencadenantes o aceleradores de la historia. Sin embargo, el cambio es hoy en día mucho más rápido que en otros momentos, lo que permite hablar más de revolución que de evolución.[129]

A tenor de los grandes y rápidos avances tecnológicos vividos en los últimos años, que se ha llegado a describir como un "tsunami tecnológico",[130] la normativa que garantiza la protección de los individuos en lo que respecta a su privacidad y el tratamiento de sus datos personales quedó de nuevo desactualizada. Hasta este momento, la norma que continuaba rigiendo la protección de datos en la Unión Europea era la Directiva de 1995. Esta norma ha dado respuesta a muchos de los nuevos retos tecnológicos surgidos durante su vigencia, pero resultaba anacrónico y falto de actualización.

Para ayudar a poner esto en contexto, pensemos que en 1995 la utilización de internet ni siquiera se encontraba generalizada. Desde entonces han transcurrido casi veinticinco años. En este tiempo hemos pasado de un mundo eminentemente analógico a uno digital, regido por las telecomunicaciones, el comercio digital y la ubicuidad de sensores. Los cambios estructurales que se han producido en nuestro entorno fruto de la evolución tecnológica necesitan verse reflejados en una normativa adaptada que tenga en cuenta situaciones como la computación en la nube, el Internet de las Cosas o el big data.

---

[128] COLUMBUS, Louis (2018): "The state of business intelligence 2018", en *Forbes*.

[129] PIÑAR MAÑAS, José Luís (2017): "Sociedad, innovación y privacidad", en *Información Comercial Española, ICE: Revista de economía*, No. 897.

[130]RALLO LOMBARTE, Artemi (2012): "hacia un nuevo sistema europeo de protección de datos: las claves de la reforma", en *Revista de Derecho Político*, N.º 85, p. 13-56.

Por este motivo, en el marco de la estrategia de desarrollo del Mercado Único Digital, la Unión Europea inició un largo -y lento- proceso de actualización que comenzó en 2010 con la apertura de un amplio debate centrado en reconceptualizar el marco jurídico de protección de datos personales. Este proceso consensuó el objetivo de la creación de un paquete normativo de protección de datos, conformado por un Reglamento General de Protección de Datos y una Directiva de protección de datos en materia de cooperación policial y judicial penal, cuyas primeras propuestas datan de 2012.

El proceso de elaboración ha sido especialmente largo y tedioso debido, entre otros motivos, a la divergencia de posturas entre los Estados miembros, la presentación de un número récord de enmiendas[131] o la influencia ejercida por distintos grupos de presión. Finalmente, ambas normas han sido adoptadas y son plenamente aplicables desde el 25 de mayo de 2018.

En palabras de la entonces Vicepresidenta de la Comisión Europea Viviane Reding con motivo del inicio de la reforma en 2012 del marco normativo que culminó con el actual RGPD, en el momento en el que se promulgó la Directiva, menos del 1% de los ciudadanos europeos utilizaban internet. En el año 2012 ya se realizaban transferencias de datos de forma cotidiana en cuestión de segundos.[132] En este contexto, se hacía necesario contar con un texto normativo que alcanzase un equilibrio entre los dos elementos clásicos del debate: la protección de datos de las personas y la innovación tecnológica, dos objetivos hacia los que debemos trabajar de manera conjunta.[133]

[131] LEE; Phil; WEBBER, Mark (2016): “The New EU Data Protection Regulation in under 60 minutes”, en *Conferencia* de 17 de mayo.

[132] COMISIÓN EUROPEA (2012): *Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses*.

[133] RECIO GAYO, Miguel (2016): *Protección de datos personales e innovación: ¿(In)compatibles?*, Reus, Madrid.

Sin embargo, existían dos piezas más del puzle que supondrá una renovación completa de las normas de protección de datos personales y privacidad en la Unión Europea. Así, en enero de 2017, la Comisión Europea presentó dos propuestas normativas. En primer lugar, un Reglamento de protección de datos de las instituciones y cuerpos europeos,[134] actualmente finalizado y aplicable desde el 11 de diciembre de 2018. En segundo lugar, el futuro Reglamento e-Privacy o de comunicaciones electrónicas, que sustituirá a la Directiva previa en la materia, que se encuentra aún en fase de borrador.

La culminación de este proceso normativo y la plena aplicación de todas las nuevas normas tiene como objetivo el aumento de la confianza y la seguridad en los nuevos servicios digitales, lo cual es una condición previa para el funcionamiento del Mercado Único Digital.

Especial relevancia merecen el RGPD y el futuro Reglamento e-Privacy.

9.2.1. *Reglamento General de Protección de Datos*

El primer factor a destacar del RGPD[135] es la elección de la figura del Reglamento como instrumento normativo frente a aquél de la Directiva a la que sustituye. El motivo de ello se encuentra en que, mientras una Directiva no es aplicable en los Estados miembros, sino que necesita de trasposición al ordenamiento jurídico -lo cual dio lugar a un escenario fragmentado con divergencias entre los 28 Estados- el Reglamento tiene eficacia directa sin necesidad de norma nacional. Con esto, la Unión Europea pretende lograr el nivel de homogeneización que estuvo en la raíz del desarrollo de la protección de datos en el ámbito comunitario desde sus inicios. A pesar de ello, diversas disposiciones del Reglamento han quedado abiertas de modo

[134] Reglamento 2018/1725, de 23 de octubre de 2018, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos, y por el que se derogan el Reglamento (CE) No. 45/2001 y la Decisión No. 1247/2002/CE.

[135] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

que cada Estado tiene un margen de decisión sobre estos aspectos. Asimismo, el modo de operar de las autoridades de control juega un papel clave en la homogeneización. La disparidad en sus interpretaciones de la norma o la intensidad de sus actividades de investigación y sanción[136] pueden crear incongruencias, precisamente aquellas que desean difuminarse mediante la figura del Reglamento.

La definición de dato personal se ha mantenido técnicamente neutral con intención de no quedar desactualizada ante el avance tecnológico, que pone en entredicho qué se considera personal en cada momento. Por otro lado, el RGPD también mantiene de manera prácticamente inalterada las condiciones que permiten servir de base de legitimación del tratamiento, entre las que se encuentran el consentimiento del interesado o la necesidad del tratamiento para la satisfacción del interés legítimo del responsable o un tercero, sujeto a la realización de un ejercicio de ponderación.

En otro orden de cosas, entre las principales novedades del RGPD se encuentra la inserción del principio de responsabilidad proactiva, que pretende crear un cambio cuasi cultural, de tendencia más anglosajona que continental, e incluso definida como más *cool*[137] por el que la aproximación a la protección de datos personales se realice bajo la premisa de otorgar un amparo efectivo a los interesados y prevenir posibles incumplimientos en ligar del mero cumplimiento de requisitos legalistas y burocráticos que corren riesgo de quedar en papel mojado. De modo similar, el principio de transparencia adquiere una gran relevancia.

Desde el punto de vista del interesado, algunos de sus derechos se han visto reforzados, tales como el de acceso o información, mientras que se

[136] TRONCOSO REIGADA, Antonio (2010): "La protección de datos personales. Una reflexión crítica de la jurisprudencia constitucional", en Cuadernos de Derecho Público, No. 19-20.

[137] TRONCOSO REIGADA, Antonio (2016): "Autoridades de control independientes", en José Luís Piñar Mañas (dir.), Reglamento General de Protección de Datos: Hacia un nuevo modelo europeo de privacidad, Madrid, Reus, p. 465 y ss.

han añadido otros nuevos derechos, como la portabilidad. A lo largo de este trabajo nos referiremos a estos derechos en más detalle.

Desde el punto de vista del responsable, el RGPD incrementa sus obligaciones. Entre estas se encuentran, por ejemplo, la obligación de todas las medias técnicas y organizativas necesarias apropiadas para dar cumplimiento al RGPD así como poder demostrarlo (art. 24), la obligación de respetar los principios de protección de datos desde el diseño y por defecto (art. 25), la creación y mantenimiento de un registro de actividades del tratamiento (art. 30) o aplicar las medidas adecuadas para garantizar la seguridad de la información (art. 32). De especial relevancia es la aproximación basada en riesgos, por la que el responsable debe ser capaz de estimar el peligro potencial de sus actividades de tratamiento y decidir cómo actuar en consecuencia para que este no llegue a materializarse. Por otro lado, el responsable adquiere también la obligación de contratar únicamente con encargados que ofrezcan garantías suficientes (art. 28).

Otras de las novedades destacadas del RGPD es la creación del conocido como mecanismo de ventanilla única y la introducción de la obligación de nombrar un Delegado de Protección de Datos en determinadas circunstancias (arts. 37-39). Asimismo, destaca en gran endurecimiento del régimen sancionador, con la pretensión de que el responsable encuentre desincentivos en la falta de cumplimiento de sus obligaciones. Por último, el RGPD crea el Comité Europeo de Protección de Datos, organismo que viene a sustituir al denominado Grupo de Trabajo de Artículo 29, y que estará integrado por representantes de las autoridades de control de cada uno de los Estados miembros y por el Supervisor Europeo de Protección de Datos (art. 68-71).

A pesar de tener eficacia directa, el RGPD ha sido adaptado a las normas nacionales de la práctica totalidad de Estados miembros. En el caso concreto de España, la LOPD ha sido sustituida por la Ley Orgánica 3/2018,

de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.[138]

9.2.2. *Propuesta de Reglamento de Comunicaciones Electrónicas*

En la actualidad, la norma que rige la protección de la privacidad y las comunicaciones electrónicas continúa siendo la Directiva e-Privacy, creada en 2002. A pesar de las reformas a las que ha sido sometida, sus normas ya se encuentran desactualizadas. Al momento de redactar este trabajo, está en marcha el proceso legislativo ordinario que culminará con la creación de un Reglamento de comunicaciones electrónicas.[139]

El futuro Reglamento e-Privacy tiene como finalidad establecer un nuevo marco legal de privacidad que complemente y particularice el RGPD en lo que respecta las comunicaciones electrónicas.[140] La propuesta de Reglamento e-Privacy tiene en cuenta los importantes avances tecnológicos y económicos en el sector de las comunicaciones electrónicas y modernizará los principios existentes de acuerdo con las nuevas prácticas. Su objetivo es promover un alto nivel de protección de la confidencialidad en las comunicaciones, independientemente de la tecnología utilizada.

El objetivo era que el nuevo Reglamento e-Privacy hubiera sido aplicable desde el 25 de mayo de 2018, simultáneamente con el RGPD. Sin embargo, este ambicioso calendario ha sufrido retrasos y la propuesta se encuentra actualmente en el proceso legislativo de la Unión Europea. En este escenario, existe una situación aún más apremiante para llegar a una versión final del texto tras la declaración del Comité Europeo de Protección de Datos (EDPB) instando a la Comisión, al Parlamento y al Consejo a

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

[139] Propuesta de Reglamento del Parlamento Europeo y del Consejo, de 10 de enero de 2017 sobre el respeto de la vida privada y la protección de los datos personales en el sector de las comunicaciones electrónicas y por el que se deroga la Directiva 2002/58/CE (Reglamento sobre la privacidad y las comunicaciones electrónicas).

[140] Considerando 5 Propuesta de Reglamento e-Privacy.

sustituir la Directiva "lo antes posible". En la misma línea, el Supervisor Europeo de Protección de Datos (SEPD) ha alegado expresamente que "no podemos poner a los responsables del tratamiento en una situación en la que se les exija aplicar simultáneamente un reglamento modernizado de protección de datos junto con normas obsoletas y fragmentadas sobre los datos de las comunicaciones concebidas para regular un mercado y las tecnologías de la comunicación que han cambiado irreconociblemente en los últimos 17 años".

La propuesta de Reglamento es un elemento clave para la ejecución de la Estrategia del Mercado Único Digital, ya que su intención es aumentar la confianza y la seguridad de los servicios digitales.[141] Para tal fin, es importante que el Reglamento e-Privacy propuesto se ajuste a diferentes conjuntos de normas, en particular el RGPD, para ofrecer un alto nivel de protección de la privacidad a los usuarios de los servicios de comunicaciones electrónicas y unas condiciones de competencia equitativas para todos los actores del mercado. En palabras de Giovanni Buttarelli, -Supervisor Europeo de Protección de Datos en el momento de pronunciarlas- "[l]a adopción de la propuesta de Reglamento e-Privacy es crucial para proteger los derechos fundamentales de privacidad y protección de los datos personales en la era digital. Es preciso avanzar rápidamente para garantizar una seguridad jurídica y la igualdad de condiciones para los operadores del mercado. También es necesario completar el marco jurídico de la UE para la protección de datos y la confidencialidad de las comunicaciones".[142] El Reglamento e-Privacy se relaciona de diversas formas con el RGPD.

En primer lugar, el RGPD funciona a modo de *lex generalis* en materia de protección de datos en la Unión Europea y, por lo tanto, se aplica a todas

[141] COMISIÓN EUROPEA (2015): *Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, "Una estrategia para el mercado único digital de Europa"*.

[142] BUTTARELLI, Giovanni (2018): “The urgent case for a new ePrivacy law”, en Blog del *Supervisor Europeo de Protección de Datos*.

las cuestiones relacionadas con el tratamiento de datos personales, independientemente del sector, siempre que no exista una ley sectorial específica que aplicar. En este sentido, el Reglamento e-Privacy es tratará de *lex specialis* que particularizará y complementará al RGPD en lo que se refiera a los datos de comunicaciones electrónicas que se consideran datos personales. En particular, las áreas de comunicaciones comerciales no solicitadas, las tecnologías de seguimiento como las cookies, y la confidencialidad se regulan de manera específica. Por otro lado, en aquellos asuntos en los que el Reglamento e-Privacy no especifique nada, el RGPD se aplicará por defecto (como en el caso de ciertas obligaciones de los responsables). Esto dio lugar, por ejemplo, a la propuesta de derogación de algunas disposiciones respecto de la Directiva e-Privacy, como las obligaciones de seguridad del art. 4 del Reglamento e-Privacy para evitar duplicidades innecesarias.[143]

Por otro lado, mientras que el RGPD desarrolla el artículo 8 de la Carta de los Derechos Fundamentales de la UE sobre protección de los datos personales, el Reglamento e-Privacy está dirigido al artículo 7 de la Carta, que protege la vida privada, el domicilio y las comunicaciones de una persona -con independencia de si se tratan datos personales o no, y de que estos se refieran a una física o jurídica-.

Esta es una de las razones por las que se argumenta la utilidad de disponer de un instrumento separado para garantizar una protección eficaz del artículo 7 de la Carta.[144] Sin embargo, también han surgido algunas voces que argumentan que la mayoría de las operaciones de tratamiento cubiertas por el Reglamento e-Privacy implicarían datos personales y, por lo tanto, estarían cubiertas por el RGPD de manera más flexible. Según este argumento, el Reglamento e-Privacy solamente impondría cargas

[143] Esta derogación se produjo en la propuesta de Reglamento de la Comisión. Por el contrario, la propuesta del Parlamento amplió las medidas medidas de seguridad. Por tanto, queda por saber cuál será el enfoque en el texto final.

[144] Memorando explicativo de la Propuesta, p.5.

innecesarias a los proveedores de servicios de comunicaciones electrónicas.[145]

Asimismo, también se puede considerar que se ha reforzado la coherencia entre el régimen de e-Privacy y el RGPD con la decisión de hacer que las mismas autoridades de supervisión independientes se encarguen de supervisar el cumplimiento de ambas normas.

Finalmente, cabe destacar que los principales objetivos de este futuro Reglamento respecto de la Directiva a la que sustituirá son:

- Ampliar su ámbito de aplicación, principalmente mediante la inclusión expresa de los llamados proveedores de servicios de comunicación Over-The-Top.
- Mejorar la armonización entre los Estados miembros de la UE y mantener la coherencia con el RGPD.
- Fomentar la innovación, por ejemplo, ofreciendo un número ligeramente mayor de excepciones al uso de metadatos y cookies que en el marco de la actual Directiva e-Privacy, al tiempo que se refuerzan los derechos de los usuarios.

9.2.3. *Reglamento de Datos No Personales*

Hasta este momento el estudio se ha centrado únicamente en la utilización de datos personales y la necesidad de encontrar un punto de equilibrio entre su libre circulación y la protección de los derechos de los individuos. Sin embargo, las tecnologías descritas a lo largo de este capítulo hacen uso también de una enorme cantidad de datos no personales. Así, el 18 de diciembre de 2018 entró en vigor el Reglamento sobre la libre circulación de datos no personales en la Unión[146] Este Reglamento ha pasado mucho más desapercibido que las demás normas aquí mencionadas, pero también

[145] CENTRE FOR INFORMATION POLICY LEADERSHIP (2018): “EPR vis-à-vis GDPR, A comparative analysis of the ePrivacy Regulation and the General Data Protection Regulation”, p. 10.

[146] Reglamento (UE) 2018/1807 del Parlamento Europeo y del Consejo, de 14 de noviembre de 2018, relativo a un marco para la libre circulación de datos no personales en la Unión Europea.

merece importancia, pues el uso de datos no personales es igualmente relevante en la economía actual. Por ejemplo, el uso de datos en el sector agrícola permite gestionar de forma eficiente las necesidades de agua, plaguicidas o automatizar la producción industrial. Por otro lado, el tratamiento de datos anónimos o anonimizados, si bien quedan fuera del ámbito de protección de las normas de protección de datos, no así respecto de este Reglamento. Este hecho es importante, por cuanto la anonimización se ha presentado en ocasiones como la gran solución frente a las extensas obligaciones de protección de datos personales (caso aparte es la dificultad de obtener un set de datos verdaderamente anonimizado, pero este no es el tema de hoy).

El Reglamento nace con la finalidad de limitar los impedimentos previamente existentes a la libre circulación de datos personales entre Estados miembros creados diferentes normas nacionales. Estas limitaciones partían de la desconfianza de las autoridades nacionales de no poder acceder a determinada información que un responsable determinado pudiera almacenar en otro Estado, escudándose en que dicha autoridad no podría investigarle por falta de competencia extraterritorial. Como consecuencia añadida, la creación de barreras al flujo de los datos deteriora la libre competencia entre prestadores de servicios basados en datos.

Sin embargo, el entorno comunitario caracterizado por la mutua confianza, que consiste en la base, además, de los principios de libertad de circulación de personas, capitales y mercancías. Todo ello por no hablar de que desde hace décadas la regulación sobre datos personales se basa asimismo en la libertad de flujo entre Estados miembros. Por este motivo, los datos no personales constituían uno de los últimos silos a abrirse.

Así, el Reglamento establece la libertad de circulación de datos salvo justificación por razones se seguridad pública. Con ello se pretende favorecer asimismo la potabilidad de los datos, de forma que se traduzca en una mayor libertad de elección de proveedores de servicios basados en datos, así como la libre competencia y precios más competitivos. Para que

este sistema funcione, el Reglamento establece la obligación de cualquier proveedor -por ejemplo, un proveedor de servicios de almacenamiento en la nube-, de poner los datos que se le reclamen a disposición de las autoridades nacionales competentes, así como la declaración de nulidad de cualquier cláusula contractual que prohíba dicho acceso.

Sin embargo, para un responsable o proveedor no siempre es una tarea sencilla identificar qué datos son personales y cuáles no personales. ¿Qué normas deben aplicarse en dicho caso? El Reglamento también ha previsto esta circunstancia, estableciendo que en dicho caso serán aplicables las normas de protección de datos personales y por tanto todas sus garantías.

En definitiva, esta norma refleja la profunda transformación que está llevando a cabo la Unión Europea para actualizar sus normas de acuerdo con las nuevas realidades basadas en datos.

10. Conclusiones

El objetivo de este capítulo ha sido señalar los principales hitos históricos que ayudan a comprender, por un lado, el desarrollo desde las formas más primitivas de tratamiento de datos hasta la irrupción de las tecnologías big data. Las tecnologías big data no consisten en un fenómeno nuevo, sino que son fruto de una larga evolución en el tratamiento de datos, tanto personales como no personales. Por otro lado, de manera paralela también hemos señalado los hechos más relevantes que han sentado las bases del actual mosaico regulatorio relativo a ciertos aspectos relacionados con el tratamiento de datos, especialmente datos personales, en la Unión Europea. Haciendo un pequeño resumen de todo lo analizado hasta ahora podremos extraer mejor algunas conclusiones preliminares de este trabajo.

Desde las tecnologías más arcaicas de recogida de datos como el mecanismo de Antiticera, pasando por las tarjetas perforadas, las primeras bases de datos, la minería de datos y la expansión de internet, hasta las tecnologías actuales de tratamiento de datos ha habido una larga evolución. Este camino, y la constatación de preocupación por la falta de

control en torno al tratamiento de datos, hizo emerger el debate en torno a la necesidad de garantizar un derecho a ser dejado en paz y a la privacidad, que no terminó de cristalizar en nuestro continente hasta 1950, cuando la Convención Europea de Derechos Humanos reconoció en su art. 8 en al respeto a la vida privada y familiar, al que con el tiempo se acabó haciendo referencia como derecho a la privacidad. Con los años, la conversación en torno a estos nuevos derechos fue desarrollándose, hasta las primeras normas de protección de la información personal, que siguieron a la primera, aquella del estado alemán de Hesse. Cabe destacar cómo desde estos primeros años, las normas se referían a la computación y la informática en términos negativos y de creación de riesgos, de los que las personas debían ser protegidos, entre otros medios, a través del consentimiento y la creación de las primeras garantías para los sujetos.

Esta concepción se mantuvo durante un largo período de tiempo y fue heredada desde el derecho a la privacidad hasta el de protección de datos personales. Ejemplo de ello fue el Convenio 108 del Consejo de Europa, primer instrumento internacional jurídicamente vinculante que utiliza el término “protección de datos”, centrado en el reconocimiento de los riesgos de la informática. Sin embargo, también con el tiempo se observa un cambio de tendencia. Las Directrices de la OCDE sobre protección de la privacidad y flujos transfronterizos de datos personales (1980), prácticamente coetáneas al Convenio 108, reconocen el valor económico del uso de los datos y busca favorecer su circulación al tiempo que valoran la función del consentimiento y los deberes de información, deja patente que no serán siempre convenientes o efectivos. Unos años más tarde, la Directiva europea de protección de datos (1995), también incluye referencias a la necesidad de garantizar la libre circulación de los datos para extraer el máximo potencial positivo de ellos. Esta Directiva, además, conceptualiza de forma clara qué otras bases de licitud del tratamiento además del consentimiento podrán ser válidas, incluyendo ya el interés legítimo en una redacción prácticamente inalterada hasta nuestros días.

Con el tiempo, la protección de datos adquirió tal importancia en nuestro continente que terminó por ser declarada derecho fundamental.

En perspectiva histórica, en cambio, ambos caminos, tecnológico y jurídico no han transcurrido de forma paralela. La evolución de la técnica y el abrazo de las innovaciones y sus beneficios han sido un proceso mucho más rápido que aquél de lograr detectar riesgos y consensuar posibles soluciones en forma de normas jurídicas.

Sin embargo, desde la década de los 2000, el desarrollo tecnológico se ha acelerado de modos sin precedentes. La gran rapidez del desarrollo tecnológico ha supuesto el paso a una economía eminentemente digital en un corto período de tiempo, lo que dejó las normas sobre protección de datos personales y privacidad rápidamente desactualizadas.

La gran mayoría de actividades cotidianas que hace solo unos años solo podían hacerse en el mundo físico podemos hacerlas hoy en entornos digitales. Por ejemplo, comprar por internet, socializar a través de redes sociales, trabajar en remoto almacenar documentos en la nube. Estos avances han tenido un punto común: la posibilidad de crear y recoger enormes cantidades de datos. En los últimos años hemos asistido a una profunda reforma de todo el marco normativo asociado al tratamiento de datos, tanto personales como no personales. El máximo exponente de ello ha sido la publicación del Reglamento General de Protección de Datos, pero desde luego no el único. Hasta el momento, varias piezas del puzle han sido actualizadas, y así contamos con una nueva Directiva de protección de datos en el ámbito penal y policial internacional, un nuevo Reglamento aplicable a las instituciones y cuerpos de la Unión Europea y un Reglamento de datos no personales. El futuro Reglamento conocido como e-Privacy, actualmente en tramitación, será la última gran pieza en reformarse. Este nuevo escenario normativo nace con el objetivo de que un conjunto de normas adaptadas al desarrollo digital regule de manera coherente y uniforme el tratamiento de datos personales en la Unión

Europea. Con ello, se pretende aportar seguridad jurídica a los responsables, así como reducir la carga administrativa en favor de aquellas tareas que tienen un impacto real en la efectiva protección de los individuos.

Estos avances nos dejan algunas lecciones relevantes. En primer lugar, la importancia del análisis sofisticado de datos en la actualidad radica en la posibilidad de descubrir información no observable a simple vista y obtener conocimiento para la toma de decisiones.

En segundo lugar, ha quedado patente que los datos aumentan de valor con su uso. En concreto, la analítica de datos permite obtener un gran valor y conocimiento de la reutilización de los datos. Esta reutilización puede realizarse, por ejemplo, para proveer un servicio, mejorar un servicio existente, personalizar un servicio, publicitar otro producto o compartir los datos con terceros. Todo ello es necesario para acceder a los grandes beneficios del tratamiento de datos, aunque también puede ser fuente de riesgos para los derechos y libertades de las personas.

En tercer lugar, es necesario crear un entorno de confianza que permita una reutilización de datos de manera lícita -y ética- entre organizaciones, sectores, y Estados. En gran medida, esta generación de confianza vendrá determinada por la defensa de los derechos de protección de datos, privacidad y por la seguridad de la información. De este modo, la protección de los datos personales de los individuos no debe ser vista como un freno al desarrollo tecnológico y empresarial. Al contrario, se trata de una ventaja competitiva para aportar calidad y valor añadido al cliente final. Un aspecto especialmente importante en este sentido es la posible existencia de asimetrías de información entre los individuos y los responsables del tratamiento, que causa deficiencias en el ejercicio de control y la efectividad de los derechos de los interesados. Por otro lado, la reciente evolución de estos derechos, y en concreto, en derecho a la protección de datos personales demuestra que nos encontramos ante un proceso de construcción constante, pues los riesgos frente a los que la normativa trata

de proteger a los individuos evolucionan en función de las nuevas aplicaciones tecnológicas.[147]

En cuarto lugar, el desarrollo de técnicas de análisis de datos provenientes de diferentes fuentes permite enriquecer la información ya existente hasta el punto de facilitar la reidentificación de datos que antes eran considerados anónimos. Ello pone en entredicho la definición misma de dato personal y la efectividad de la anonimización como medio de garantía de los derechos de los individuos.

En quinto lugar, a pesar de que el estado de la técnica lo permita, el grado de madurez de las organizaciones o sus prácticas internas en ocasiones implica que los datos se almacenen aún en silos incomunicados. Ello causa falta de coherencia entre los datos de una misma organización, lo cual resulta un factor de riesgo para la calidad del conocimiento que se extraiga del análisis de esos datos y de las decisiones que se tomen a partir de ellos. Ello es especialmente cierto si dichas decisiones afectan de manera significativa a la persona.

En sexto lugar, queda patente la importancia que el derecho a la protección de datos personales le ha otorgado a la figura del consentimiento desde sus inicios. Ello no obstante, desde la creación de los primeros instrumentos jurídicos internacionales a principios de los años 80 que han inspirado todo el desarrollo normativo posterior hasta la actualidad-Directrices sobre privacidad y flujo transfronterizo de datos de la OCDE de 1980 y el Convenio 108 de 1981-, también queda claro que el consentimiento nunca se vislumbró como el único medio, ni siquiera el principal, para poder legitimar el tratamiento de datos. En la misma línea, la Directiva de protección de datos personales de 1995, la Carta de Derechos Fundamentales de la UE de 2000 y el RGPD de 2016, mantienen

[147] DE LA QUADRA-SALCEDO FERNÁNDEZ DEL CASTILLO, Tomás (2018): “Retos, riesgos y oportunidades de la sociedad digital”, en Tomás de la Quadra-Salcedo y José Luis Piñar (dirs.), Sociedad digital y Derecho, Madrid, BOE-Red.es, p. 50.

dicha postura. Bien es cierto que, sorprendentemente, la Directiva e-Privacy y la propuesta de futuro Reglamento que se espera la sustituya, se circunscriben al consentimiento para legitimar aquellos tratamientos de datos -personales o no personales- que no sean necesarios.

Por último, la efectiva protección de los derechos y libertades de las personas, en especial la protección de sus datos personales y su esfera de privacidad requieren amplias labores de educación y concienciación, máxime en un momento en el que la velocidad del desarrollo dificulta que el ciudadano medio se mantenga actualizado sobre cómo se tratan los datos personales y cómo puede afectarle. Asimismo, las labores de concienciación que deben ir dirigidas a todos aquellos que interfieran en el ciclo de vida del dato dentro de una organización que actúe como responsable, desde los responsables del tratamiento a nivel personal, pasando por los trabajadores de una empresa, los funcionarios de la Administración o los desarrolles de tecnologías.

CAPÍTULO III. APROXIMACIÓN A UN MODELO EN FASES DE LAS TECNOLOGÍAS BIG DATA

> Vivimos en un mundo en el que cada vez hay más y más información, y menos y menos significado. En todas partes se busca producir sentido, hacer que el mundo signifique, hacerlo visible. Sin embargo, no corremos el riesgo de que nos falte significado; al contrario, nos llenamos de significado y nos está matando" .[148]

1. Introducción

En el capítulo anterior analizamos la evolución de ciertos desarrollos tecnológicos y los principales hitos que culminaron con la aparición de las tecnologías big data así como con el cuerpo normativo actual en materia de protección de datos de la Unión Europea. En este capítulo, realizamos una inmersión hacia los factores más relevantes que nos ayuden a comprender cómo funcionan las tecnologías big data, e introducimos las primeras pinceladas sobre algunos de los problemas que pueden sufrir en relación con el tratamiento de datos personales. Con ello sentamos las bases para el análisis jurídico que realizaremos en los capítulos siguientes.

En este capítulo se muestra una esquematización de los procesos big data a partir de un modelo en tres fases. La primera fase se corresponde con la recolección de los datos de origen y su preparación. En una segunda fase se realiza la analítica de datos, búsqueda de correlaciones y patrones, creación de nuevo conocimiento y de un modelo algorítmico. En una tercera fase, dicho modelo se pone en funcionamiento y se aplica sobre los datos de una persona concreta. Con ello, es posible elaborar perfiles y tomar decisiones que afectan al interesado. Durante todo el proceso, los nuevos

[148] BAUDRILLARD, Jean (1981): *Simulacres et Simulation and Simulation*, Éditions Galilée.

datos generados sirven para realimentar el modelo y realizar un entrenamiento automatizado.

Este esquema de tres fases supone una reducción del modo en que funciona un proyecto de uso de tecnologías big data en la práctica. El motivo de ello es que el objetivo es comprender la existencia de diferentes momentos que pueden suponer el tratamiento de datos personales y diferenciar claramente cada uno de ellos, pues cada fase despliega consecuencias jurídicas diferentes que corren el riesgo de ser confundidas o malinterpretadas sin el conocimiento previo de dichas fases del ciclo de vida de un proyecto big data. En la práctica, las líneas y momentos que dividen estas fases son difusas y dinámicas, e incluso serán diferentes en cada caso. En consecuencia, el objetivo de esta sección no es la realización de una descripción detallada de procesos técnicos que trascienden el alcance y la utilidad de nuestro estudio.

Hoy en día, el desarrollo de tecnologías que permiten mayores volúmenes de almacenamiento de datos, una transmisión y potencia de cálculo más rápida y un análisis más sofisticado facilitan la recogida de datos cada vez más variados y la extracción de relaciones de los mismos, lo que permite la creación de perfiles más precisos. Los usos de los perfiles son muy variados, y sus mayores oportunidades son la descripción y, sobre todo, la predicción de comportamientos con fines que van desde la calificación crediticia hasta el marketing directo o la prevención del crimen. Si bien las actividades de elaboración de perfiles tienen enormes beneficios, también pueden crear riesgos, en particular cuando se utilizan sin el conocimiento de las personas afectadas.

2. Fase 1 del big data: Recolección de datos

Esta fase implica la recogida de los datos que serán la base del proyecto big data o de las actividades de tratamiento que hagan uso de tecnologías big data para su posterior explotación.

2.1. Adquisición de datos

2.1.1. Origen diverso

La adopción de nuevas tecnologías de recolección automática de datos conlleva una intensificación de las actividades de recolección de datos. El origen de los datos que se generan en la actualidad es muy variado, y esto supone recoger tanto datos estructurados como no estructurados. En términos sencillos, los datos estructurados son aquellos que se pueden almacenar en tablas como las hojas de cálculo, compatibles con bases de datos relacionales. Se trata de datos generalmente ordenados y fácilmente analizables de manera automatizada. Los datos provenientes de sensores como el número de pasos que da una persona al día, la fecha de nacimiento o las transacciones bancarias de una cuenta son datos estructurados.

Por el contrario, los datos no estructurados son aquellos que no tienen un formato definido, o en otras palabras, no contienen campos fijos con los que sistematizarlos, sino que se trata de un conjunto de datos heterogéneo y desordenado más difícilmente analizable. Por este motivo, este tipo de datos no son fácilmente procesables a través de bases de datos relacionales, que no fueron pensadas en origen para esta finalidad, sino que son manejadas con herramientas como Hadoop. El análisis de estos datos tiene un alto valor potencial, pero este solo se puede extraer en la medida en que la tecnología permita organizar la información subyacente que aportan. Algunos ejemplos de datos no estructurados son archivos de voz, que requieren, por ejemplo, tecnologías de reconocimiento de voz para poder comprender su contenido, los mensajes de redes sociales, que pueden ser sometidos a tecnologías de procesamiento de lenguaje natural para comprender si el sentido del mensaje emite una emoción positiva o negativa, o las imágenes. Estos datos han supuesto uno de los mayores retos en lo que se refiere a la gestión de la información y el big data, pero también una gran cantidad de valor por la riqueza del conocimiento que se puede extraer de ellos.

2.1.2. *Metadatos*

En ocasiones, los datos (estructurados y, sobre todo, no estructurados), pueden asociarse a otros datos que ayudan a describirlos y sistematizarlos, y que conforman metadatos. Así por ejemplo, la hora, el lugar y la configuración de las opciones técnicas de un dispositivo pueden ser metadatos que describan a una fotografía o una llamada telefónica. Estos datos aportan una gran cantidad de información adicional sobre el dato principal, incluso sin necesidad de acceder a este. De este modo, la información sobre la duración de una llamada telefónica, que no constituye dato personal, puede revelar una GRAN cantidad de información sobre el emisor de la llamada, incluso sin conocer quién es dicha persona y sin acceder al contenido de la comunicación. De manera similar, el acceso a la localización de un teléfono inteligente -un dispositivo estrechamente ligado a una persona- permite inferir dónde vive la persona asociada a dicho teléfono (por ejemplo, conociendo dónde se localiza el dispositivo todas las noches), o incluso la creencia religiosa de la persona (si por ejemplo la localización muestra la entrada en un centro de culto religioso de manera periódica). De este modo, un conjunto de metadatos que en un inicio eran datos no personales como la localización de un teléfono pueden llegar a constituir datos personales e incluso categorías especiales de datos personales. Información esta a la que se puede acceder gracias a la creciente capacidad de recoger datos a través de sensores, de ordenarlos y almacenarlos gracias a la reducción de los costes de almacenamiento, principalmente en la nube, y de posteriormente analizarlos.

2.1.3. *Fuentes de los datos*

En la actualidad, prácticamente todas nuestras acciones cotidianas generan datos que son recogidos y almacenados. La capacidad de recoger y almacenar datos para extraer valor de ellos hace que las fuentes de los datos se hayan diversificado enormemente de manera paralela al avance técnico. Mientras las tecnologías tradicionales necesitaban, en general, poder contar con una planificación previa sobre el tipo de datos y de fuentes

de datos que servirían de flujo de entrada, las tecnologías más avanzadas como las que hacen uso de los sistemas big data permiten un alto nivel de flexibilidad en este sentido. Existen diversas formas de clasificar las fuentes de origen de los datos, siendo algunas de estas las siguientes.

Los datos pueden provenir directamente de la persona, por ejemplo, cuando el interesado es requerido para rellenar un formulario con su nombre, dirección y fecha de nacimiento; la huella dactilar que puede servir de medio de autenticación biométrico; o la grabación de una conversación telefónica. Es relevante señalar que los datos obtenidos mediante manifestación del interesado son menos confiables que otras fuentes de datos (¿quién no ha aportado datos falsos o incompletos en alguna ocasión en un formulario en internet?). La problemática de ello es que, en muchas ocasiones, el usuario puede no ser consciente del tipo de actividades de tratamiento a que se destinarán los datos ni de las posibles consecuencias de haber aportado información errónea. Por su parte, el responsable deberá implementar mecanismos para verificar la veracidad de los datos en atención al principio de calidad de los datos, pues de lo contrario, el análisis y decisiones tomadas sobre la base de estos pueden ser incorrectos.

Por otro lado, los datos pueden proceder de sensores cada día más numerosos en todos los ámbitos, tanto cotidianos como industriales. Los sensores pueden recoger información sobre una persona, como el ritmo cardíaco, información de procesos, por ejemplo, la velocidad de entrega de un paquete, o información sobre un dispositivo, por ejemplo, la localización, la temperatura de una pieza de maquinaria, o señales inalámbricas emitidas por el dispositivo como wifi o bluetooth.

Los datos pueden ser obtenidos en el curso normal de las actividades del responsable del tratamiento como, por ejemplo, las transacciones de una compañía con cada cliente. Entre las fuentes internas de una organización hay que tener en cuenta los datos generados por cada departamento, como marketing, contabilidad, etc. También encontramos, por ejemplo, aquellos

archivos que han creado personas concretas que no están integrados con los datos de la compañía pero que pueden ser de alto valor. El almacenamiento de estos datos debe ser un repositorio común, pues esto permite obtener una visión de conjunto y una posterior extracción de valor y explotación de todos los datos. Asimismo, esto minimiza el riesgo de que datos básicos de la organización sean erróneos cuando están almacenados en silos no comunicados. Por ejemplo, en el departamento financiero de una organización, el dato de número de cliente totales puede calcularse como la suma de todos los usuarios que existen registrados en el sistema, mientras que para el área de contabilidad el mismo dato puede calcularse en función del número de personas que alguna vez han comprado nuestros productos en los últimos 12 meses. Este número puede no coincidir si, por ejemplo, una misma persona tiene dos usuarios registrados. De este modo, diferentes maneras de contabilizar un mismo dato pueden dar lugar a incongruencias internas y restar calidad a los datos.

Asimismo, los datos pueden también tener su origen en terceros agentes de los que se obtienen, lo que constituye la base del mercado de datos y de los modelos de negocio de los *data brokers*. Este es, de hecho, el motivo por el cual las cookies y otros medios de rastreo del usuario en sus actividades en internet se encuentran tan extendidos en la actualidad. Por otro lado, los datos pueden tener su origen en fuentes como redes sociales o internet, quizás una de las más ampliamente utilizadas. Estas no deben confundirse, no obstante, con aquellas "fuentes accesibles al público", definidas jurídicamente. Este flujo de datos provoca que el número de agentes que potencialmente pueden tener acceso a los datos personales replicados de un individuo es incalculable.

Mención especial merece también la información inferida,[149] que se obtiene a partir de otra información adicional, y que puede ser utilizada posteriormente para tomar acción son respecto a una persona (por ejemplo,

[149] ABRAMS, Martin (2014): "The Origins of Personal Data and Its Implications for Governance", en *OECD Expert Roundtable Discussion `Protecting Privacy in a Data-Driven Economy: Taking Stock of Current Thinking´*.

mediante la elaboración de perfiles y la asignación de un perfil concreto a una persona determinada).

Esto muestra que el proceso de adquisición de los datos es dinámico, en la medida en que se da a lo largo de todo el ciclo de vida de los datos y de un proyecto. Ello se debe, no solo a la capacidad de generar y obtener flujos de datos en tiempo real, y la consiguiente realimentación de las fuentes de datos con la nueva información. Por último, los datos pueden ser de naturalezas infinitas: financieros, de salud, macroeconómicos, tráfico de comunicaciones, etc.

2.2. Proceso ETL (extracción, transformación y carga)

Tras la captación de los datos, el siguiente paso consiste en realizar el denominado proceso ETL, es decir, de extracción, transformación y carga, según sus siglas en inglés. Es decir, en este momento los datos primarios se mueven desde sus fuentes de origen, se "limpian" de manera que se unifican los formatos de cada uno de ellos, se preparan los datos para su posterior análisis y se cargan en un repositorio común o *datawarehouse*. Este paso constituye una de las bases de un proyecto que emplee tecnologías big data y sin él no sería posible tratar los datos en su conjunto y transformarlo en conocimiento. De hecho, el proceso ETL conlleva más de un 50% del tiempo total de un proyecto de explotación de datos.

2.2.1. Extracción

En la medida en que un determinado sistema haga uso de datos provenientes de diversas fuentes, estos tendrán en origen formatos diversos incompatibles entre sí, o estarán organizados de manera diferente. Por ello, el primer paso será extraer los datos de cada una de las fuentes. Generalmente, los datos se cargan en repositorios intermedios que sirven de puente entre el origen de los datos y su destino final en los sistemas de la organización o la nube.

2.2.2. Transformación

Uno de los motivos de la importancia del proceso ETL es la existencia de los llamados datos sucios, esto es, aquellos datos duplicados, incorrectos, datos en blanco, falsos, inexactos o con formatos diferentes que no pueden ser comparados. En entornos en los que las fuentes de los datos no sean tan dispares, o la cantidad de datos analizados no sea masiva, será más sencillo poder corregir errores en los datos primarios de manera manual. Sin embargo, en entornos en los que se tratan volúmenes masivos de datos y estos provienen de fuentes tan diversas como las analizadas, normalizar la estructura de todo el flujo es crucial, pues de lo contario los modelos algorítmicos construidos sobre la base de datos sucios serán erróneos.[150] En consecuencia, la existencia de fuentes de datos tan dispares provoca que la organización deba crear reglas de transformación adaptadas a cada fuente de origen, lo cual conlleva un gran esfuerzo y cantidad de recursos.

La corrección de los errores más comunes en los datos se realiza de manera automatizada. Un ejemplo sencillo es la necesidad de unificar expresiones como “C/” o “calle” que se usan indistintamente, pues el sistema en el que se analizarán los datos únicamente reconoce un formato estandarizado para saber que un dato se refiere a la primera parte de la dirección de una persona. Otras operaciones de transformación de datos pueden incluir la selección de determinados atributos y el deshecho de otros o el cálculo valores, que se da, por ejemplo, cuando los datos de origen indican el volumen de ventas de cada producto y su precio, mientras que deseamos guardar el dato final del total de ventas. También se consideran las reglas de validación de datos por las que, por ejemplo, aquellos atributos con datos en nulos o en blanco sean automáticamente rechazados. Por último, otras transformaciones pueden ser más complejas o requerir procesos manuales.

[150] LUCKER, John; HOGAN, Susan K. ; BISCHOF, Trevor (2017): “Predictable inaccurate. The prevalence and perils of bad big data”, en *Deloitte Review*, No. 21.

Durante este proceso, además, los datos no estructurados son transformados en datos estructurados de modo que puedan ser integrados con el resto de información en la base de datos de destino.

2.2.3. *Carga*

A partir de entonces, los datos ya pueden ser cargados y almacenados en un repositorio común, que recibe el nombre de *datawarehouse*. La información se etiqueta a través de metadatos, se almacena y se deja preparada para su análisis. Además, a partir de este repositorio general pueden crearse otros más específicos, llamados *datamarts*, que sirvan a las finalidades específicas de un subgrupo de usuarios, que puede ser, por ejemplo, un área concreta de la organización. Esto permite que determinados usuarios tengan acceso a los datos que necesitan sin crear almacenes de información desconectados que conduzcan a incongruencias internas.

Hoy en día, la capacidad de almacenamiento en la nube ha provocado un gran abaratamiento de los costes de almacenamiento, favoreciendo que las organizaciones prefieran conservar datos para la toma de decisiones y el entrenamiento de modelos algorítmicos en lugar de desecharlos. Estas prácticas pueden causar tensión con el principio de minimización de datos personales, por el cual los datos deben ser, no solo adecuados y pertinentes en relación con la finalidad del tratamiento, sino también estar limitados a lo necesario para perseguir dichas finalidades. En otras palabras, las organizaciones no deben recoger más datos de los necesarios para la finalidad que se persigue (que recordemos, debe estar también limitada).

Este principio choca con la base de las tecnologías basadas en datos, que se basan en lo que se ha venido a denominar “maximización de datos”.[151] Ello es porque el funcionamiento de un dispositivo o servicio específico puede no necesitar la recogida de grandes cantidades de datos, pero los

[151] WACHTER, Sandra (2018): “The GDPR and the Internet of Things: a three-step transparency model”, en *Law, Innovation and Technology*, Vol. 10, No. 2, p. 272.

servicios big data que se nutren de estos para posteriormente personalizar acciones sí necesitan grandes cantidades de datos. Por todo ello, es importante el respeto a los principios del tratamiento de datos personales, con especial énfasis en la limitación de la finalidad, así como los principios de licitud y lealtad, ligados a la elección de una base de legitimación del tratamiento válida.

3. Fase 2 del big data: Análisis y descubrimiento

Esta fase conlleva realizar un análisis de los datos obtenidos en la fase anterior a través del uso intensivo de técnicas de inteligencia de negocio, minería de datos y modelos algorítmicos para descubrir correlaciones, patrones de comportamiento y, en definitiva, conocimiento que se encontraba oculto en la complejidad de los datos y que no es patente a simple vista. Además de ello, quizás una de las grandes promesas de las tecnologías big data es la capacidad de poder realizar predicciones futuras con mayor nivel de precisión que cuando se utilizan datos menos actualizados y en menor volumen.

En el momento de la recogida de los datos, las posibles correlaciones que se encuentren no pueden ser anticipadas. De hecho, el gran valor del big data reside precisamente en esa información que se consigue desvelar que de otro modo hubiera escapado a la percepción y en los nuevos usos que se le pueden dar a los datos. De este modo, estos usos secundarios de los datos son la base de un cambio de paradigma que llega con el big data.

3.1. Funcionamiento

Estos modelos funcionan sobre aplicaciones avanzadas que pueden incluir minería de datos, aprendizaje automático, inteligencia artificial u otras técnicas que, en realidad se encuentran en constante cambio y cuyo uso dependerá del caso concreto. Uno de los beneficios de estas técnicas es la posibilidad de comenzar el análisis de los datos sin necesidad de partir de una hipótesis preestablecida, como sería el caso en un proyecto de

estadística tradicional.[152] No obstante, tienen su origen en métodos estadísticos y matemáticos, y cuyos resultados se pueden resumir en muchas ocasiones en términos de probabilidad. Esto tiene como consecuencia, por un lado, que la calidad de los datos obtenidos durante la Fase 1-Adquisición de datos determinará los resultados que se obtengan en la Fase 2-Análisis.[153] Del mismo modo, la realimentación del modelo con los nuevos datos y el aprendizaje automático que realice, así como la elección entre un modelo u otro determinará los resultados. Como ya ha sido señalado por la doctrina,[154] los resultados algorítmicos no se pueden reducir a términos de exactitud matemática, pues las decisiones previas relativas a los datos con los que se construye un modelo, así como el propio modelo algorítmico pueden contener sesgos, prejuicios o errores que son achacables al ser humano, no a la tecnología.

De este modo, cuando se "replica al hombre en la máquina"[155] aquél que toma las decisiones sobre los datos de origen, su calidad y la configuración del modelo estaría dando lugar potencialmente a dos fenómenos: en primer lugar, la imprimación de su propio criterio en el modelo o, en su caso, de pensamiento vigente en un momento concreto del tiempo reflejado en la estadística. En segundo lugar, la cristalización de esos patrones en el futuro, en la medida en que tales algoritmos serán utilizados para tomar decisiones a posteriori.

Por lo anterior, corremos el riesgo de perpetuar criterios estáticos que correspondían a un momento de tiempo pasado, y que no serán revisados

[152] INFORMATION COMMISSIONER'S OFFICE (2017): *Big data, artificial intelligence, machine learning and data protection* (versión 2.2).

[153] De hecho, el RGPD extiende el principio de calidad de los datos, no solo al momento de la recogida de los datos, sino al tratamiento posterior y al momento final de su supresión. PUYOL MONTERO, Javier (2016): "Los principios del derecho a la protección de datos", en José Luís Piñar Mañas (dir.), *Reglamento General de Protección de Datos: Hacia un nuevo modelo europeo de privacidad*, Madrid, Reus.

[154] DE LA QUADRA-SALCEDO FERNÁNDEZ DEL CASTILLO, Tomás (2018): "Retos, riesgos y oportunidades de la sociedad digital", en Tomás de la Quadra-Salcedo y José Luis Piñar (dirs.), *Sociedad digital y Derecho*, Madrid, BOE-Red.es, p. 78-79.

[155] RODOTÀ, Stefano (2014): *El derecho a tener derechos*, Madrid, Trotta.

con el dinamismo que exige el progreso. En efecto, la consideración de matices cambiantes, abstractos o sensitivamente complejos que respondan al sentir de la sociedad en cada momento es una cualidad humana que en la mayoría de las ocasiones no podrá ser trasladada a una máquina de manera sencilla.

De este modo, los resultados pueden contener sesgos imperceptibles o errores que conduzcan a resultados discriminatorios, incorrectos o que dejen fuera factores relevantes en el caso concreto.

3.2. Simplificación de la realidad

Bien es cierto que la capacidad actual de generar, recopilar, almacenar y tratar cantidades mayores de datos, de mayor variedad y de modos más precisos permiten mayor precisión en los procesos de "dataficación", o lo que en ocasiones ha sido referido como el paso de la realidad al bit. A pesar de ello, cualquier modelo de la realidad implica considerar solo una parte del contexto completo, y por tanto, parte de realizar una reducción. Por todo ello, es preciso que los responsables de las actividades de tratamiento, los desarrolladores de modelos, sistemas, aplicaciones o servicios, así como los agentes de toma de decisiones se hagan conscientes de la posibilidad de la existencia de errores en el modelo, del hecho de que todo modelo supone una simplificación de una realidad previamente dataficada. En palabras de Lorena Jaume Palasi, "por mucho que vistamos a la estadística de seda, estadística se queda".[156]

Por otro lado, es preciso resaltar que la búsqueda de correlaciones entre los datos responde, de nuevo, a métodos basados en la estadística que no conllevan causalidad. De este modo, es posible que dos variables de datos muestren una relación de manera tal que el comportamiento de una afecte al comportamiento de otra. Dichas relaciones podrán obedecer a relaciones de causalidad, pero también pueden responder al mero azar o a la

[156] JAUME-PALASÍ, Lorena (2018): en entrevista realizada por David Martínez Pradales, Nobbot, 2018. Disponible en: https://www.nobbot.com/general/etica-algoritmos-lorena-jaume-palasi/.

existencia de una tercera variable oculta que es la que realmente influye en el comportamiento observable.

3.3. Anonimización y seudonimización

En la medida en que lo relevante de este proceso es poder observar patrones de los datos, la identidad de la persona a la que se refieran generalmente no será relevante para el responsable. Por este motivo, en esta fase los datos personales pueden ser anonimizados, lo cual constituye una actividad de tratamiento de datos personales en sí misma, aunque desde el momento en que la anonimización se haya completado, el tratamiento de datos se encontrará fuera del ámbito de aplicación del RGPD-. En otras ocasiones, la anonimización no será posible o la funcionalidad del tratamiento puede requerir conocer la identidad de la persona o, al menos, un código de identificación. En dichos casos, los datos pueden ser seudonimizados, de modo que, a pesar de continuar siendo datos personales, aporten mayores garantías. De hecho, parece que la toma de consciencia del legislador europeo sobre la dificultad de alcanzar el estándar jurídico de anonimización (ver considerando 26 RGPD), así como de la mayor garantía que ofrece la seudonimización ha hecho que el RGPD contenga una declaración expresa que incentive dichos procesos de seudonimización. Así, el considerando 29 RGGPD establece que el responsable podrá llevar a cabo actividades de analítica de datos cuando estos hayan sido seudonimizados y existan otras medidas técnicas y organizativas que garanticen que la información adicional necesaria para re-asociar los datos con la identidad de cada persona se mantenga por separado. Estas medidas pueden incluir autorizaciones de acceso a los datos únicamente a personas concretas, establecer un control técnico sobre dichos accesos, implementar medidas de seguridad que garanticen que la información accesoria que permita la identificación directa de la persona no sea accedida ni de otro modo tratada, etc. Parece, de hecho, que el legislador abre así la puerta a realizar un análisis secundario de los datos, a pesar de no ser anónimos, en tanto existan medidas por las que la

persona que acceda a dichos datos no pueda atribuirlos a una persona y, por tanto, en ese contexto y momento concreto puedan asemejarse a datos anónimos.

3.4. Elaboración de modelos

El objetivo en esta fase es poder analizar los datos disponibles, descubrir nueva información e investigar posibles utilidades secundarias. Con ello, es posible identificar una nueva utilidad de los datos y realizar un modelo algorítmico. Por ejemplo, una organización puede analizar los datos históricos de sus interacciones con cada cliente y detectar de manera sorpresiva -sin haber previsto una posible relación entre variables y sin haber previsto una hipótesis-, que la combinación de diez factores ha indicado en el pasado el descontento del cliente con la organización y su baja. Algunos de dichos clientes contratan el servicio con un competidor mientras que otros simplemente causan baja. Este comportamiento de un grupo relativamente reducido de clientes de entre toda la masa de clientes de una gran organización puede no ser visible de manera evidente, cuanto menos, la capacidad de asociar este comportamiento a determinados factores específicos.

Para la determinación de esta circunstancia, típicamente se utiliza una muestra del conjunto de los datos sobre la que se realiza la analítica para encontrar correlaciones, detectar patrones y elaborar un modelo. El resto de los datos no utilizados en la elaboración del modelo se utilizan para evaluarlo. De este modo, se puede valorar la fiabilidad y desempeño del modelo mismo, compararlo con otros modelos y realizar cambios hasta conseguir que la probabilidad que muestra el modelo tenga un elevado nivel de confianza.

Ejemplo: detección de clientes insatisfechos

Imaginemos que una organización puede detectar que, en el pasado, la combinación simultánea de factores tales como que aquel usuario que contacta con el servicio de atención al cliente durante dos veces

al mes durante tres meses, unido a una calificación por debajo de 4 en la encuesta posterior sobre el servicio recibido, una bajada en x% en el nivel de consumo, etc. fue indicativa de que el cliente dio de baja su contrato en un plazo de un cuatrimestre si este era hombre de 30-39 años. La capacidad de detectar que ese patrón de comportamiento se repite en un número elevado de usuarios a lo largo del tiempo permite que el responsable pueda perfilar a los usuarios con riesgo alto de abandonar la organización. Con esta información, sería posible diseñar una estrategia por la que, cuando se observe ese comportamiento durante el primer mes, la organización pueda ponerse en contacto con el cliente y ofrecerle una promoción.

3.5. El resultado de esta fase no es dato personal

Los datos de origen utilizados para observar este patrón pueden ser anónimos o personales -en dicho caso, idealmente seudonimizados, tal y como adelantábamos-. Por su parte, el resultado de esta fase serán la definición de un perfil en abstracto que únicamente consista en determinar qué combinación de factores produce un resultado concreto con un nivel de confianza específico y un margen de error concreto. Esta información, de gran valor para una organización no es dato personal, pues en este momento no se atribuye esta información a ninguna persona en concreto.

En esencia, en esta fase, las herramientas de análisis de datos se pueden utilizar, no solo para detectar patrones y relaciones entre variables a partir de datos históricos, sino también acceder a nueva información y elaborar modelos predictivos así como la creación de nuevos productos o servicios a partir del nuevo conocimiento obtenido.

4. Fase 3 del big data: Aplicación del modelo

En esta fase se acciona el conocimiento obtenido en la Fase 2- Análisis en un entorno real. Hasta este momento, el modelo no había sido puesto en funcionamiento, sino únicamente creado, entrenado y testeado. En esta

fase se aplican los modelos creados en la fase anterior a individuos concretos para determinar en qué perfil encaja la persona, qué información nueva podemos obtener sobre ella y qué decisiones relativas a dicha persona se pueden tomar en consecuencia.

En muchas ocasiones esta fase requiere que los datos personales que se refieren a un individuo se introduzcan en el modelo. Generalmente se trata de una pequeña cantidad de información obtenida directamente del individuo u observable sobre este. Esta es combinada con una gran cantidad de información que no proviene del individuo: todos aquellos datos originados en la Fase 1-Recopilación y que fueron utilizados en la Fase 2-Análisis, junto con el conocimiento secundario creado en la Fase 2 para obtener un resultado sobre el que se toman decisiones. Esto tiene consecuencias en la medida en muchas de las decisiones que afecten al individuo se toman sobre la base de una gran cantidad de información proveniente de diversas fuentes y de otras personas a través de modelos de alta complejidad.

Esta fase sí entraña un tratamiento de datos personales. En primer lugar, de aquellos datos obtenidos u observados del individuo que se introducen en el modelo. En segundo lugar, aquella información que se infiere del individuo y que sirve en gran medida para predecir su comportamiento, gustos o situación y tomar decisiones sobre él. Por ello esta fase entraña riesgos mayores en términos de protección de derechos de los individuos.

Retomando el ejemplo anterior sobre el desarrollo de un modelo de detección de señales de insatisfacción de clientes que predicen cuándo se marcharán de una compañía. Esta fase supondría que los datos recabados sobre los clientes son insertados en el modelo para determinar si cada uno de ellos a título personal muestra síntomas de descontento. De este modo, la organización podrá saber que el cliente con código 284620YT muestra síntomas leves de enojo. Es decir, podemos categorizarle en el perfil de “clientes con riesgo medio de abandono”, ya que comparte determinadas características con un grupo más amplio de clientes que tuvieron una tasa

moderada de x% de causar baja. Para revertirlos, la compañía puede decidir llamarle y mostrar de manera proactiva una atención personalizada.

Por otro lado, el cliente 786204HO es categorizado dentro del perfil de "clientes con riesgo muy alto de abandono" en función de aquellos otros factores que comparte con clientes que mostraron en el pasado un determinado comportamiento. En este caso, la compañía puede analizar además, si el cliente es solvente, tiene riesgo de impago, etc. Con esta información, el perfil de la persona se enriquece: "otros clientes que en el pasado han mostrado este comportamiento abandonaron la compañía causando una disminución de rentabilidad"; "otros clientes que en el pasado han mostrado este comportamiento y que además son categorizados como malos pagadores abandonaron la compañía y ello supuso una mejora en la ratio de impagos". En función del perfil o perfiles finales en los que pueda incluirse a cada persona, pueden inferirse otras características sobre él que, a pesar de que no sean observables para este cliente en concreto, lo fueron para otros. Con todo ese conocimiento, la compañía puede decidir no atender al cliente descontento y dejarle marchar, ofrecerle un nuevo plan de contratación con un descuento, ofrecerle otro tipo de incentivos, etc.

Es decir, en esta fase se elaboran perfiles detallados de cada persona, que la definen y aportan información adicional sobre esta. Estos perfiles ya constituyen un tratamiento de datos personales y una toma de decisiones (automatizada o no) que afecta al cliente. Por ello, esta es la fase en la que se prevé, por ejemplo, la personalización de servicios.

De modo similar, sería posible conocer en qué nivel exacto de solvencia crediticia de los 100 que podría haber previsto una organización se puede incluir a una persona concreta en relación con servicios bancarios y decidir acerca de la concesión de un crédito el nivel de intereses o las garantías que se le exijan. También es posible detectar comportamientos indicativos de fraude y denegar la realización de una operación, etc.

Quizás lo más relevante en este momento es diferenciar claramente entre la configuración de un perfil y la creación de un modelo algorítmico (es

decir, la determinación de las características, comportamientos, variables y factores que identifican la probabilidad de que se suceda un resultado específico; lo cual se realiza en la Fase 2- Análisis), con la aplicación de dicho perfil y modelo (lo cual se realiza en la Fase 3- Aplicación). Por ello mismo, es necesario reconocer claramente que existen dos grupos de personas que típicamente pueden confundirse. En primer lugar, las personas cuyos datos son recopilados en la Fase 1-Recolección, y las personas sobre las que se aplica el modelo en la Fase 3-Aplicación. En ocasiones, puede haber personas que estén presentes en ambos grupos, sin embargo, esto no tiene que ser necesariamente así. En todo caso, el rol de cada grupo es diferente, y por tanto el tratamiento jurídico de las personas en cada fase será también diferente.

4.1. Creación de perfiles[157]

El art. 4.4 RGPD define la elaboración de perfiles como "toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física" (énfasis añadido).

Por su parte, el Consejo de Europa se refiere a la actividad de perfilado como la aplicación a un individuo concreto del perfil que caracteriza a un grupo con el que se puede identificar a partir de los datos recogidos sobre él. Este proceso, por tanto, conlleva la creación de nuevos datos personales,[158] pues nuevas características son inferidas del individuo que es perfilado únicamente por el hecho de compartir otras características que

[157] Parte del contenido de esta sección ha sido objeto de publicación en GIL GONZÁLEZ, Elena; De HERT, Paul (2019): "Understanding the legal provisions that allow processing and profiling of personal data—an analysis of GDPR provisions and principles", en *ERA Forum*. Vol. 19. No. 4. Springer Berlin Heidelberg, p. 597-621.

[158] CONSEJO DE EUROPA (2010): *The protection of individuals with regard to automatic processing of personal data in the context of profiling, Recommendation CM/Rec (2010) 13 and explanatory memorandum*, de 23 de noviembre.

sí son observables. El riesgo de ello es considerar que los nuevos datos personales asumidos sobre la persona tienen carácter de certeza absoluta, pues en la medida en que se basan en probabilidad estadística, siempre existe un margen de incertidumbre.

Es por ello que el resultado de realizar inferencias a partir de un conjunto rico de datos, así como de la agregación de datos de un subgrupo de la población[159] cada vez más amplio tiene más probabilidad de certeza que las inferencias realizadas a partir de menos atributos o de atributos de un grupo más reducido de población.[160] Por este motivo el análisis de datos masivos resulta tan interesante: permite realizar asunciones sobre la realidad mucho más certeras, con menos error. Esta precisión tiene un valor económico. Y es de hecho, la mayor precisión en el cálculo de probabilidades y la granularidad de las conclusiones lo que subyace a la economía de los datos actual.

En este sentido, quizás el tipo de perfilado más relevante por sus consecuencias y por ser quizás el más frecuente es el perfilado no distributivo de grupos. En este, no todos los individuos del grupo presentan absolutamente todas las características, pero son tratados como si así fuera.

Por ejemplo, el sector bancario utiliza de manera intensiva actividades de perfilado de sus clientes para calcular su tasa de riesgo y otorgarle una calificación crediticia. Para ello, la institución bancaria analiza grandes cantidades de información, tanto proveniente de sus clientes como del mercado y otras fuentes de manera que puedan identificar qué variables predicen la probabilidad de riesgo de impago. De este modo, cuando un nuevo cliente solicita un préstamo, un crédito u otro producto, el banco recoge datos relativos a la persona en concreto, los introduce en su modelo

[159] CONSEJO DE EUROPA (1973): *Explanatory Report to: Council of Europe - Committee of Ministers, Resolution (73) 22 on the Protection of the Privacy of Individuals Vis-à-Vis Electronic Data Banks in the Private Sector*.

[160] GARRETT, Thomas A. (2003): "Aggregated versus disaggregated data in regression analysis: implications for inference", en *Economics Letters*, Vol. 81, No. 1, p. 61-65.

e infiere otras características sobre él que determinan su calificación final. Este proceso incluye un margen de error en la medida en que se aplican datos pasados de otras personas para predecir el comportamiento futuro de este cliente. Así, el posible que la institución bancaria deniegue la concesión de un préstamo por el hecho de que el resultado de la Fase 3-Aplicación muestra como resultado que el individuo pertenece a un perfil asociado a una baja calificación. Ello puede suceder incluso a pesar de que dicho individuo no haya incurrido en situaciones de impago con anterioridad.

En palabras de Vedder, "la información contenida en el perfil o generalización contempla a los individuos como miembros de un grupo; no contempla a los individuos como tales".[161]

El tratamiento de datos personales en esta fase entraña riesgos que el RGPD ha tomado en consideración. Así por ejemplo, el art. 22 regula la toma de decisiones automatizadas, incluida la elaboración de perfiles. De hecho, el considerando 71 RGPD indica que en relación con la elaboración de perfiles o la toma de decisiones automatizadas cuyos efectos puedan tener un efecto significativo sobre el interesado, el tratamiento debe estar sujeto a garantías. Entre ellas, el RGPD incluye los deberes de información al interesado o el derecho a obtener intervención humana, aunque también cabrían añadirse deberes específicos sobre el proceso de creación y modelado del sistema de perfilado como que garanticen la veracidad de la información con la que se alimenta el modelo, entre otras.

5. Conclusiones

Las herramientas de análisis de datos se pueden utilizar, no solo para detectar patrones y relaciones entre variables a partir de datos históricos, sino también acceder a nueva información y para elaborar modelos predictivos. Más aún, el potencial de los datos puede utilizarse tanto para

[161] VEDDER, Anton (1999): "KDD: The challenge to individualism", en *Ethics and Information Technology*, Vol. 1, No. 4.

mejorar la toma de decisiones internas de la compañía como para la creación de nuevos productos o servicios basados en datos. De hecho, en los últimos años se observa una clara tendencia hacia la comodificación de servicios basados en datos. De este modo, los datos han pasado de ser un factor residual de una actividad principal, a convertirse en el centro de valor de los modelos de prestación de servicios a ser el objetivo principal de monetización, relegando la creación de valor real para el usuario a un segundo plano.

Uno de los grandes riesgos de este cambio de tendencia es la oferta de productos o servicios, en muchas ocasiones a través de internet y sin contraprestación económica, cuya finalidad real no es la satisfacción de una necesidad del usuario, sino la de servir de medio para la creación y recolección de datos que puedan posteriormente monetizarse. Ello explica las solicitudes de recolección de información no necesaria para la prestación de servicios, la inclusión de todo tipo de sensores en objetos o el desarrollo de prácticas oscuras que abarcan desde la mera creación de datos y su tratamiento posterior.

Por su parte, los procesos big data implican, por su propia naturaleza, la imposibilidad de predecir los resultados de la analítica de datos e incluso la dificultad de comprender cómo funcionan los modelos analíticos.

Tampoco debemos olvidar que el conjunto de tecnologías big data crean un reto de equilibrio entre beneficios y riesgos. Por un lado, la mayor fuente de beneficios de los datos surge, hoy en día, cuando estos son agregados en grandes cantidades de modo que representen contextos cada vez más completos de la realidad. Esto permite, a su vez, utilizar el análisis de datos para obtener información nueva, dando como resultado un nuevo ciclo de creación de más y más datos. Por otro lado, no obstante, la acumulación de datos y su agregación es fuente de riesgos[162] derivados de poder adquirir un nivel de comprensión de cada individuo sin precedentes. No solo

[162] SOLOVE, Daniel (2006): “A Taxonomy of Privacy”, en *University of Pennsylvania Law Review*, Vol. 154.

eso, la capacidad de adquirir conocimiento de la masa de individuos a nivel colectivo es, quizás, uno de los mayores riesgos. En efecto, el conocimiento de la colectividad permite llevar a cabo acciones coordinadas que pueden provocar la manipulación del comportamiento o la erosión de libertades de modos que pasan más desapercibidos porque no son detectados por cada individuo a título particular.

En esencia, los proyectos que conllevan el uso de tecnologías big data, procesos de análisis de volúmenes masivos de datos resultan complejos e impredecibles de un modo que no ocurría con anterioridad. Todo ello dificulta que el interesado comprenda qué tipo de datos se recoge sobre él, cómo se tratan y qué consecuencias tendrán dichos procesos. En resumen, existe un problema creciente de asimetrías de información entre la persona y los proveedores de servicios y responsables, que se refleja en la cantidad de información creada y recolectada, así como en los medios a través de los cuales se tratan dichos datos.[163] Como consecuencia, el control que se puede ejercer sobre las personas a través de la captación y tratamiento de sus datos forja poderes cada vez más centralizados y a su vez una disminución de derechos que deben ser adecuadamente reequilibrados.[164]

A pesar de ello, el interesado sigue sometido diariamente y de manera constante a cláusulas informativas y modelos de consentimiento. En esta situación, las relaciones entre el hombre y las máquinas deben ser consideradas desde la dimensión del Derecho.[165]

En el capítulo siguiente analizaremos la figura del consentimiento, algunos de los problemas que ha mostrado tener en entornos digitales, especialmente en aquellos de alta complejidad como los que son objeto de este trabajo, y la respuesta que ha dado el RGPD.

[163] AUSLOOS, Jeff (2018): The Right to Erasure in EU Data Protection Law, Oxford University Press.

[164] RODOTÀ, Stefano (2016): “Internet and Privacy: There Is a Judge in Europe Who Curbs the United States”, en *The Federalist Debate*, No. 1.

[165] RODOTÀ, Stefano (2014): El derecho a tener derechos, Madrid, Trotta.

CAPÍTULO IV. CONSENTIMIENTO

"Para que no pueda abusarse del poder es preciso que, por la disposición de las cosas, el poder contenga al poder ".[166]

1. Introducción

Tal y como adelantamos en el Capítulo II, el desarrollo jurídico del derecho a la protección de datos personales ha otorgado una importancia crucial al consentimiento del individuo desde sus inicios. Quizás el motivo principal de ello sea el hecho de que el consentimiento permite al individuo ostentar un poder de elección sobre si autorizar o no el tratamiento de los datos personales que se refieren a este. La lógica subyacente es que el consentimiento es el instrumento que nos permite manifestar una decisión consciente, razonada y a la que llegamos de manera autónoma y voluntaria.

A pesar de ello, el consentimiento nunca fue considerado el único instrumento con el que debía contar el Derecho de protección de datos para legitimar el tratamiento de datos personales ni para ofrecer protección al individuo frente a posibles usos o abusos en el tratamiento de estos. En este sentido deben leerse las Directrices sobre privacidad y flujo transfronterizo de datos de la OCDE (1980) y el Convenio No. 108 (1981) que han servido de base para la creación normativa de las décadas posteriores, como la Directiva protección de datos personales de 1995 (Directiva 95/46), la Carta de Derechos Fundamentales de la UE de 2000 y el actual RGPD. Por otro lado, sin embargo, el desarrollo normativo en el ámbito específico de las comunicaciones electrónicas, que actualmente se encuentra en la Directiva e-Privacy, confía en el consentimiento para la legitimación de aquellos tratamientos no necesarios, y la propuesta de

[166] Barón de MONTESQUIEU (1748): *Del espíritu de las leyes*.

futuro Reglamento e-Privacy, que se espera sustituya a la Directiva, también se orienta en el mismo sentido.[167]

En este capítulo examinaremos la figura del consentimiento tal y como ha sido regulada en la Directiva 95/46, el RGPD y el marco de protección de comunicaciones electrónicas. El objetivo es realizar un análisis crítico sobre la idoneidad de situar al consentimiento en el centro del sistema de protección del individuo cuando este actúa en entornos digitales como los descritos en el Capítulo III: esto es, donde existen tratamientos de datos personales a gran escala, de manera constante, de alta complejidad y los resultados de cuyas analíticas resultan imprevisibles.

Los principios relativos al tratamiento de datos personales se encuentran descritos en el art. 5 RGPD, que viene a actualizar el ya derogado art. 6 Directiva 95/46. En concreto, el art. 5.1.a) RGPD establece que los datos personales deban ser tratados de manera lícita, leal y transparente en relación con el interesado; esto es, rescata los principios de licitud y lealtad de la Directiva 95/46, y consagra por primera vez de forma expresa el principio de transparencia. En relación con el principio de licitud, el art. 8.2 de la Carta de los Derechos Fundamentales de la UE indica en su art. 8.2 que el responsable debe contar con una base que legitime el tratamiento de datos personales.

1.1. Las seis bases de legitimación

Por su parte, el art. 6 RGPD -y antes que este, el art. 7 de la Directiva 95/46- desarrolla el principio de licitud, y exige que se aprecie al menos una de las seis bases de prevé para que una operación de tratamiento de datos

[167] Al menos, esto es cierto para la propuesta de Reglamento e-Privacy de la Comisión y la propuesta enmendada del Parlamento. Al momento de finalización de este trabajo (junio de 2020) el texto final del Consejo no se conoce, de modo que, con carácter general, no será tomado en consideración. Este aspecto se desarrolla en más detalle en una sección posterior de este capítulo.

personales de los interesados[168] sea considerada lícita. Descritas de manera sucinta, estas bases son:

- Consentimiento (art. 6.1.a): el interesado debe manifestar su conformidad para el tratamiento de datos personales con una o varias finalidades específicas.
- Contrato (art. 6.1.b): el tratamiento de los datos es necesario para la ejecución de un contrato en el que el interesado es parte o para la realización de acciones precontractuales a petición de este.
- Obligación legal (art. 6.1.c): el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento, diferente de aquellas obligaciones que se derivan de un acuerdo contractual.
- Intereses vitales (art. 6.1.d): el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física.
- Interés público (art. 6.1.e): el tratamiento de datos personales es necesario para el desempeño de una función de interés público o en el ejercicio del poder público, cuando estas sean previstas por ley.
- Interés legítimo (art. 6.1.f): el tratamiento es necesario para satisfacer un interés legítimo del responsable del tratamiento o un tercero, salvo que sobre estos intereses prevalezcan los intereses o derechos y libertades fundamentales de interesado. Esta base de licitud no será de aplicación si el responsable del tratamiento es una autoridad pública en ejercicio de sus funciones.

[168] De manera interesante, Borja Adsuara destaca varios aspectos respecto del término español “interesado” y el inglés “data subject”. En primer lugar, pareciera que la traducción española amplía el concepto original de sujeto, que en rigor, no es lo mismo, pues se puede estar interesado por unos datos personales a pesar de no ser sujeto de derecho respecto de ellos. En cualquier caso, creemos que esta traducción no amplía ni modifica las consecuencias jurídicas del término. En segundo lugar, destaca el hecho de que la versión ingles utiliza un lenguaje “políticamente correcto desde el punto de vista de género”, pues se refiere a *he or she*, cosa que no sucede en la versión oficial española, en la que se utiliza el término genérico “interesado”. ADSUARA VALERA, Borja (2016): “El consentimiento”, en José Luís Piñar Mañas (dir.), *Reglamento general de protección de datos. Hacia un nuevo modelo europeo de privacidad*, Madrid, Reus, p.151-170.

Si bien el RGPD sigue un carácter continuista respecto de la anterior Directiva, las autoridades públicas han sufrido uno de los cambios más relevantes. Bajo el RGPD deben acudir en primer lugar al interés público para la mayor parte de sus tratamientos, y ostentan un margen más limitado para confiar en el consentimiento del interesado o los intereses legítimos propios o de terceros.

1.2. No existe jerarquía entre las bases

Como se aprecia, el consentimiento es solo una de las múltiples bases que permiten legitimar el tratamiento de datos personales.[169] Ninguna base puede ser considerada con carácter general "mejor" que otras ni existe jerarquía entre las seis. Especialmente importante es recalcar que esta falta de jerarquía es fruto de una decisión consciente del legislador europeo. Muestra de ello es que, de hecho, la primera propuesta de Directiva de protección de datos presentada por la Comisión Europea el 27 de julio de 1990 sí establecía en su art. 8.1 el consentimiento como una suerte de base de legitimación principal para el tratamiento de datos en el sector privado, sujeto a excepciones .concretamente, la existencia de una relación contractual, el interés legítimo del responsable o que los datos se encontrasen en fuentes accesibles al público-.[170] Sin embargo, durante la tramitación legislativa de la Directiva este criterio fue modificado hasta su

[169] En realidad, afirmación no resulta pacífica. Este principio de no jerarquía podría resultar más directo desde el punto de vista del Derecho comunitario la interpretación de la Directiva de protección de datos y el RGPD. Sin embargo, como veremos más adelante al hablar de interés legítimo, la tradición jurídica en España y la trasposición de la Directiva al ordenamiento interno marcó claras diferencias en este aspecto en concreto. Como consecuencia, una parte de la doctrina española más autorizada opina que la base de licitud del consentimiento debería ser vista como la regla general, mientras que las demás bases de licitud serían excepciones: "No estamos de acuerdo con este enfoque (…) pues se pone al mismo nivel la regla que las excepciones; y creemos que ha de destacarse, por encima de todo, el principio de libertad y autodeterminación respecto de los propios datos". ADSUARA VALERA, Borja (2016): "El consentimiento", en José Luís Piñar Mañas (dir.), *Reglamento general de protección de datos. Hacia un nuevo modelo europeo de privacidad*, Madrid, Reus, p.151-170.

[170] COMISIÓN EUROPEA (1990): *Proposal for a Council Directive concerning the protection of individuals in relation to the processing of data* (COM(90) 314 final), de 27 de julio. Disponible en: https://resources.law.cam.ac.uk/cipil/travaux/data_protection/1%2027%20July%201990%20Proposal.pdf.

expresión final por la que el consentimiento pasa a ser únicamente una alternativa más de entre las varias existentes sin rango de jerarquía entre ellas, criterio que ha mantenido el RGPD.

Así, como ha sido reconocido por el GT29 en sus opiniones sobre el consentimiento[171] y sobre el interés legítimo,[172] el orden en el que aparecen listados en el RGPD (y antes de él, en la Directiva 95/46) no tiene consecuencias jurídicas. En consecuencia, no se podría argumentar, por ejemplo, que el hecho de que el interés legítimo aparezca en último lugar en el art. 6.1 RGPD signifique que únicamente deba ser utilizado en casos excepcionales.

De este modo, parecería que pudiera concluirse que, de acuerdo con esta enumeración, una gran parte de los tratamientos de datos personales estarán legitimados en alguna de las bases dispuestas en los aparatados b-f) del artículo.[173] Y sin embargo, como será desarrollado más adelante, la experiencia indica que el consentimiento se ha considerado una pieza clave en la aplicación de las normas de protección de datos y así también lo ha expresado la doctrina al calificarlo de piedra angular.[174]

1.3. Una triple clasificación

Por su parte, en relación con este listado de bases de legitimación, el Abogado General del Tribunal de Justicia de la Unión Europea en el caso Rigas[175] señalaba que estas pueden clasificarse en tres tipos de bases. En

---

[171] GRUPO DE TRABAJO DEL ARTÍCULO 29 (2011): *Dictamen 15/2011 sobre la definición del consentimiento* (WP 187), de 13 de julio; COMITÉ EUROPEO DE PROTECCIÓN DE DATOS (2018): *Guidelines on consent under Regulation 2016/679* (WP259 rev.01), de 10 de abril.

[172] GRUPO DE TRABAJO DEL ARTÍCULO 29 (2014): *Dictamen 06/2014 sobre el concepto de interés legítimo del responsable del tratamiento de los datos en virtud del artículo 7 de la Directiva 95/46/CE* (WP 217), de 9 de abril, p.10.

[173] BYGRAVE, Lee A. (2002): *Data Protection Law: Approaching Its Rationale, Logic and Limits*, Kluwer law international, p. 66.

[174] FERRETTI, Federico (2012): "A European perspective on data processing consent through the re-conceptualization of European data protection's looking glass after the Lisbon Treaty: taking rights seriously", en *European Review of Private Law*, No. 2, p- 484.

[175] TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA (2017): Asunto C-13/16, Rïgas, Opinión del Abogado General, de 26 de enero. ECLI:EU:C:2017:43, párrafos 56-57.

primer lugar, el consentimiento del interesado del apartado a) conformaría una categoría propia. En segundo lugar, las bases descritas en los apartados b)-e), en las que los intereses del responsable del tratamiento se presumen. Por último, la base del apartado f) en la que los intereses legítimos del responsable no se presumen, sino que su existencia debe probarse, y además deben ganar un juicio de ponderación contra los intereses y libertades de los interesados. De este modo, el ámbito de aplicación del artículo 6.1. f) RGPD es amplio y está descrito en términos abiertos. Sin embargo, debe someterse a un juicio de ponderación, requisito que no se exige para la aplicación de otras bases de legitimación.

1.4. La importante decisión de la elección de la base

La selección de la base de legitimación para cada una de las finalidades del tratamiento puede llegar a ser una de las decisiones más delicadas para el responsable del tratamiento. Todo ello, paradigmáticamente, a pesar de que no se trate de una cuestión para nada novedosa. Efectivamente, las seis bases de legitimación recogidas en el art. 6 RGPD han permanecido prácticamente inalteradas con respecto a la Directiva 95/46. Dicha elección debe producirse antes del inicio del tratamiento, y debe quedar documentado, pues, entre otras cosas, el responsable está obligado a informar al interesado de forma clara y transparente sobre la base del tratamiento conforme a los arts. 13 y 14 RGPD. Asimismo, el cambio de base de legitimación a posteriori puede implicar que el responsable incurra en incumplimiento del RGPD, sujeto a una correspondiente sanción económica.

Como normal general, el tratamiento realizado para una finalidad concreta no podrá sostenerse en varias bases alternativas. Lo contrario produciría situaciones en las que el uso de una base de legitimación es ficticio. Así por ejemplo, si un tratamiento de datos para una finalidad concreta pudiera ser basado en el consentimiento del interesado y al mismo tiempo en un interés público, la capacidad de decisión otorgada al individuo para no aceptar el tratamiento sería una mera ilusión. Del mismo modo, por

ejemplo, el responsable no podrá considerar con carácter retroactivo que un tratamiento de datos concreto estaba basado en el interés legítimo cuando se enfrente a un problema de validez del consentimiento.

Lo que sí es posible, en cambio, en la medida en que un mismo dato personal pueda utilizarse para diferentes finalidades es que el tratamiento de un mismo dato personal sí pueda legitimarse sobre diferentes bases. Esto es relevante porque, de hecho, las finalidades de los datos son cada día más abundantes. Así por ejemplo, un conjunto de datos personales utilizados por un comercio minorista para el cobro de una compra mediante pago electrónico también podrá ser utilizado, siempre en cumplimiento de todas las obligaciones del RGPD y con la adecuada base de legitimación, para finalidades de analítica de datos.

Asimismo, de esta decisión también dependerán los derechos que resulten una prerrogativa para el interesado. Por ejemplo, el interesado únicamente dispone de un derecho a la portabilidad de sus datos bajo el RGPD cuando la base de legitimación es su consentimiento o la ejecución de un contrato; mientras que el derecho de oposición únicamente se da -con limitaciones- cuando el tratamiento se basa en el interés público o el interés legítimo. Por todo ello, la elección de la base de legitimación es un proceso delicado que puede convertirse incluso en un aspecto más de la estrategia de gobernanza de datos de la organización, de necesario estudio por parte de todos los agentes relevantes: el propio responsable, el equipo jurídico, etc.

Para el sector privado, la mayor parte de las operaciones de tratamiento pueden legitimarse mediante, al menos, una de las siguientes tres bases: consentimiento, contrato o interés legítimo. En este capítulo centraremos el énfasis en el estudio del consentimiento y la necesidad del tratamiento para la ejecución de un contrato o precontrato.

2. Los estándares del consentimiento

El análisis del consentimiento puede realizarse desde diferentes prismas. Por un lado, el consentimiento en sentido material es un medio de

expresión de la voluntad libre y autónomamente creada de la persona. Por otro lado, el reflejo de ello en la norma da como resultado el consentimiento en un sentido formal, compuesto por aquellos requisitos mínimos con que el legislador califica cuándo dicha expresión volitiva es jurídicamente válida. Como derivada de ello, aquí se propone un análisis del consentimiento en tanto instrumento de la normativa de protección de datos personales realizado sobre la base de tres estándares diferentes, cada uno de los cuales complementa a los demás, pero también muestra sus propias limitaciones.

2.1. Estándar del interesado medio razonable

Este define aquellos elementos del consentimiento que, con carácter general, se exigen en la norma para considerar que el interesado realmente ha expresado su voluntad. En otras palabras, es aquél estándar que debería reflejar formalmente la intención material del consentimiento desde el punto de vista de aquél que lo presta. Así pues, se trata de facto de la definición de consentimiento dada por el RGPD y los elementos formales que lo componen.

Para ello, el punto de referencia de quién otorga su consentimiento debe ser un “interesado medio razonable”, es decir, el usuario tipo objetivo del producto o servicio que presenta las características que razonablemente puedan suponerse del grupo que debe prestar su consentimiento. En este sentido, por ejemplo, el nivel de comprensión sobre el acto del consentimiento y las consecuencias que pueda deducirse al interesado medio de un videojuego infantil será muy diferente de aquél que se pueda exigir al usuario medio de un software orientado a juristas. Este hecho debe orientar al responsable en el modo de presentar la información relevante o incluso de considerar si el consentimiento debe ser la base de licitud del tratamiento más adecuada para un tratamiento concreto.

En esencial, el estándar del interesado medio razonable hace referencia a los requisitos que, con carácter genérico, debe reunir el consentimiento para cada actividad y finalidad de tratamiento.

2.2. Estándar subjetivo del interesado

En segundo lugar, el estándar subjetivo del interesado pretende observar qué otros aspectos adicionales necesitarían un interesado en particular para poder concluirse que ha podido ejercer su capacidad de expresión de la voluntad. Este pretende identificar posibles limitaciones por las que, a pesar de que los requisitos formales del consentimiento se estén cumpliendo, no puede considerarse que un interesado está siendo realmente capaz de tomar su propia decisión. En otras palabras, indica aquellas condiciones por las que, desde el punto de vista del interesado, se cumple la función formal pero no material del consentimiento.

2.3. Estándar del responsable medio razonable

Por último, este estándar muestra a la contraparte, aquél que solicita el consentimiento y debe garantizar el cumplimiento de los requisitos formales, así como las limitaciones potenciales que pueden suceder.

En un escenario ideal estos tres estándares deberían coincidir. Sin embargo, como se desarrollará en las próximas páginas, existen algunas limitaciones en relación a cómo ejecutar en la práctica los requisitos formales del consentimiento, cómo asegurar que un interesado ha sido realmente capaz de formar su voluntad y expresarla y cómo el responsable puede tener dificultades para cumplir con el estándar del consentimiento o incluso incentivos para no hacerlo.

3. Estándar del interesado medio razonable en el consentimiento

Como se adelantaba, el estándar del interesado medio razonable es la expresión formal de los elementos que permiten considerar, con carácter genérico, que un interesado ha podido comprender las circunstancias del tratamiento de datos personales, elaborar una opinión al respecto y manifestar su decisión. Por ello, en términos sencillos, se trata de cómo la norma define y regula el consentimiento.

El consentimiento se ha convertido en la piedra angular de la protección de datos en toda la UE, debido a la doble promesa de que por un lado permite legitimar el tratamiento de datos, y por otro mantiene la autonomía individual en la toma de decisiones. ¿Cuál es esta expresión formal de la que hablamos?

3.1. El consentimiento en la Directiva 95/46

La Directiva 95/46 define el consentimiento del interesado como toda manifestación de voluntad, libre, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernan (art. 2.h), que debe se prestado de manera inequívoca (art. 7.a). Uno de los problemas de la Directiva era la falta de armonización entre Estados miembros, que en el caso del consentimiento tomaba la forma de diferentes interpretaciones sobre los mismos requisitos. Por ejemplo, mientras algunos Estados miembros requerían la prestación del consentimiento por escrito, otros aceptaban su manifestación de manera tácita, exigiendo que fuera explícito únicamente cuando se refiriese a categorías especiales de datos (tales como datos referentes a la salud, el origen racial o étnico de la persona, o su orientación sexual).

Estos atributos han sido ampliamente discutidos y desarrollados, tanto por la doctrina, el Grupo de Trabajo del Artículo 29 (ahora Comité Europeo de Protección de Datos, CEPD), las resoluciones de cada autoridad de control en los Estados miembros y la jurisprudencia del TJUE.

A pesar de todo, durante los años de vigencia de la Directiva emergieron las dudas y críticas sobre el insuficiente grado de protección que aportaba el consentimiento, al menos bajo la redacción dada por la propia Directiva. Incluso la Comisión Europea señaló esta falta de concreción y la necesidad de que el RGPD clarificase los requisitos durante los análisis previos a la primera propuesta de Reglamento.[176] Estas críticas partían de una

[176] COMISIÓN EUROPEA (2010): *A comprehensive approach of data protection in Europe (COM 2010)*, de 4 de noviembre, p. 7-9. Disponible en: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0609:FIN:EN:PDF.

aparente desconexión entre la presunción de que el consentimiento es una manifestación de una elección consciente y razonada y la realidad práctica que contradecía estas asunciones. Es decir, ya antes de la elaboración del RGPD, la Comisión Europea mostraba su preocupación por una posible falta de coherencia en relación con el estándar del interesado medio razonable.

3.2. El consentimiento en el RGPD

Como consecuencia, el RGPD tenía como fin ser el medio por el que se reforzaran los requisitos del consentimiento con el objetivo de aumentar la capacidad de autonomía del interesado.

Así, el art. 4.11 RGPD define como consentimiento del interesado "toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen". De este modo, el RGPD indica que el acto de aceptación deba darse mediante una declaración o clara acción afirmativa, esto es, que deba ser expreso o manifestarse a través del tipo de prácticas conocidas como *opt-in* o fórmulas equivalentes. Es decir, con la aplicación del RGPD el consentimiento tácito ya no resulta válido, de modo que el silencio del interesado, las casillas pre-marcadas o la inacción no pueden legitimar ya el tratamiento de los datos personales. Por último, en lo que se refiere a los datos sensibles, se añade que el consentimiento deba ser explícito (art. 9.1.a), esto es, confirmado mediante la palabra, no mediante otro tipo de acción positiva.

Cuando el tratamiento tenga varios fines, debe darse el consentimiento para todos ellos. Asimismo, el RGPD aplica los principios de transparencia a la prestación del consentimiento de modo que para considerar que el consentimiento es válido, el RGPD también exige que su solicitud se presente de forma diferenciada de los demás asuntos, de fácil acceso, y en un lenguaje claro y sencillo. Del mismo modo, el interesado podrá retirar su consentimiento en cualquier momento, debiendo ser tan fácil retirarlo como

fue darlo.[177] Todo ello es aún más importante en el contexto actual de la Internet de las Cosas, la publicidad basada en el comportamiento y la aparición de modelos de negocio basados en la monetización de los datos de las personas, que se basan en gran medida en obtener el consentimiento del interesado para la recopilación y análisis de sus datos por parte del propio responsable y de terceros, así como para la personalización de servicios.

Del mismo modo, los artículos 7 y siguientes establecen diferentes medidas tendentes a hacer más estricto el proceso de otorgar el consentimiento. En este sentido, se establece que el responsable del tratamiento deberá ser capaz de demostrar que el interesado consintió el tratamiento de sus datos personales. Para ello, cobrará importancia para las organizaciones revisar los sistemas de registro del consentimiento de modo que sea posible aportar evidencias ante una auditoría o un procedimiento de la autoridad de control o acción judicial. La solicitud de consentimiento deberá presentarse diferenciada de los demás asuntos, de fácil acceso, utilizando un lenguaje claro y sencillo.

De hecho, con la entrada en aplicación del RGPD el 25 de mayo de 2018, todos los tratamientos que estuvieran basados en un consentimiento tácito devendrían inválidos. En esta situación, los responsables del tratamiento debían buscar una base legal para continuar con el tratamiento, o requerir de nuevo un consentimiento que cumpliera las nuevas garantías, circunstancia que causó la recepción de un volumen de comunicaciones sin precedentes por las que se solicitaba la renovación del consentimiento de los usuarios, o la información sobre qué nueva base de legitimación se aplicaría a partir de dicho momento. Ello ejemplifica cómo, bajo la Directiva, el consentimiento se utilizaba como base de legitimación por defecto a

[177] Bajo esta redacción, el interesado tiene la potestad de retirar el consentimiento en cualquier momento sin necesidad de argumentar los motivos de su decisión. Esto supone un avance en las garantías de los interesados respecto de la redacción anterior dada por la norma española, que establecía que el consentimiento podría ser revocado "cuando exista causa justificada para ello". ADSUARA VALERA, Borja (2016): "El consentimiento", en José Luís Piñar Mañas (dir.), *Reglamento general de protección de datos. Hacia un nuevo modelo europeo de privacidad*, Madrid, Reus, p.151-170.

pesar de que pudiera no ser la más adecuada. El consentimiento sólo es adecuado si el responsable del tratamiento puede ofrecer a los particulares una verdadera posibilidad de elección sobre la aceptación o no del tratamiento, así como control y responsabilidad sobre el uso de sus datos personales. Esto es, el objeto de la aplicación normativa debe ser que redacción formal del consentimiento coincida con el contenido material de este. Si el responsable debe realizar el tratamiento de datos a pesar de la no aceptación por parte de los interesados, pedir el consentimiento sería "engañoso e intrínsecamente injusto".[178] En tal caso, el responsable del tratamiento deberá utilizar otra base de legitimación.

En resumen, parece que el modelo de consentimiento bajo el RGPD es continuista respecto de la Directiva 95/46 en sus aspectos más importantes, en el sentido de que mantiene los requisitos principales que ya se encontraban en la Directiva 95/46. Por otro lado, sin embargo, el RGPD ha reforzado a figura del consentimiento. En primer lugar, mediante el endurecimiento de los requisitos ya existentes, siendo un claro ejemplo de ello la ampliación de la información que el responsable debe aportar y que está directamente relacionada con el consentimiento informado, que incluye la obligación de comunicar al interesado su derecho a retirar el consentimiento. En segundo lugar, mediante la incorporación de cambios con el ánimo de que supongan garantías adicionales. Entre ellas, la necesidad de que el consentimiento deba prestarse de manera expresa o que el responsable deba ser capaz de demostrar que lo obtuvo.

En las páginas siguientes ampliaremos sobre cuál es el estándar del interesado medio razonable a través de los requisitos que debe reunir un consentimiento válido según la definición aportada por el RGPD. A pesar de ello, para conocer cómo se interpretarán en la práctica determinados aspectos del RGPD habremos de esperar a la consolidación de jurisprudencia del TJUE. En esencia, el art. 4.11 RGPD pretende dar

[178] INFORMATION COMMISSIONER'S OFFICE (2018): *Lawful basis for processing, consent*.

respuesta a las cuestiones básicas del proceso de decisión y expresión de la voluntad del interesado, esto es, el cómo, el para qué y el cuándo del consentimiento. En los siguientes epígrafes se tratan estas preguntas.

3.3. ¿Cómo debe prestarse el consentimiento?

A esta pregunta responden dos de las características de la definición dada al consentimiento, aquellas de ser prestado de manera libre e inequívoca.

3.3.1. Consentimiento libre

Como regla general, el RGPD prescribe que no será válido el consentimiento cuando no exista un control real del interesado sobre la forma en que se utilizan sus datos. De este modo, únicamente cuando el interesado adquiera un rol protagonista en el proceso de elaboración de la decisión sobre si aceptar un determinado tipo de tratamiento de datos personales estará actuando de forma libre. Por este motivo, siguiendo la calificación dada por el CEPD en su Opinión sobre el consentimiento,[179] se pueden identificar tres circunstancias principales que podrían cuestionar la libertad de un interesado.

Desequilibrio de poder y perjuicio

Si el sujeto se siente compelido a consentir, si su negativa provocase consecuencias negativas, o si no fuera posible retirar el consentimiento, este no se habrá prestado libremente. Por ello, cualquier circunstancia que cree una percepción de coerción en el interesado viciará su autonomía y por tanto el acto del consentimiento.

Por este motivo, el RGPD excluye, al menos de principio, el consentimiento generalizado en determinadas situaciones en las que aprecia una posible relación basada en desequilibrios de poder. Tal es el caso en la relación entre autoridades públicas respecto de los ciudadanos o de los empleadores respecto de sus empleados.

[179] COMITÉ EUROPEO DE PROTECCIÓN DE DATOS (2018): *Guidelines on consent under Regulation 2016/679* (WP259 rev.01), de 10 de abril.

Pues bien, analógicamente, cabría argumentar que en entornos de altos niveles de automatización, aplicación de innovaciones tecnológicas poco comprendidas por las personas y uso de datos personales generados en prácticamente todos los aspectos de nuestra cotidianidad, se establece una relación entre responsable/prestador de servicios y el interesado/usuario que refleja una clara asimetría en la distribución del conocimiento y del poder.

Condicionalidad

La obligación de prestar el consentimiento para tratar más datos personales de los estrictamente necesarios limita la libertad de los interesados. En este sentido, el art. 7.4 trata este extremo estableciendo que "al evaluar si el consentimiento se ha dado libremente, se tendrá en cuenta en la mayor medida posible el hecho de si, entre otras cosas, la ejecución de un contrato, incluida la prestación de un servicio, se supedita al consentimiento al tratamiento de datos personales que no son necesarios para la ejecución de dicho contrato".

Granularidad

Asimismo, la falta de granularidad también afecta la libertad del interesado. El considerando 43 amplía este aspecto indicando que "se presume que el consentimiento no se ha dado libremente cuando no permita autorizar por separado las distintas operaciones de tratamiento de datos personales pese a ser adecuado en el caso concreto, o cuando el cumplimiento de un contrato, incluida la prestación de un servicio, sea dependiente del consentimiento, aun cuando este no sea necesario para dicho cumplimiento". Asimismo, el art. 7.2 indica que "no será vinculante ninguna parte de la declaración que constituya infracción del presente Reglamento". Este extremo es relevante en la medida en que parece no dejar opción al interesado a renunciar a las garantías que el RGPD le otorga, plasmadas en requisitos formales y materiales que debe cumplir el consentimiento solicitado por el responsable.

Como ejemplos de este tipo de consentimiento agrupado podemos referirnos a las llamadas "tracking walls" por su término en inglés. Se trata de funcionalidades que operan en entornos en línea y ofrecen a los usuarios la posibilidad de elegir entre la privacidad y el acceso a un servicio. Es decir, funcionan cuando los proveedores niegan a los usuarios el acceso a un servicio o funcionalidad con el argumento de que no han prestado su consentimiento para tratar, almacenar y recopilar datos a pesar de que estos no sean necesarios para la prestación de tal servicio o funcionalidad. Esto ocurre, por ejemplo, cuando a una persona se le niega el acceso a un sitio web si no presta su consentimiento para que se almacenen en su dispositivo cookies no necesarias.[180]

3.3.2. *Consentimiento inequívoco*

Tal y como ya ha sido expuesto, el art. 4.11 RGPD indica que el consentimiento debe tratarse de una manifestación de la voluntad inequívoca, mediante una declaración o una clara acción afirmativa. Esto sucede cuando el interesado actúa de manera deliberada e intencional para manifestar su aprobación. Sin embargo, lo que deba interpretarse como inequívoco está abierto a debate. Un ejemplo de ello es el uso de casillas pre-marcadas, que implican que la inacción del usuario pudiera ser tomada como asentimiento. Si bien el RGPD ha despejado las dudas e indica claramente que no podrán ser consideradas manifestaciones inequívocas de aceptación, la Directiva 95/46 no contenía dichas precisiones, lo que llevó a divergencias interpretativas e inseguridad jurídica. En relación con esta práctica concreta, el TJUE ha declarado en su reciente sentencia en

[180] Además de los requisitos de consentimiento previstos en el RGPD, el futuro Reglamento e-Privacy probablemente abordará el problema de las llamadas *tracking walls* o barreras de rastreadores mediante la prohibición de estos. Concretamente, el art. 8 de la propuesta de Reglamento del Parlamento de la UE establece que no podrá denegarse a un usuario acceso a un servicio o funcionalidad, independientemente de que sea remunerado o no, por el hecho de no haber prestado su consentimiento para el tratamiento de datos personales que no sean necesarios para la prestación de dicho servicio.

el asunto Planet49,[181] juzgado sobre la base de la Directiva 95/46, que este método no constituye una expresión válida de consentimiento.

En entornos digitales, este tipo de acciones puede tornarse en ocasiones problemáticas, dado el hecho de que en la actualidad prácticamente cualquier servicio que se preste a través de internet o dispositivo conectado realiza una recolección y tratamiento de datos, en muchas ocasiones, personales. Por ello, los usuarios son expuestos a multitud de solicitudes de consentimiento cada día que interrumpen la experiencia. El responsable deberá ser creativo en los modos de obtener una expresión inequívoca de consentimiento, que pueden consistir en deslizar el dedo por una pantalla, moverse ante una cámara inteligente o mover el teléfono de formas determinadas tales como el sentido de las agujas del reloj o realizando la figura de un ocho.[182]

En esencia, la consideración de lo que deba constituir un acto inequívoco se encuentra abierta. Ello puede dar lugar a que los avances, la creación de nuevos modos de recabar datos y la presentación de los dispositivos o servicios vuelvan a crear presión interpretativa. Para ello, la creación de códigos de conducta sectoriales o la publicación de directrices por parte de las autoridades de protección de datos es un mecanismo ágil de concreción de los nuevos retos que se presenten, máxime cuando la alternativa de aguardar a las decisiones del TJUE resulta larga y, como en el asunto Planet49, puede llegar cuando la norma de aplicación ya ha sido derogada.

3.4. ¿Para qué debe prestarse el consentimiento?

Para poder asegurar que el interesado conoce la finalidad del tratamiento, el consentimiento debe ser específico e informado.

[181] TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA (2019): Asunto C-673/17, Planet49 GmbH, de 1 de octubre. ECLI:EU:C:2019:801.

[182] COMITÉ EUROPEO DE PROTECCIÓN DE DATOS (2018): *Guidelines on consent under Regulation 2016/679* (WP259 rev.01), de 10 de abril.

3.4.1. *Consentimiento específico*

Esto implica que el consentimiento deba prestarse para una o varias finalidades específicas. Así, este requisito se relaciona también con el deber de información del responsable sobre los fines del tratamiento y la base jurídica (arts. 13.1.c y 14.1.c RGPD), con el principio de limitación de la finalidad (art. 5.1b)[183] y con la obligación del responsable de presentar cada una de las finalidades de manera independiente de manera que, cuando la base de licitud sea el consentimiento, el interesado pueda elegir aceptar o no cada una de ellas por separado.

¿Requiere un deber mayor de especificación que otras bases?

Una lectura conjunta sobre el principio de limitación de la finalidad en relación con el deber de información sobre dicha finalidad nos lleva a concluir que con independencia de cuál sea la base elegida por el responsable, sea o no el consentimiento, el responsable está obligado en todo caso a llevar a cabo un análisis por el que concrete sus finalidades y las exprese. En cambio, el hecho de que, a pesar de ello, se reincida en la necesidad de que el consentimiento se preste para uno o varios fines específicos ¿implica que, si esta es la base de legitimación elegida, se impone un deber mayor de concreción y especificación? Otro modo de entender esta precisión es que el legislador europeo quisiera simplemente resaltar que el consentimiento debe prestarse de manera granular, esto es, un consentimiento para cada finalidad.

Especificación vs las fases del big data

Sea como fuere, para cumplir este requisito, el responsable debe ser capaz de conocer, antes de comenzar la recopilación de los datos, qué datos necesitará y para qué finalidades específicas. Además, si la finalidad del tratamiento cambia en algún momento, el usuario deberá ser informado de nuevo y deberá obtenerse un nuevo consentimiento referido al nuevo

[183] GRUPO DE TRABAJO DEL ARTÍCULO 29 (2013): *Opinion 03/2013 on Purpose Limitation* (WP 203), de 2 de abril, p. 15-16.

tratamiento de los datos o buscarse otra base de legitimación del tratamiento. En consecuencia, cuando un responsable recopila los datos para una o varias finalidades específicas, debe poder conocer, como mínimo, dichas finalidades antes de comenzar la Fase 1-Recogida. De manera conjunta, en caso de que, además, deseen tratarse los datos como insumo de la Fase 2-Análisis, el responsable debería prever este hecho e informar de ello también antes del inicio del tratamiento, esto con independencia de si la base para el tratamiento de los datos con dicha finalidad es el consentimiento o no. En cambio, la Fase 3-Aplicación, depende de resultados en muchas ocasiones impredecibles, de manera que el responsable no se encontrará en posición de poder determinar dichas finalidades e informarlas de manera específica.

Esta conclusión es de gran importancia en el contexto de las tecnologías big data pues el principal valor del big data reside en que la nueva información que se genera con la analítica de datos permite descubrir información de manera imprevisible y ello permite a su vez otorgar nuevos usos a los datos.

3.4.2. *Consentimiento informado*

El requisito del consentimiento informado se encuentra estrechamente relacionado con los principios de lealtad y, principalmente, de transparencia (art. 5.1.a) y con la premisa de que muchos de los desafíos del cumplimiento normativo se pueden superar siendo abierto sobre lo que está haciendo. A pesar de que la transparencia ha sido un principio implícito en la normativización de la protección de datos desde sus inicios, el RGPD destaca su importancia al incorporarlo en el elenco de principios del tratamiento. Asimismo, este requisito está directamente relacionado con los derechos de información establecidos de los arts. 13 y 14, que en todo caso deben observarse sea cual sea la base de licitud y no únicamente si esta es el consentimiento.

Esto conlleva que antes de prestar el consentimiento el individuo debe poder acceder a toda la información relevante de forma comprensible y

completa. Por el contrario, cuando falta dicha información el consentimiento prestado no podrá ser considerado válido y por tanto el tratamiento carecerá de licitud. Ello es consecuencia necesaria del poder de disposición y capacidad de control que pretende cumplir la figura del consentimiento. Esta información debe proveerse con independencia de si los datos han sido obtenidos directamente del interesado o no. Así, el responsable que tenga base de legitimación para ello podrá ceder datos personales a un tercero, que deberá informar al interesado adecuadamente.

Políticas de privacidad. ¿Panacea?

El modo en que los responsables del tratamiento han encontrado la forma de facilitar información a los interesados en el entorno digital y, en caso necesario de obtener su consentimiento, se ha basado en avisos y políticas de privacidad en línea. El objetivo de los requisitos de notificación e información es proporcionar a los interesados la capacidad de decidir con conocimiento de causa cómo se utilizarán sus datos personales y para qué fines. Por lo tanto, la razón de ser de las notificaciones es que el consentimiento se presta en coherencia con la voluntad y la autonomía de una persona.

Ya desde los años de vigencia de la Directiva 95/46, estos avisos han demostrado ser demasiado complejos, largos y dados a utilizar una jerga legalista, algo que en muchas ocasiones ha sido explicado como reflejo de que, en realidad, las políticas de privacidad son vistas como un modo de limitación de responsabilidad formal del responsable más que un medio efectivo para comunicar a los interesados en qué consiste el tratamiento. Sea como fuere, el uso de textos largos y formalistas provocaba que los avisos de privacidad no fueran leídos o comprendidos por el interesado medio razonable, lo que daba lugar a que la manifestación del consentimiento no reflejase una elección real de la persona. Este fue el motivo por el que el RGPD, en su énfasis del principio de transparencia, introdujo el requisito de que la información sea presentada de manera

inteligible y utilizando un lenguaje sencillo y claro (arts. 7.2, 12, considerando 42 y 58).

Esta idea fue también discutida por algunos autores antes de que el RGPD fuese aplicable, entre ellos, Baroccas y Nissebaum,[184] que argumentaron que, a pesar de lo favorable de no utilizar un lenguaje complicado, cabría la posibilidad de que utilizar un lenguaje sencillo no fuese capaz de proporcionar una explicación lo suficientemente detallada sobre aspectos del tratamiento que cada vez son más enrevesados. Esto podría provocar que determinados aspectos complejos e importantes quedaran manifestados sin el detalle suficiente como para considerarse informados.

Entorno transparente

Como alternativa, Culnan y Bruening proponen pasar de un modelo basado en meras notificaciones a otro basado en un "entorno de transparencia".[185] Esto supondría, pode ejemplo, no limitarse únicamente a la publicación de las prácticas de una empresa (enfoque de notificación), sino abrirse a la divulgación genuina en varias direcciones, en la que las notificaciones serían sólo una de ellas (enfoque de transparencia).

Desde este punto de vista, los avisos pueden seguir siendo un buen punto de partida para lograr la transparencia, aunque sean complejos y largos. De hecho, incluso cuando un aviso complicado y legalista pudiera ser de poca utilidad para el interesado medio razonable, sí pueden ser una de las mejores maneras de entender las complejidades del tratamiento y los detalles para lectores avanzados y expertos, para aquellos usuarios más interesados en las sutilezas y dispuestos a tomarse el tiempo para leer los avisos, así como para las autoridades de control.

[184] Por ejemplo, BAROCCAS, Solon; NISSEBAUM, Helen (2014): "Big data´s End Run Around Anonymity And Consent", en *Privacy, big data and the public good. Frameworks for engagement*, Cambridge University Press, p.44-75.

[185] CULNAN, Mary J.; BRUENING, Paula. (2018): "Privacy Notices Limitations, Challenges, and Opportunities", en Evan Selinger, Rochester Institute of Technology, New York, Jules Polonetsky, Omer Tene (eds.), *The Cambridge Handbook of Consumer Privacy*, Cambridge University Press, pp. 524-545.

Sin embargo, sin duda no serían suficientes para lograr una transparencia total y tendrían que trabajar conjuntamente con una variedad adicional de medidas. Algunas de las medidas propuestas incluyen notificaciones "justo a tiempo" por medios originales en los que la recogida y tratamiento de datos pueden ser sensibles o no obvios para el interesado, por ejemplo, cuando se utilizan dispositivos conectados que acceden a datos como la localización en determinados momentos. Otras propuestas en esta dirección han sido también enfoques contextuales en los que la información se presente de manera que se destaquen los usos de los datos que se derivan de lo que es socialmente aceptable; el uso de imágenes, iconos o sonidos en lugar de texto; y la educación y la sensibilización del público para que el público pueda llegar a conocer mejor el ecosistema de los datos en su conjunto.

Esta idea se alinea con el principio de responsabilidad proactiva del artículo 5 del GDPR. Esto se debe a que la búsqueda por parte de los responsables del tratamiento de datos de formas innovadoras de proporcionar información completa a los usuarios a los que van dirigidos suele ser el resultado de un replanteamiento de todas las actividades de tratamiento llevadas a cabo por el responsable y el flujo de datos personales. Esto permite al responsable obtener una visión más profunda de los flujos de datos, desde la recogida inicial (qué tipos de datos se recogen, de quién, para quién, para qué finalidades), hasta el tratamiento que se da a esos datos dentro de la organización (enriquecimiento de datos con otras fuentes adicionales, minería de datos, aplicación de medidas de seguridad contra actividades ilícitas, realización de transferencias de datos, combinación de silos de datos, etc.), a los usos finales de los datos.

Algunos de estos modelos, sugerencias y prácticas ya se utilizan en la actualidad. Por ejemplo, el considerando 60 de GDPR ya promueve el uso de iconos, aunque a modo de simple recomendación, pues este extremo no fue trasladado al articulado del RGPD.

Asimismo, la noción de protección de datos por diseño y por defecto se incorpora como disposición vinculante en el art. 25 RGPD, que, aunque no menciona expresamente los requisitos de información y transparencia, establece que "el responsable del tratamiento (...) aplicará las medidas técnicas y organizativas adecuadas (...) destinadas a aplicar los principios de protección de datos". Así, por ejemplo, en línea con dicha previsión, Apple ha anunciado recientemente que desde octubre de 2019 exigirá a todos los proveedores de aplicaciones la publicación de un aviso de privacidad como requisito para poder aparecer en su App Store, independientemente de si el desarrollador almacena o no datos personales.[186] Este aviso debe informar a los usuarios de los dispositivos de Apple sobre, entre otros extremos, los datos recopilados por el software, sus usos y cómo eliminarlos. Por su parte, las políticas de desarrolladores de Android también contienen una previsión similar respecto de aquellas aplicaciones que traten datos personales.[187]

De este modo, la decisión se integra en el proceso de la empresa de y diseña el requisito de una mayor transparencia en línea con la obligación de la protección de datos desde el diseño.

Qué información debe incluirse

Otra cuestión que surge es si la obligación del responsable del tratamiento de informar sobre la recogida de los datos se circunscribe a la información que explícitamente recoge, o si debe adoptarse un criterio más amplio y entender que este deber de información también alcanza a aquella información que la institución pudiera obtener tras el tratamiento.

Numerosos autores opinan que los deberes de información y la necesidad de recabar el consentimiento debe referirse, no solo al hecho de que se

[186] Chris VELAZCO (2018): “Apple requires a privacy policy for everything in the app store”, en *Engadget*,; App Store Review Guidelines, apartado 5.1. Disponible en: https://developer.apple.com/app-store/review/guidelines/#legal.

[187] Google Play, Políticas del Programa para Desarrolladores. Disponible en: https://play.google.com/intl/es/about/privacy-security-deception/user-data/#!?zippy_activeEl=personal-sensitive#personal-sensitive.

recaben datos primarios, sino también a la información que se puede extraer de un análisis sofisticado de estos, incluyendo la información que pueda extraerse de la agregación de datos que recaba la empresa con datos provenientes de otras fuentes y ficheros. No obstante, esta aproximación tiene muchas dificultades prácticas, en tanto que, por su propia naturaleza, el análisis big data se caracteriza precisamente por lo inesperado de los resultados que revela. Así, ¿cómo explica el responsable del tratamiento que resulta imposible saber con antelación qué información revelará el tratamiento de los datos recabados? Sería razonable argumentar que el consentimiento prestado bajo estas circunstancias no es el consentimiento informado que la ley exige.

La paradoja de la inferencia

De lo anterior cabe preguntarse ¿tiene el responsable una obligación de informar sobre la obtención de datos personales que no se han obtenido del interesado, sino a través de las operaciones de tratamiento de la Fase 3-Aplicación? Como indicábamos en el Capítulo III, los datos recogidos durante la Fase 1-Recogida son utilizados como insumo para la Fase 2-Análisis, de modo tal que el responsable puede encontrar correlaciones en los datos de las que deduzca inferencias y pueda modelar perfiles. En la medida en que esta información no se refiera a personas identificables no se tratará de datos personales. Sin embargo, en la Fase 3-Aplicación, los datos personales de otro grupo de interesados son tratados con la finalidad de poder aplicar sobre ellos los modelos creados en la fase anterior, descubrir nueva información y subsumirles en un perfil concreto, todo ello para tomar decisiones. No obstante, la información adicional "creada" como resultado de la Fase 3 no es certera, pues el método analítico mantiene un margen de error. Esto crea lo que podríamos bautizar como la paradoja de la inferencia por la que la creación de información mediante inferencia estadística podría no ser considerada dato personal y por tanto, ajena a las obligaciones ligadas al tratamiento de datos personales. Sin embargo, en la medida en que un responsable otorgue valor y veracidad a dicha información y actúe como si fueran datos personales cuyo tratamiento

impacta en el interesado, está convirtiendo la probabilidad estadística en un dato personal. De este modo, el interesado no conoce qué información se está creando sobre él, quién la trata, con qué fines ni su grado de veracidad.

Imprevisibilidad sobre usos secundarios

Culnan y Bruening[188] ya mencionaron también que uno de los principales problemas planteados por las tecnologías de datos masivos en relación con el consentimiento informado es la imprevisibilidad de los resultados analíticos y, por lo tanto, la falta de conocimiento de los usos secundarios de los datos. Ello conlleva que, aunque los individuos puedan estar informados sobre la recopilación y el uso inicial de los datos para un determinado fin, pierdan el control sobre los usos subsiguientes de dichos datos, o incluso el conocimiento sobre estos usos secundarios. En cuanto al aprendizaje automático, se ha discutido mucho sobre la existencia de cajas negras[189] y las dificultades para proporcionar información en la que intervienen algoritmos y análisis complejos en el procesamiento. Una de las razones es el funcionamiento inherente del proceso analítico. Mientras que en las estadísticas tradicionales el enfoque era proponer una hipótesis para luego recopilar y analizar los datos en busca de concluir si pueden ser rechazados o no, el enfoque cuando analizamos grandes conjuntos de datos es buscar correlaciones en los datos a la espera de lo que pueden decir. Estos nuevos planteamientos introducidos por los avances de las tecnologías pueden hacer que las notificaciones sean difíciles de redactar o inadecuadas para que los usuarios dispongan de una herramienta que les permita comprender el tratamiento y decidir sobre el mismo.

[188] CULNAN, Mary J.; BRUENING, Paula. (2018): "Privacy Notices Limitations, Challenges, and Opportunities", en Evan Selinger, Rochester Institute of Technology, New York, Jules Polonetsky, Omer Tene (eds.), *The Cambridge Handbook of Consumer Privacy*, Cambridge University Press, pp. 524-545.

[189] PASQUALE, Frank (2015): *The black box society: The secret algorithms that control money and information*, Cambridge, Londres: Harvard University Press.

3.5. ¿Cuándo debe prestarse el consentimiento?

El consentimiento debe prestarse antes del inicio del tratamiento de datos, y el responsable no podrá decidir a posteriori modificar la base de licitud del tratamiento.

Consentimiento por adelantado

El ciclo de vida de la información en entornos en los que se lleva a cabo un tratamiento de datos masivos conforme a las fases explicadas en el capítulo anterior crea tensión sobre la prestación del consentimiento. Ello es debido a la imprevisibilidad de las deducciones del proceso analítico sobre los datos, de modo que en ocasiones no es posible saber de antemano qué nueva información podrá generarse o qué consecuencias puede tener el tratamiento. Por este motivo, el responsable no tiene capacidad para especificar en el momento de la recogida de los datos, es decir, antes del inicio de la Fase 1-Recogida, las finalidades para las que podrán ser utilizados los datos, las consecuencias o el tipo de datos que será tratados en la Fase 3-Aplicación. A pesar de ello, en ocasiones el interesado es expuesto a solicitudes de consentimiento que abarcan todas las fases del tratamiento.

Es decir, surge una nueva dificultad derivada del hecho mismo de que el mayor valor de la información ya no reside en un uso primario, sino que ahora se encuentra en los usos secundarios, y esto afecta al núcleo de la protección de datos personales. Sobre la validez del consentimiento otorgado en un primer momento y que se pretende sirva para legitimar operaciones de tratamiento de datos posteriores, cabe recordar las conclusiones del Abogado General en el asunto Fashion ID:[190]

> "Me resulta difícil aceptar la idea de que (…) deba haber un tratamiento diferenciado (menos protector) para los usuarios de

[190] TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA (2019): Asunto C-40/17, Fashion ID GmbH & Co. KG vs Verbraucherzentrale, de 29 de julio. ECLI:EU:C:2019:629. Petición de decisión prejudicial planteada por el Oberlandesgericht Düsseldorf (Tribunal Superior Regional de lo Civil y Penal de Düsseldorf, Alemania).

> Facebook por haber aceptado estos previamente la posibilidad de (cualquier tipo de) tratamiento de sus datos personales por Facebook. De hecho, semejante argumento supone que, al abrir una cuenta en Facebook, el usuario acepta por adelantado todo tratamiento de datos con respecto a cualquier actividad en línea de ese usuario de Facebook por parte de cualquier tercero que mantenga cualquier tipo de vínculo con Facebook. Y ello incluso en una situación en que no hay ningún indicio concreto de que tenga lugar tal tratamiento (como parece suceder cuando simplemente se visita la página web de la demandada). (…) Además, de nuevo, es evidente que el consentimiento se ha de dar y la información facilitar antes de que los datos sean recabados y transferidos".

Renovación del consentimiento

Por otro lado, los usuarios pueden querer prestar su consentimiento a diferentes usos de los datos a lo largo de la relación con el responsable, en lugar de que se les pida que den su consentimiento al principio. Por ejemplo, pensemos el caso de una app que solicita el consentimiento para acceder a la localización del dispositivo[191] para prestar determinadas funcionalidades. El interesado se verá menos invadido en su esfera de intimidad si la app muestra un aviso sencillo antes del inicio de la recogida del dato cada vez que ello ocurra solicitando aceptar el tratamiento. De este modo, el interesado se mantiene consciente a lo largo del tiempo de que esta información es objeto de tratamiento y podrá decidir rechazarlo cuando así lo prefiera.

Caducidad del consentimiento

Por último, el RGPD no impone un límite temporal hasta el cual el consentimiento es válido, sino que dependerá del contexto y es obligación

[191] En función de las circunstancias del caso concreto, el dato de localización podrá ser un dato personal sujeto al RGPD. En el caso de que no lo fuere, la recolección de esta información estará sometida a la normativa e-Privacy que también requiere consentimiento del usuario conforme al RGPD.

del responsable ponderar todas las circunstancias para solicitar el consentimiento de manera periódica según proceda.

4. Estándar subjetivo en el consentimiento

Una vez analizados los requisitos del consentimiento que permitirían cumplir con el estándar que un interesado medio razonable necesitaría para poder prestar su consentimiento al tratamiento de datos personales de manera efectiva y en cumplimiento con la norma, analizaremos el estándar subjetivo del consentimiento.

Este analiza el consentimiento desde la perspectiva de aquél que debe prestarlo, y hace referencia al hecho de si un interesado particular es capaz de ejercer su expresión de voluntad autónoma en el contexto específico. En ocasiones, a pesar de que los requisitos formales del consentimiento se respeten, sobre el interesado actúan otros factores que cuestionan la confiabilidad en la manifestación de aquiescencia. Esto es, el estándar subjetivo indica aquellas condiciones por las que, desde el punto de vista del interesado, se cumple la función formal pero no material del consentimiento.

El consentimiento como herramienta básica para otorgar control sobre el uso de los datos personales a los interesados sin duda ha sido de gran valía, especialmente en las primeras fases de la automatización del tratamiento de datos personales. No obstante, el estado de la técnica actual, caracterizado por prácticas más extendidas, intensivas e impredecibles ha modificado el valor real del consentimiento del interesado. Así, el consentimiento ha mostrado ciertas deficiencias, que se agudizan en entornos big data y cuyo estudio merece atención.

4.1. No se lee la información

La mayor parte de los individuos no lee las políticas de privacidad, que se han convertido en el mecanismo más utilizado para recabar el consentimiento en entornos digitales.

Según los datos del informe especial sobre el RGPD del eurobarómetro de 2019,[192] únicamente una minoría de ciudadanos (13%) afirma leer la totalidad de las políticas de privacidad. Entre los motivos principales manifestados se encuentran la longitud de las políticas y su dificultad para comprenderlas, es decir, tenemos limitaciones derivadas de nuestras propias facultades cognitivas para procesar información.[193]

En un sentido similar, en un reciente estudio de Axios,[194] una mayoría de personas afirma no leer las políticas de privacidad antes de aceptarlas. La evidencia muestra que los individuos declaran ampliamente la importancia de comprender cómo se tratan los datos personales por parte de los responsables, y sin embargo, no actúan en consecuencia. Sorprendentemente, el estudio manifiesta que si uno "lee entre líneas" esta divergencia pueda explicarse en el hecho de que los interesados[195] no valoren su privacidad tanto como expresan. Se trata de una conclusión controvertida y que seguro encontrará numerosas críticas, pues la experiencia indica que los interesados sí valoran su privacidad y el uso que se haga de sus datos personales. Quizás más cercana a la realidad sea la posibilidad, también mencionada en dicho estudio, de que los individuos son expuestos a tantas decisiones diarias que se crea fatiga, volviendo dichas decisiones ineficaces.[196]

---

[192] COMISIÓN EUROPEA (2019): Special Eurobarometer 487ª, The General Data Protection Regulation, de junio.

[193] ÁLVAREZ CARO, María (2017): *La privacidad en la sociedad de la información: el derecho al olvido en la UE como reto derivado del avance digital*, tesis doctoral, Teseo.

[194] HART, Kim (2019): "Privacy policies are read by an aging few", en *Axios*.

[195] El estudio, realizado sobre la base de entrevistas entre adultos en Estados Unidos, se refiere a "consumidores" terminología coherente con la perspectiva de defensa de los derechos del consumidor desde la que se analiza el tratamiento de datos personales. A pesar de ello, la aseveración conserva su sentido al hablar de interesados, en el sentido del RGPD y la defensa del derecho de protección de datos.

[196] De hecho, esta divergencia entre pensamiento y comportamiento no es nueva. Por ejemplo, ya en 1971, la Federación Americana de Sociedades de Tratamiento de la Información (AFIPS) junto con Time Magazine llevaron a cabo una encuesta sobre la percepción pública de los ordenadores. Casi el 40% de los encuestados consideraba los ordenadores una amenaza para la privacidad, y sin embargo, el 85% consideraba que el avance tecnológico de las décadas anteriores había ayudado a mejorar su calidad de vida. Ver HONDIUS, Frits (1975): *Emerging Data Protection in Europe*, North-Holland, p. 3-4.

Ejemplos: Gamestation y Faceapp

Como ejemplo anecdótico de la falta de lectura de los avisos mostrados en sitios web, o en su caso, de la manifestación de aceptación de unos términos a pesar de no estar conforme, destaca la solicitud de consentimiento del sitio web Gamestation, negocio de comercialización de videojuegos por internet. En ella, al realizar un pedido a través de su sitio web el usuario aceptaba ceder a la empresa su alma inmortal por toda la eternidad, eso sí, manteniendo un período de cinco días para ejercer reclamaciones por escrito.[197]

Otro ejemplo reciente de que los usuarios no leen las políticas de privacidad es el sucedido a consecuencia de la viralización de la aplicación FaceApp. Se trata de una aplicación que aplica filtros sobre la fotografía seleccionada de modo que la persona de la imagen parezca, por ejemplo, más joven o más envejecida. Los resultados realistas de los filtros de la fotografía y su utilización repentina por personalidades famosas viralizó la utilización de esta aplicación durante el verano de 2019, lo que llevó también atención a su política de privacidad, convirtiéndose en foco mediático y creando preocupación entre amplios sectores sociales por el uso de los datos personales. Dejando aparte el hecho de los graves incumplimientos legales de dichas condiciones[198], los usuarios reaccionaron sorprendidos por el tratamiento de los datos personales por parte del responsable, lo que demuestra que los usuarios de la aplicación no habían leído, con carácter generalizado, las condiciones que estaban, supuestamente, autorizando.

---

[197] SMITH, Catharine (2011): "7,500 Online Shoppers Accidentally Sold Their Souls To Gamestation", en *Huffpost*.

[198] La política no se encontraba actualizada al marco regulatorio surgido del RGPD. Entre otras prácticas, por ejemplo, no se informa con claridad (mucho menos con transparencia) de qué datos recoge la aplicación, aunque la información sí permite observar que se recogen más datos de los necesarios para la prestación del servicio; no se detallan las finalidades de manera específica ni las bases de legitimación. Asimismo, tampoco se informa de los derechos de los usuarios ni de cómo ejercerlos.

4.2. Nivel razonable de comprensión

El consentimiento presupone que el individuo debe comprender la información que se le presenta, así como la elección que realiza y otorgar una indicación clara de conformidad con ello. Por ello, para cumplir con su propósito, el consentimiento necesita que el interesado tenga un nivel razonable de comprensión acerca de la información que se le provee y de las implicaciones de su decisión. Esta es, de hecho, por ejemplo, la motivación que subyace al hecho de que el RGPD otorgue especial consideración al modo en que se solicita y se presta consentimiento de los niños.

Sin embargo, la experiencia también muestra que el interesado medio no comprende la información o sus implicaciones y termina por seleccionar de manera automática las opciones de “sí”, “aceptar” o similares, prestando un consentimiento que gozará de validez legal pero no funcional.

En ocasiones, esta falta de comprensión no se da únicamente en interesado medio. En muchas ocasiones, también para el lector más experto, jurista, resulta complejo comprender qué prácticas se están aceptando al prestar el consentimiento.

Un motivo para ello puede ser la falta de claridad en la información, en cuyo caso, es posible que los requisitos del RGPD no se estén cumpliendo o que el esfuerzo que debe llevar a cabo el interesado para comprender lo que se le expone es desproporcionado.

En otros casos, la razón de la falta de comprensión se debe a que las circunstancias, tratamientos y riesgos son de alta complejidad, lo cual podría viciar el consentimiento, todo ello, a pesar de que el responsable hubiera cumplido con las obligaciones que impone el RGPD.

Esto es relevante, en concreto, en circunstancias en las que los métodos de recogida de datos cambian constantemente, las técnicas de rastreo de los usuarios son cada vez más intensas, ubicuas y desapercibidas, de modo que en muchas ocasiones los usuarios no son conscientes ni siquiera

de que sus datos están siendo recogidos. Por ejemplo, ya en 2008, cuando Piñar Mañas señalaba la preocupación por el hecho de que las nuevas tecnologías permiten obtener y tratar información de todo tipo, de formas novedosas y con un desarrollo difícil de predecir, creando herramientas de poder y control más poderosas que las conocidas hasta la fecha y por tanto, con riesgos tampoco conocidos.[199]

En otras ocasiones, los usuarios sí son conscientes de que su comportamiento en línea puede ser rastreado, pero no alcanzan a comprender la intensidad del rastreo o el funcionamiento del mercado de la personalización de servicios.[200]

Por otro lado, las prácticas por las que dichos datos se hacen accesibles a terceros evolucionan a gran velocidad, y las finalidades del tratamiento pueden tener efectos obscuros y complejos. En concreto, entornos impredecibles, de rápido avance tecnológico como aquellos en los que se usan tecnologías big data pueden ser propensos a esta falta de un nivel razonable de comprensión por parte del interesado medio, poniendo en entredicho que la manifestación de su voluntad sea realmente informada.

Sin embargo, tal y como ha señalado la autoridad inglesa de protección de datos, la aparente complejidad del análisis de grandes volúmenes de datos no debe convertirse en una excusa para dejar de obtener el consentimiento cuando así se requiera. Las organizaciones deben encontrar el punto en el que explicar los beneficios de los análisis y ofrecer al usuario una elección significativa -y luego respetar esa elección cuando se están procesando sus datos personales.[201]

---

[199] PIÑAR MAÑAS, José Luís (2008): "¿Existe la privacidad? Lección magistral", en *CEU Ediciones*.

[200] COMITÉ EUROPEO DE PROTECCIÓN DE DATOS (2019): *Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects*, de 8 de octubre.

[201] INFORMATION COMMISSIONER'S OFFICE (2014): *Big data and data protection*, p. 19.

En un mismo orden de cosas, también se han alzado algunas voces en nuestro panorama nacional. Así, por ejemplo, María Loza indica, en determinados casos, "el consentimiento no es viable y por ello, el individuo ni decide, ni puede decidir. En concreto, indica ¿[s]ignifica ello que hemos de resignarnos ante la evolución tecnológica y admitir por defecto que hay una parte de nuestra privacidad que no podemos controlar? En nuestra opinión, la respuesta no puede ser afirmativa, no podemos admitir una "pérdida de privacidad colateral" sólo porque no sepamos, o no queramos, establecer las medidas de protección oportunas".[202]

De hecho, la complejidad en la información sobre una situación determinada no es característica única del tratamiento de datos personales en entornos altamente tecnológicos. En ámbitos tales como la información nutricional o alimenticia, el consumidor no ostenta la carga de conocer cada compuesto químico y su funcionamiento en el metabolismo para poder hacer su compra semanal, sino que la información se le presenta de manera relativamente normalizada, en términos de valores nutricionales por 100 g o códigos. Del mismo modo, para el tratamiento de datos personales, debemos ser capaces de identificar qué información básica necesita un interesado para poder superar el estándar subjetivo y asegurar que la recibe sin necesidad de tener que exponerse a sobreinformación.

Por otro lado, cuando un interesado accede a un servicio para el que se le remite una solicitud de consentimiento, este tiene confianza en el hecho de que el responsable del tratamiento llevará a cabo sus prácticas de manera lícita y leal. Esta confianza se ve quebrada cuando una solicitud de consentimiento incluye prácticas alejadas de lo razonablemente esperado de manera poco transparente a las que el interesado acepta sin haber realizado el ejercicio de conformar su propia voluntad.

El RGPD ha tratado de dar una solución a algunas de estas limitaciones a través del requerimiento de separar el consentimiento para el tratamiento

[202] LOZA CORERA, María (2017): "De los microdatos a los datos masivos. Cuestiones legales", en Universitat de València, p. 412.

de datos del resto de términos y condiciones y de solicitar un consentimiento diferente para cada actividad del tratamiento. A pesar de todo, la suposición de que un individuo ha comprendido todas las consecuencias del tratamiento cuando lleva a cabo una manifestación de consentimiento se torna en problemática, pues esta realidad choca con el estándar del interesado medio razonable. Sin embargo, el responsable que obtiene el consentimiento adquiere una prueba jurídicamente válida que le blinda para llevar a cabo sus actividades de tratamiento de manera lícita.

De este modo, en contextos como los que aquí nos incumben, cambiantes e impredecibles, resulta muy complicado para un usuario poder ejercer control sobre cómo se utilizan sus datos. Sin embargo, la función del consentimiento se llega a instrumentalizar para solicitar autorizaciones que no cumplen con el estándar subjetivo del interesado.

Esto supone que el consentimiento, herramienta creada para otorgar control a los interesados, se convierte en un arma de doble filo que vuelve contra sus intereses y aporta mayor protección jurídica al responsable que al propio interesado.

5. La cara B del consentimiento: estándar del responsable

Tras analizar el consentimiento desde el punto de vista del interesado, debemos observar la otra cara de la relación, el responsable. Así, en tercer lugar, haremos referencia al estándar de responsable. Este es quien solicita el consentimiento y quien debe garantizar que los requisitos legales se cumplen, esto es, el estándar del interesado medio razonable. Idealmente, también debe garantizar el estándar subjetivo del interesado. Así, la situación ideal en la que el consentimiento despliega su función material y formal es aquella en la que los tres estándares coinciden.

Es obligación del responsable garantizar que el interesado está realmente siendo partícipe del proceso de toma de decisión. Sin embargo, tal y como ocurría desde la perspectiva del interesado, existen factores que también dificultan el debido cumplimiento del estándar del responsable medio

razonable. Algunos factores son ajenos a la voluntad del responsable y se explican por la complejidad del tratamiento, mientras que otros pueden resultar del hecho de que el responsable no actúe de manera ética y en cumplimiento de su obligación.

5.1. Falta de conocimiento del responsable

En entornos impredecibles como los que aquí se analizan será factible pensar que, en muchas ocasiones, el responsable del tratamiento no conozca de antemano, en el momento de solicitar el consentimiento para las finalidades primarias, el elenco de posibles opciones y fines secundarios que se pueden abrir al uso posterior de los datos.

El funcionamiento de aquellos procesos big data puede ser complejo incluso para el propio responsable, pues los datos ni siquiera quedan bajo su amparo, sino que pueden transferirse de un responsable a otro y generar valor y riesgos que no son conocidos en el momento de la recogida de los datos en la Fase 1. De hecho, el consentimiento se ha llegado a definir como un cheque en blanco.[203]

El responsable ve también expuesta su seguridad, pues en muchas ocasiones ni siquiera este podrá conocer, en el momento de redactar la cláusula informativa, todas las consecuencias de los tratamientos de datos que desee realizar ni de las decisiones que de dicho tratamiento puedan derivarse. En última instancia, esto se traduce en la inseguridad de estar asumiendo como válida la base jurídica del art. 6.1.a) RGPD de manera incorrecta, lo que despliega el nivel más grave de sanciones por infracción del Reglamento.

5.2. Finalidades compatibles

En caso de que los fines del tratamiento cambien o haya nuevas finalidades que no pudieron ser anticipadas en un primer momento, será necesaria una

[203] BAROCCAS, Solon; NISSEBAUM, Helen (2014): “Big data´s End Run Around Anonymity And Consent”, en *Privacy, big data and the public good. Frameworks for engagement*, Cambridge University Press, p.44-75.

nueva base de legitimación, salvo que las finalidades no sean incompatibles.

En este trabajo partimos de la premisa más protectora de que las finalidades de las Fases 1-Recogida, Fase 2-Análisis y Fase 3-Aplicación no pueden considerarse compatibles, de modo que requieren una base de legitimación independiente. Esto es, el consentimiento prestado para la Fase 1 no puede extenderse hasta cubrir todo el espectro de actividades hasta la Fase 3. Incluso aunque fueran compatibles, tal y como el ICO ha recalcado,[204] generalmente no podrá continuarse el tratamiento para dichas nuevas finalidades cuando la base del tratamiento originaria fue el consentimiento. En dicho caso, sería necesario recabar un nuevo consentimiento que cubra específicamente dicho tratamiento, o encontrar una nueva base de legitimación. Es decir, ambos caminos -tanto si podemos considerar que las finalidades son compatibles como si no- conducen a la misma conclusión: será necesario contar con una nueva base de legitimación del tratamiento para las finalidades secundarias.

5.3. Asimetría de información

El uso de términos ambiguos y la falta de transparencia crean asimetrías en la información entre los responsables del tratamiento y los interesados. Para poder manifestar su voluntad y ejercer sus derechos, un interesado debe tener, al menos, un grado mínimo de conocimiento significativo sobre qué datos son objeto de tratamiento, para qué fines y qué consecuencias puede tener. Sin este mínimo conocimiento, el interesado no puede ejercer sus derechos con las debidas garantías. Del mismo modo, sin el conocimiento adecuado, un interesado podría ser más propenso a consentir el tratamiento automatizado de sus datos personales o la realización de perfiles, o no tendrían facilidad a ejercer su derecho a no ser objeto de este tipo de decisiones (art. 22 GDPR).

[204] INFORMATION COMMISSIONER'S OFFICE (2019): *Lawful basis guidance*.

Por ello, el responsable del tratamiento puede tener motivaciones para no comunicar toda la información relevante a los interesados y para crear una ilusión de complejidad que en realidad pretender crear lo que Martin denominó "obscuridad diseñada".[205] En un camino similar, Reidenberg et al ya señalaron que cuando las notificaciones son tan vagas, en la práctica equivalen a una falta de notificación.[206]

5.4. Información engañosa

Por otro lado, el responsable puede utilizar prácticas engañosas en su modo de transmitir la información sobre las actividades de tratamiento, sus finalidades o qué datos se recogen, entre otros. En función de qué información se aporte o de cómo, esto podría constituir una infracción de los deberes de información de los arts. 13 y 14 RGPD, independientemente de la base de licitud. En otras ocasiones, sin embargo, el responsable puede cumplir estrictamente con la información que se requiere en los arts. 13 y 14 y, a pesar de ello, aportarla de manera poco clara o recurriendo a prácticas engañosas, en ocasiones relacionadas con las prácticas conocidas como patrones oscuros ("*dark patterns*" por su término en inglés). En dicho caso, habría que estar al caso concreto para poder argumentar si sobre la base de estas prácticas puede alegarse infracción del principio de transparencia o una vulneración de los requisitos que determinan la validez del consentimiento informado y específico.

En ocasiones, estas prácticas pueden considerarse lo que Stefano Rodata[207] denominó micro violaciones de la protección de datos, aquellas que son percibidas por las personas sin otorgarles la importancia que

[205] MARTIN, Kirsten E. (2015): "Privacy Notices as Tabula Rasa: An Empirical Investigation into How Complying with a Privacy Notice Is Related to Meeting Privacy Expectations Online", en *Journal of Public Policy and Marketing*, Vol. 34, No.2, p. 210–227.

[206] REIDENBERG, Joel R., et al (2014): "Privacy Harms and the Effectiveness of the Notice and Choice Framework", en *I/S: A Journal of Law and Policy for the Information Society*, Vol. 1, No. 2, p. 485-524.

[207] PIÑAR MAÑAS, José Luís (2009): "Seguridad, transparencia y protección de datos: el futuro de un necesario e incierto equilibrio. Documento de trabajo 147/2009", en *Laboratorio de Alternativas, Centro de Estudios Políticos y Constitucionales*.

merecen, y que en realidad ocultan otras violaciones más graves que pasan desapercibidas. Una de las primeras consecuencias de ello es que dichas infracciones pasan desapercibidas, creando un contexto de impunidad entre aquellos responsables infractores, generando sobre los ciudadanos una sensación de despreocupación que en la mayoría de las ocasiones no coincide con la realidad.

Además de todo ello, este tipo de prácticas pueden tener un mejor encaje jurídico en otras ramas del Derecho con las que la protección de datos debe confluir para una óptima protección de los derechos del interesado, como por ejemplo, la defensa de los consumidores, que protege al consumidor de cualquier información que pueda conducir a error.

5.5. Consentimiento como pago por servicios

En otro orden de cosas, cabe destacar que el avance de la sociedad digital es fruto del desarrollo de servicios en línea, la proliferación del uso de dispositivos móviles, la conectividad, el mayor uso de redes sociales o el comercio electrónico. En ocasiones, la prestación de estos servicios se realiza a cambio de un pago monetario al prestador de dicho servicio, pero en otras ocasiones los servicios son prestados a cambio de mostrar publicidad a los usuarios. En la medida en que el funcionamiento del sector publicitario se basa en la mayor tasa de “clicks” que un usuario hace sobre los anuncios que se le muestran, la personalización de la publicidad incrementa los márgenes de beneficios de proveedor.[208] Como consecuencia, la recopilación de datos, el seguimiento del comportamiento de los usuarios en línea y creación de perfiles cada vez más detallados buscan conocer los gustos de cada usuario para personalizar la publicidad y los servicios de manera que el negocio de la monetización de los datos sea más lucrativo.

[208] ZUIDERVEEN BORGESIUS, Frederik J. (2015): *Improving Privacy Protection in the Area of Behavioural Targeting*, Kluwer Law International BV.

En otras palabras, en la actualidad, nuestra privacidad y datos personales han sido objeto de mercantilización. Sin embargo, ello tampoco debe significar que los interesados comercien con todos sus derechos y deban desprenderse de ellos.

Además del profundo debate sobre el consentimiento basado en opciones de "lo tomas o lo dejas", e incluso aceptando la posibilidad de que los datos personales puedan ser utilizados como moneda de cambio por servicios digitales, otros problemas subsisten.

5.6. ¿Cuál es el precio?

Esta situación pretende asemejarse a aquella por la que se intercambia una cosa a cambio de un precio, lo que es la base del contrato de compraventa regulado en el Derecho Civil, contrato que por su parte se perfecciona por el consentimiento de las partes una vez que han convenido cuál es el objeto del contrato y cuál es el precio. Tomando como referencia lo establecido en el Código Civil español[209] dicho precio debe ser determinado de antemano y no quedar al arbitrio de uno de los contratantes.[210]

En muchas ocasiones, no obstante, el precio, en término de prestar el consentimiento para la recogida y tratamiento de datos personales a cambio del disfrute de un servicio no queda especificado ni puede ser objeto de negociación por el interesado. Por ejemplo, cuando se solicita consentimiento para almacenar cookies y otros rastreadores similares, o para acceder a la información almacenada o emitida por el dispositivo, el interesado no conoce qué datos está aportando en el intercambio. Asimismo, en muchas ocasiones, tampoco tiene capacidad para decidir quién podrá acceder a sus datos, más allá de la capacidad de aceptar o denegar sin granularidad las cookies de terceros. Incluso cuando existe la opción, seleccionar uno a uno entre las decenas o cientos de nombres

[209] En lo que aquí se discute, los elementos y la perfección del contrato de compraventa son muy similares en los Estados miembros, siendo este análisis extrapolable al debate general sobre el uso de datos personales como pago por el acceso a servicios.

[210] Arts. 1445 y ss del Código Civil español.

terceros que muestra un aviso de cookies tampoco otorga al usuario una capacidad real de control, en la medida en que el funcionamiento del mercado de datos y los agentes específicos no es transparente ni conocido por el usuario medio. Por otro lado, en ocasiones la solicitud de consentimiento se presenta en términos de aceptar o rechazar la recepción de publicidad u otras funcionalidades de manera personalizada. Sin embargo, la negativa a prestar este consentimiento ¿es una negativa a que se recojan los datos o una negativa a que sean utilizados para funcionalidades de personalización? De este modo, incluso una concepción económica de los datos como precio por un producto o servicio no cumpliría algunos de los requisitos que la norma exige en la determinación del precio.

En relación con ello, también se abre el debate de si, por consiguiente, el consentimiento para el tratamiento de la información proveniente de cookies y tecnologías similares como precio debería ser restringido a aquellos servicios provistos sin contraprestación económica, como el acceso al contenido de un periódico digital, o también a aquellos otros servicios por los que el usuario ya paga un precio, como la realización de una compra de ropa a través del sitio web de la compañía.

En esencia, existen multitud de aristas que deben ser analizadas en aras de una mayor protección de los interesados y usuarios.

5.7. Espinacas vs azúcar refinado

Por naturaleza, el ser humano muestra una tendencia hacia aquellos comportamientos que le repercuten en recompensa a corto plazo, a pesar de que estas acciones no sean beneficiosas o incluso sean contrarias a los objetivos largoplacistas. Este es el mecanismo que subyace, por ejemplo, en la dificultad de muchas personas de poder iniciar un estilo de vida de comida sana a pesar de sabemos que conllevaría beneficios en el largo plazo, como un mayor estado general de salud. Al ser humano le gusta el azúcar refinado, de modo que en muchas ocasiones no se podrá resistir a comer los dulces que continuamente se le ofrecen, incluso siendo

consciente de que esta elección le aleja de su estado de bienestar óptimo futuro.

El primero de los motivos que explican esta tendencia es que el ser humano percibe el futuro de manera ambigua, abstracta y vaga. En cambio, el presente es tangible, concreto y podemos visualizarlo. De este modo, una recompensa actual y concreta es mucho más atractiva que una recompensa futura y abstracta, más aún en el caso de un castigo o penalización o riesgo futuro. El segundo motivo que explica nuestro comportamiento es que, cuando el individuo visualiza una recompensa inmediata, actúa a través de la impulsividad.

A todo ello se añade que, generalmente, las decisiones relacionadas con la prestación de consentimiento para el tratamiento de datos personales se toman en el curso de una acción no relacionada, como una compra a través de internet.

En el ámbito de los tratamientos masivos de datos, el azúcar refinado es equiparable a aquellas pequeñas recompensas que el usuario de un servicio recibe a cambio de aceptar el tratamiento de sus datos personales. Por ejemplo, la realización de una compra por internet o la recompensa de acceder al resultado de una aplicación que inserta un filtro sobre la fotografía de una persona para hacerla parecer envejecida a cambio de aceptar los términos de una política de privacidad que establece un tratamiento de datos personales invasivo.[211] El equivalente de las espinacas en este ejemplo sería leer detenidamente la política de privacidad, dedicarle tiempo a comprenderla y tomar una decisión plenamente informada, pues ello sería más positivo para la persona en el largo plazo. Sin embargo, la diversión a corto plazo es más atractiva que la precaución en torno a consentir el tratamiento de nuestros datos personales para prevenir posibles usos futuros nocivos.

[211] DEL CASTILLO, Carlos (2019): “FaceApp, el viaje por el mundo de tu cara y por qué la privacidad sigue `brutalmente incumplida´ por las apps”, en *ElDiario.es*.

6. Necesidad para la ejecución de un contrato

Los responsables del tratamiento que operen en el ámbito privado podrán legitimar la mayoría de sus actividades en alguna de las tres bases siguientes: consentimiento, ejecución de un contrato o interés legítimo. En la primera parte de este capítulo hemos centrado la atención al análisis del consentimiento, por ser uno de los instrumentos principales del derecho de la protección de datos. Ahora nos detendremos a realizar algunas apreciaciones en relación con el contrato como base de licitud.

El art. 6.1.b) RGPD establece como base de licitud del tratamiento el hecho de que este seA necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales. Recientemente, el CEPD ha publicado sus directrices en relación con la aplicación de esta base de licitud,[212] en las que incorpora algunas especificaciones relevantes para el tema que nos ocupa que serán la base de este epígrafe.

El debido cumplimiento de la normativa de protección de datos por parte del responsable del tratamiento cuando este utiliza la necesidad para la ejecución de un contrato o precontrato como base de legitimación para el tratamiento de dichos datos personales es independiente del cumplimiento de otros cuerpos normativos complementarios y también relevantes como la defensa de los derechos de los consumidores, la libre competencia o la validez del documento contractual *per se*. A pesar de ello, nuestro análisis se centrará únicamente en los aspectos relevantes desde el punto de la protección de datos personales.

La incorporación de esta base en el listado de circunstancias que legitiman el tratamiento en el art. 6 RGPD se alinea con la libertad de empresa recogida en el art. 16 de la Carta de Derechos Fundamentales de la UE, bajo la premisa de que, en determinadas circunstancias, el tratamiento de

[212] COMITÉ EUROPEO DE PROTECCIÓN DE DATOS (2019): *Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects*, de 8 de octubre.

datos personales se realiza en beneficio de ambas partes del contrato, pues de otro modo no sería posible ejecutarlo. Así, el art. 6.1.b) consagra una suerte de presunción de que los intereses de ambas partes de un contrato han sido considerados y se ven protegidos, por lo que el tratamiento de datos puede llevarse a cabo.

Ello, con independencia de si la contraprestación del contrato es un pago económico que realiza el interesado, o si el modelo de negocio no conlleva un desembolso económico del usuario, sino que la prestación del servicio se sostiene sobre la base de la venta de espacios publicitarios digitales. En dicho caso, el modelo de negocio se beneficia del tratamiento de datos personales que permiten el perfilado de los usuarios, conocer sus preferencias y personalizar el contenido publicitario que se le muestra, de modo tal que quien es expuesto a la publicidad tenga más posibilidades de completar una compra.

Por otro lado, la acción de redactar una determinada cláusula en un acuerdo contractual no legitima por sí mismo, un tratamiento de datos con una finalidad concreta en la ejecución de dicho contrato si no se cumplen las demás condiciones que impone el RGPD, entre ellas, la “necesidad” del tratamiento. Es decir, el hecho de que determinadas actividades de tratamiento hayan sido estipuladas a modo de obligación contractual no las hace “necesarias” para la satisfacción del objeto fundamental del contrato, de modo que la mera aceptación de un usuario de unos términos y condiciones no implica, *per se*, que el tratamiento cumpla los requisitos del art. 6.1.b), ni, por supuesto, con el resto de las obligaciones y principios del RGPD.

6.1. Cómo influye el avance técnico

Como ya comentábamos con anterioridad, los avances tecnológicos de los últimos años hacen que cada vez sea más sencillo recopilar datos, por ejemplo, a través de rastreadores como *cookies*. Asimismo, los modos por los que se produce la recogida de los datos, su análisis y su aplicación en el entorno digital actual no son claros para los usuarios de servicios en

línea, aplicaciones, páginas web o dispositivos conectados. Por este motivo, como destaca el CEPD, "en la práctica es casi imposible para un interesado poder ejercer una decisión informada sobre el uso de sus datos". Todo ello es, además, cuanto más importante por el hecho de que, con carácter general, las cláusulas contractuales que sostienen los modelos de negocio en línea no son negociadas de manera individual.

6.2. Limitación de la finalidad y minimización de datos

La facilidad técnica unido a la expectativa de mayores beneficios hace que un responsable tenga incentivos para querer recoger una cantidad cada vez mayor de datos, que le permitan realizar perfiles más precisos y traducirlos en beneficios económicos. Ello puede desembocar en la redacción de cláusulas contractuales ambiguas y poco específicas sobre las que se pretenda legitimar una recolección extensa de datos y su posterior tratamiento. Ello contravendría los principios de limitación de la finalidad (art. 5.1.b) y de minimización de datos (art. 5.1.c)). De hecho, como ya ha sido expresamente señalado por el GT29, la redacción ambigua de la finalidad del tratamiento corrompe estos principios, y por tanto no son válidas expresiones de finalidad como "la mejora de experiencia de usuario", "actividades de marketing", etc.[213] ¿Cómo limitar esta posible tendencia expansiva?

6.3. La necesidad del tratamiento

La garantía principal con la que cuenta el interesado en relación con la aplicación del art. 6.1.b como base de licitud del tratamiento es el requisito de que dicho tratamiento de datos sea "necesario" para la ejecución del contrato o precontrato. Requisito que, por otra parte, está directamente relacionado con los mencionados principios de limitación de la finalidad (art. 5.1.b) y de minimización de datos (art. 5.1.c)). En el capítulo siguiente comentaremos algunos de los aspectos principales de este requisito de

[213] GRUPO DE TRABAJO DEL ARTÍCULO 29 (2013): *Opinion 03/2013 on Purpose Limitation* (WP 203), de 2 de abril, p. 15–16.

necesidad, de modo que aquí únicamente nos centraremos en cómo ello influye en la ejecución contractual en entornos en los que se pueden aplicar tecnologías de análisis masivo de datos.

El requisito de necesidad conlleva que el responsable deba poder argumentar los motivos por los que la actividad de tratamiento es realmente necesaria para la prestación de un determinado servicio, interpretado de manera estricta. De este modo, el hecho de que el tratamiento favorezca los intereses del responsable no será suficiente. Debe ser también preciso para favorecer los intereses de la parte contratante, en el sentido de que esta pueda ver cumplidas sus expectativas contractuales. Por ello, si existe un medio menos intrusivo para conseguir la misma finalidad, el tratamiento no será necesario y no podrá basarse en el art. 6.1.b. En otras palabras, el estándar a cumplir en este caso debe ser que el responsable pueda argumentar la existencia de un nexo de causalidad de modo tal que, sin dicha actividad de tratamiento, la prestación contractual no puede ser atendida.

En este sentido, surge la cuestión de qué sucede si el contrato está formado por varios servicios diferentes. En el caso de que todos ellos sean dependientes unos de otros, será más sencillo analizar si el tratamiento de los datos personales cumple el requisito de necesidad. Sin embargo, cuando existan diferentes servicios que pueden ser prestados de manera independientes, las actividades de tratamiento deben ser analizadas por separado para concluir qué tratamientos pueden basarse en la necesidad para prestar el servicio o qué servicios han sido solicitados por el interesado de toda la gama disponible.

6.4. Qué ocurre cuando no se cumplen los requisitos

Si el tratamiento no es necesario para la ejecución de un contrato, el responsable encontrará mayor encaje en el uso de otras bases de legitimación, en particular, el consentimiento o el interés legítimo. De hecho, si el responsable puede recurrir al consentimiento, es muy posible que dicho tratamiento no sea, por consiguiente, necesario para la ejecución del

contrato, con lo que en multitud de ocasiones se tratará de bases de legitimación incompatibles.

A pesar de ello, la relación entre las bases del consentimiento y la ejecución de un contrato no es siempre pacífica. Tal y como señala el CEPD en sus directrices, en ocasiones los interesados o incluso los responsables tienen la sensación de que al aceptar unos términos y condiciones se está prestando consentimiento y la base de licitud es el art. 6.1.a) en lugar del 6.1.c, con las consecuencias legales que ello tiene, como el ejemplo, la existencia del derecho a retirar en consentimiento en cualquier momento, que no tiene derecho equivalente bajo el contrato.

Por otro lado, en esta relación consentimiento-contrato también es relevante el art. 7.4 RGPD que diferencia claramente entre el consentimiento prestado libremente o la necesidad para la ejecución de un contrato, al establecer que ha de analizarse si la prestación de un servicio o ejecución de un contrato se hace condicional a la aceptación para tratar datos personales que no son necesarios dicho contrato.

6.5. Fases del big data

Todo lo anterior nos conduce a la conclusión de que cuando los datos hubieran sido recabados por el responsable en la Fase 1-rRecolección con la finalidad concreta de dar ejecución a un contrato, estos datos únicamente podrán ser utilizados para la Fase 2-Análisis y Fase 3-Aplicación (realización del perfil de la persona) si ello fuera necesario o imprescindible, o si el responsable contase con otra base de licitud. De hecho, en la medida en que el contrato viniera ejecutándose con normalidad antes del inicio de la actividad de analítica de los datos, es muy posible que la Fase 2 no fuera una actividad necesaria, sino útil o favorable para el interés del responsable. Por ello, el mero hecho de que el responsable pueda obtener un beneficio en la prestación de servicios personalizados no hace que dicho tratamiento sea necesario para la prestación de su servicio.

Así, por ejemplo, el CEPD considera que, con carácter general, la ejecución de un contrato no podrá legitimar actividades de mejora del servicio (que se realizan analizando datos sobre, por ejemplo, cómo interactúan los clientes dentro de una página web, etc.). Tampoco para la realización de perfiles, pues el interesado acude a la organización para recibir un servicio determinado, no con la finalidad de ser perfilado con motivo de recibir publicidad personalizada, incluso aunque la publicidad sea el modo en que dicho servicio se financia.

Por su parte, en el caso concreto de la personalización de contenidos, el tratamiento podría ser -aunque no siempre necesariamente-, necesario para la ejecución de un contrato. Ello dependerá de las características del servicio. Así, por ejemplo, si la personalización únicamente se realiza para aumentar el grado de implicación del usuario en el servicio, posiblemente no será necesaria. Por el contrario, pensemos en un servicio consistente, precisamente, en el acceso a un motor de recomendación musical cuyo valor diferencial en el mercado es que cada usuario recibe propuestas de canciones acordes a lo que previsiblemente puede gustarle, así como avisos de conciertos y otros eventos que vayan a tener lugar cerca de su lugar de residencia. En este caso, el núcleo esencial del servicio es la personalización y, por tanto, el tratamiento de los datos necesarios para poder perfilar a la persona e inferir sus preferencias sí será necesario para la ejecución del contrato y acorde con las expectativas del usuario.

En todo caso, la intensidad de la recogida de los datos, su análisis y su aplicación para llevar a cabo el perfilado también jugará un papel relevante. De hecho, el CEPD expresa que “los datos personales no pueden ser considerados como una mercancía comercializable. Incluso si el interesado está de acuerdo con el tratamiento de datos personales, no puede renunciar a sus derechos fundamentales a través de este acuerdo”. Esta aseveración va, de hecho, en línea sobre lo ya expresado en relación con el consentimiento como pago por servicios.

6.6. Conclusión

Esta base de licitud, por tanto, se diferencia del consentimiento en varios aspectos vertebrales. Por un lado, no permite ejercer un control sobre el uso de los datos personales en el mismo sentido que lo permite el consentimiento, en tanto las cláusulas contractuales no son, en su mayoría, negociadas de manera individual y adaptadas al caso concreto. Sin embargo, los interesados son vestidos de otro tipo de garantías que les permiten mantener la seguridad de que el tratamiento será lícito. En primer lugar, la necesidad de que el tratamiento de datos deba ser "necesario". En segundo lugar, el hecho de que la mera incorporación de una cláusula en el contrato relativa al tratamiento de datos personales no legitima la actividad, sino que deben concurrir además el resto de las obligaciones que impone el RGPD. Cuando estas circunstancias se dan, la norma presume que los intereses de ambas partes -interesado y responsable- se encuentran en equilibro, de modo que se da luz verde al tratamiento.

Ello es relevante, y de hecho no se trata de la única base que toma en cuenta el equilibro entre los intereses de las partes. El art. 6.1.f) que regula el interés legítimo, parte de la misma premisa, si bien en relación con circunstancias para las que no se puede presumir la existencia de un equilibrio de intereses, sino que este deberá ser demostrado. Esta base será el objeto central de estudio del siguiente capítulo.

7. La regla del consentimiento en la propuesta de Reglamento e-Privacy

La Estrategia para el Mercado Único Digital de la Unión Europea tiene como objetivo aumentar la confianza y la seguridad de los servicios digitales. Para ello, la reforma del marco regulador de protección de datos personales de la Unión Europea, a través de la introducción del RGPD, constituyó un paso esencial para aumentar la confianza en la seguridad de los servicios

digitales.[214] Tras la reforma del RGPD, la estrategia también incluyó una revisión de la Directiva 2002/58/CE[215]. De hecho, el 10 de enero de 2017, la Comisión Europea presentó una propuesta de Reglamento sobre Privacidad y Comunicaciones Electrónicas (Reglamento e-Privacy),[216] por el que se derogará la Directiva e-Privacy.[217] El futuro Reglamento e-Privacy tiene como objetivo establecer un nuevo marco legal en materia de protección de datos personales completando y precisando el RGPD.[218] La propuesta de Reglamento e-Privacy tiene en cuenta los importantes avances tecnológicos y económicos en el sector de las comunicaciones electrónicas y tiene por objeto modernizar los principios existentes con arreglo a las nuevas prácticas.[219] Su objetivo es promover un alto nivel de protección de la confidencialidad en las comunicaciones, independientemente de la tecnología utilizada.[220]

El 26 de octubre de 2017, el Parlamento Europeo votó a favor de las enmiendas propuestas por la Comisión de Libertades Civiles, Justicia y Asuntos de Interior (LIBE) en sesión plenaria. La versión final del Consejo no ha sido publicada en el momento de escribir estas líenas.

---

[214] COMISIÓN EUROPEA (2015): *Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, "Una estrategia para el mercado único digital de Europa*.

[215] Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas), modificada en dos ocasiones por la Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, y por la Directiva 2009/136/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009 (la Directiva e-Privacy).

[216] El contenido de las primeras secciones de este epígrafe han sido objeto de publicación en GIL GONZÁLEZ, Elena; DE HERT, Paul; PAPAKONSTANTINOU, Vagelis (2020): "The proposed e-Privacy Regulation, The Commission's and the Parliament's drafts at crossroad?", en *Data Protection and Privacy, Data Protection and Democracy*, Hart Publishing, Oxford, 2020.

[217] Propuesta de Reglamento del Parlamento Europeo y del Consejo, de 10 de enero de 2017 sobre el respeto de la vida privada y la protección de los datos personales en el sector de las comunicaciones electrónicas y por el que se deroga la Directiva 2002/58/CE (Reglamento sobre la privacidad y las comunicaciones electrónicas).

[218] Considerando 5 de Propuesta de Reglamento e-Privacy.

[219] Considerando 6 de Propuesta de Reglamento e-Privacy.

[220] Considerando 14 de Propuesta de Reglamento e-Privacy.

7.1. La relación entre el Reglamento e-Privacy y el RGPD

La UE, en sus esfuerzos por actualizar su marco normativo de protección de datos y las normas conexas, tenía como objetivo, entre otras cosas, garantizar una aplicación más coherente de las normas en la Unión, para alcanzar un mayor grado de protección de las personas y de seguridad jurídica para las organizaciones.

El RGPD establece la *lex generalis* en materia de protección de datos en Europa. Por lo tanto, se aplica a todas las cuestiones relacionadas con el tratamiento de datos personales, independientemente del sector, siempre que no exista una ley sectorial específica que aplicar. La comunicación electrónica es uno (si no el único) de estos ámbitos. En este sentido, la propuesta de Reglamento e-Privacy constituye una *lex specialis* en relación con el RGPD, precisándolo y completándolo en lo que respecta a los datos de comunicaciones electrónicas que se consideran datos personales. En particular, en el Reglamento e-Privacy se regulan de manera más específica las áreas de la publicidad no solicitada, las tecnologías de seguimiento (por ejemplo, las *cookies*) y la confidencialidad. Sin embargo, en aquellas cuestiones en las que la propuesta de Reglamento e-Privacy no se pronuncie, se aplicará por defecto el RGPD (por ejemplo, algunas obligaciones de los responsables del tratamiento). No obstante, se podría argumentar que la mayoría de las operaciones de tratamiento cubiertas por el Reglamento e-Privacy implican datos personales y, por lo tanto, estarían cubiertas por el Reglamento RGPD, que, como veremos, regula de manera más flexible.

Además, la elección de un Reglamento en lugar de una Directiva como instrumento jurídico tanto para el RGPD como para el nuevo marco de e-Privacy está orientada a la creación de un régimen más uniforme en todos los Estados miembros. Los reglamentos suprimen la necesidad de promulgar legislación nacional, aumentando de esta manera la coherencia entre e-Privacy y el RGPD. Esta es también la razón por la que las mismas

autoridades de control independientes son responsables de supervisar el cumplimiento de ambos conjuntos de normas.

Por último, mientras que el RGPD garantiza la protección de los datos personales (art. 8 de la Carta de los Derechos Fundamentales de la UE), el Reglamento e-Privacy garantiza la confidencialidad de las comunicaciones (art. 7 de la Carta), que también pueden contener datos no personales y datos relativos a una persona jurídica.

7.2. Ámbito de aplicación del Proyecto de Reglamento e-Privacy

El ámbito de aplicación de la propuesta de Reglamento e-Privacy es más amplio que el de la Directiva e-Privacy, aunque todavía se están debatiendo algunas cuestiones.

En primer lugar, se ha llevado a cabo una ampliación del ámbito de aplicación territorial. De hecho, al igual que el RGPD, el Reglamento e-Privacy pretende tener un efecto extraterritorial, y regula las actividades, aunque el tratamiento no tenga lugar en la UE o los proveedores no estén situados en la UE. Esto puede llevar a los proveedores a designar a un representante en la Unión, pero también podría provocar el bloqueo geográfico de determinados servicios.

Por su parte, el ámbito de aplicación material también ha sido ampliado mediante la inclusión explícita de los proveedores de servicios libres, la aclaración de determinadas definiciones, como la de "servicios de comunicaciones electrónicas" y la inclusión explícita de las interacciones de máquina a máquina. Esto tiene en cuenta acontecimientos recientes, como la expansión de las comunicaciones en el entorno digital y el Internet de las Cosas, con el fin de crear unas condiciones de competencia equitativas.

7.3. Confidencialidad de las comunicaciones

La Directiva e-Privacy preveía que los Estados miembros garantizaran la confidencialidad de las comunicaciones y de los datos de tráfico

relacionados en las redes y servicios públicos de comunicaciones. Por lo tanto, se prohibió escuchar, pinchar, almacenar o participar en otros tipos de interceptación o vigilancia de las comunicaciones y de los datos de tráfico relacionados sin el consentimiento del ciudadano afectado (excepto cuando esté legalmente autorizado). Esta disposición cubría tanto el contenido de la comunicación (por ejemplo, la voz en una llamada telefónica) como los datos de tráfico relacionados (por ejemplo, la hora de la llamada). Estas normas no eran plenamente eficaces para proteger la confidencialidad de las comunicaciones. Por ejemplo, algunas de las razones fueron la exclusión de los servicios[221] OTT (denominados en inglés "Over-the-Top" y conocidos por su sigla en inglés "OTT") o la redacción obsoleta (que no incluía intrusiones automáticas sin intervención humana).

7.3.1. *Cambio de terminología*

El nuevo Reglamento elimina el concepto de datos de tráfico y datos de localización y utiliza en su lugar "metadatos",[222] que parece ser un concepto más amplio y que se contrapone al de contenido. El Reglamento e-Privacy, tal y como fue redactado en su borrador inicial por la Comisión, tiene por objeto proteger tanto el contenido de las comunicaciones como los metadatos relacionados.

Esta nueva definición engloba lo que la Directiva e-Privacy definió como datos de tráfico y como datos de localización. La razón de esta fusión radica en la creciente generación de datos y en la capacidad informática para almacenarlos y analizarlos. Estos avances tecnológicos hicieron que, aunque se suprimieran algunos datos de las comunicaciones electrónicas, el análisis de los datos de tráfico y de localización procedentes de múltiples

[221] Si bien es cierto que el RGPD regula el tratamiento de datos personales a través de servicios OTT, el nuevo Reglamento e-Privacy debe garantizar la confidencialidad de las comunicaciones. Esto es necesario para proteger a los usuarios y garantizar unas condiciones de competencia equitativas para todos los proveedores, independientemente de la tecnología utilizada, en particular en la era del Internet de las Cosas.

[222] El SEPD había solicitado que se adoptara el concepto de metadatos en SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS, Opinion 5/2016, Preliminary EDPS Opinion on the review of the ePrivacy Directive (2002/58/EC), de 22 de julio, p. 13.

fuentes pudiera mostrar patrones emergentes que podrían dar lugar posteriormente a la creación de perfiles individuales y grupales, lo que aumentaría el impacto potencial en la privacidad. Esto también se trata de un punto especialmente importante, debido a las formas encubiertas e inesperadas que podrían llevar a la recogida y el análisis masivo de datos.

La razón de la protección de los datos de las comunicaciones electrónicas es que el contenido de las comunicaciones electrónicas puede revelar información muy delicada o sensible sobre las personas físicas que participan en la comunicación (experiencias personales, emociones, preferencias sexuales o políticas, etc.), cuya divulgación tiene claras implicaciones para la privacidad.[223] Además, los metadatos derivados de las comunicaciones electrónicas también pueden revelar información muy delicada o sensible y de carácter personal, como reconoció expresamente el TJUE.[224]

7.3.2. *La importancia de estas disposiciones por el avance tecnológico*

La protección explícita tanto del contenido como de los metadatos es de enorme importancia hoy en día. En el pasado, la confidencialidad de los datos de contenido podía considerarse más relevante debido a su mayor potencial para revelar información sobre el comportamiento de los usuarios finales, sus pensamientos o su inclinación hacia determinadas ideas. Sin embargo, las tecnologías actuales permiten una recogida más fácil y barata de grandes cantidades de metadatos a partir de los cuales también se pueden observar patrones y comportamientos. Por lo tanto, fragmentos individuales de metadatos que podrían haber sido inocuos hace años ahora pueden exponer información privada, y muchos de ellos también pueden clasificarse como datos personales. Además, se puede efectuar todo lo

[223] Considerando 2 de Propuesta de Reglamento e-Privacy.

[224] Exposición de motivos de la Propuesta de Reglamento e-Privacy, p. 4. Véase TJUE, asuntos acumulados C-293/12 y C-594/12 *Digital Rights Ireland y Seitlinger y otros,* ECLI:EU:C:2014:238; TJUE, asuntos acumulados C-203/15 y C-698/15 *Tele2 Sverige AB y Secretario de Estado del Ministerio del Interior,* ECLI:EU:C:2016:970.

anteriormente expuesto incluso sin observar el contenido de la comunicación, lo que representa la innovación del mundo actual. Por ejemplo, existe la posibilidad de deducir las creencias religiosas de una persona si se puede acceder a los datos de localización de su teléfono, en los que se revele que acude a una iglesia específica cada semana. Existen innumerables ejemplos. Además, mientras que los datos de contenido estarán, casi siempre, en un formato no estructurado y, por lo tanto, serán más difíciles de analizar, los metadatos pueden recogerse en formatos estructurados y analizarse en tiempo (casi) real. Asimismo, es importante señalar los torrentes cada vez mayores de datos procedentes del Internet de las Cosas y de la sociedad conectada. Esto amplía la capacidad de analizar los datos del usuario final en un intento de monetizarlos, con la consiguiente violación de la privacidad. Por lo tanto, fragmentos individuales de datos que podrían haber sido inocuos hace años ahora pueden exponer información privada, y muchos de ellos también pueden clasificarse como datos personales. Estas razones justifican la necesidad de una definición más clara de los metadatos y de su protección.

7.3.3. *Regla general*

Como resultado, el Reglamento e-Privacy mantiene la regla general de confidencialidad de las comunicaciones electrónicas y permite excepciones limitadas, en virtud de las cuales pueden tratarse los metadatos o el contenido de las comunicaciones electrónicas (art. 5 y 6 del Reglamento e-Privacy). Ambas categorías de datos (contenido y metadatos) pueden utilizarse cuando resulte necesario (por ejemplo, para garantizar la seguridad de la red).

7.3.4. *Metadatos*

Además, los metadatos también pueden utilizarse cuando sea necesario para ciertos fines establecidos por la norma (por ejemplo, para fines de facturación o para cumplir las obligaciones en materia de calidad del

servicio[225] de acuerdo con la legislación específica; por ejemplo, cuando el proveedor necesite adaptar la calidad de una imagen a la configuración de la pantalla del usuario). Aparte de los casos de necesidad tasados por la norma, los metadatos solo podrán ser tratados con el consentimiento del usuario para la prestación de determinados fines o servicios específicos, cuando dichos servicios no puedan cumplirse sin los datos en cuestión (por ejemplo, cuando se muestren al usuario las gasolineras más baratas de la zona mediante el seguimiento de su ubicación en tiempo real).

7.3.5. *Contenido*

Sin embargo, el contenido de las comunicaciones electrónicas solo puede tratarse con consentimiento, siempre que se cumplan algunos requisitos adicionales, debido a su carácter delicado y al hecho de que ninguna razón técnica justificaría tal interferencia con la privacidad.

Sin embargo, ¿para qué fines se puede solicitar el consentimiento? El consentimiento podría solicitarse en dos casos. En primer lugar, el consentimiento del usuario podría solicitarse para la prestación de servicios específicos solicitados por dicho usuario, siempre que el servicio no pueda ser prestado sin el tratamiento de dicho contenido "por el proveedor", tal y como se añade en el texto modificado del Parlamento.[226] De conformidad con esta disposición, los proveedores no pueden solicitar el consentimiento para el uso de más datos de contenido de los necesarios para los fines de los servicios, y estos deben ser específicos. Esta apreciación es relevante, pues, de facto, añade un principio de necesidad a la base del consentimiento, que es la única que bajo el RGPD parecía no tenerlo. Esto evitará, por ejemplo, que un proveedor de correo electrónico transfiera sus datos a una tercera empresa especializada en algoritmos de tratamiento de lenguaje natural y que, por lo tanto, podría estar interesada en acceder al texto de sus correos electrónicos para mejorar su servicio.

[225] Art. 6.2.a) de Propuesta de Reglamento e-Privacy.

[226] Art. 6.3.a) de Propuesta de Reglamento e-Privacy, enmienda del Parlamento 78.

En segundo lugar, también podría solicitarse a todos los usuarios el consentimiento para utilizar el contenido de los datos de las comunicaciones electrónicas para fines específicos con arreglo al actual proyecto de Reglamento e-Privacy, siempre que dichos fines no puedan lograrse utilizando información anónima y que el proveedor haya consultado a la autoridad de control de conformidad con los art. 36.2 y 36.3 del RGPD. Esto englobaría aquellos casos en los que los servicios no sean solicitados por el propio usuario, sino más bien ofrecidos por el proveedor. Esto sucede cuando una red social presenta a los usuarios una funcionalidad con la que escanea sus imágenes a través de la red para etiquetarlo automáticamente o para enviarle alertas cuando alguien suba una imagen donde aparece.

Por último, la enmienda del Parlamento establece una excepción en virtud de la cual no se exigirá el consentimiento de todos los usuarios si el tratamiento se realiza en el marco de un servicio solicitado expresamente por uno de ellos, con su consentimiento y cuando no afecte negativamente a los derechos e intereses de los demás usuarios. Esto simplificaría el proceso de obtención del consentimiento para las prácticas exclusivamente personales y crearía una suerte de exención doméstica.[227] De este modo, la propuesta muestra una clara preferencia por el consentimiento como base legal para el tratamiento, al mismo tiempo que intenta evitar la fatiga de consentimiento del usuario.

Como garantía adicional para los usuarios, no se permitiría a los proveedores pedir a los clientes que renuncien a sus derechos de privacidad consintiendo prácticas invasivas.

[227] El GT29 había solicitado una excepción doméstica en el tratamiento de datos de comunicaciones electrónicas (tanto de contenido como de metadatos) con fines puramente personales, como el uso de servicios de texto a voz. Esto significaría que, para el uso de los datos de las comunicaciones electrónicas con cualquier otro fin, como la publicidad comportamental, debería solicitarse el consentimiento de todos los usuarios. Véase GRUPO DE TRABAJO DEL ARTÍCULO 29, Dictamen 01/2017, p. 3. El Parlamento siguió esta recomendación solo parcialmente, ya que el consentimiento de todos los usuarios *no* fue introducido como requisito para el uso de metadatos, sino solo del contenido. Por otra parte, para el uso de los datos de contenido, se introdujo la excepción doméstica.

A modo de ejemplo, la autoridad sueca de protección de datos inició un procedimiento de reclamación de información a Google sobre el uso de patrones oscuros para obtener el consentimiento de los usuarios para acceder a los datos de localización, preocupados por el hecho de que Google pueda estar utilizando "un diseño engañoso, información engañosa y presiones repetidas para manipular a los usuarios con el fin de que permitan el seguimiento constante de sus movimientos".[228]

7.3.6. Aproximación más limitada que RGPD

Al exigir el consentimiento para el tratamiento de los datos de comunicaciones electrónicas, la legislación sobre e-Privacy opta por un enfoque más restrictivo que el del RGPD, que podría permitir un conjunto más amplio de bases de licitud, como la ejecución de un contrato o el interés legítimo, así como usos secundarios de los datos cuya finalidad pueda considerarse no incompatible.

7.4. Protección de equipos terminales

La Directiva e-Privacy tiene como objetivo proteger la confidencialidad de la información contenida en los equipos terminales de los usuarios, como ordenadores o smartphones, exigiendo el consentimiento del usuario antes de almacenar o acceder a la información. Esta información incluye cookies, balizas, spyware, imágenes y vídeos, contenido de correos electrónicos, calendario, etc.

El art. 5.3 de la Directiva e-Privacy (una de las disposiciones más polémicas de la Directiva, a menudo conocida como la "disposición de las cookies") permite el uso de cookies y otras tecnologías de seguimiento similares siempre que el usuario haya dado su consentimiento informado. Esto condujo a la llamada fatiga de consentimiento, derivada del uso cada vez mayor de los banners de cookies, que hace que los usuarios se enfrenten

[228] Véase solicitud de información completa: DATAINSPEKTIONEN (2019) : *Request for Reply and Further Clarification*.

a solicitudes de consentimiento que ni leen ni entienden, mientras que algunas cookies se instalan sin consentimiento.

La norma relativa al consentimiento de la Directiva e-Privacy no protegía correctamente a los usuarios. Tenía un alcance a veces demasiado amplio, ya que algunas prácticas no intrusivas necesitaban consentimiento (como la instalación de cookies analíticas de origen), lo que causaba fatiga entre los usuarios, y otras demasiado limitado, ya que no abarcaba claramente las últimas tecnologías de rastreo (como la huella digital). Hoy en día, el rastreo no puede realizarse únicamente a través de medios activos, mediante el "almacenamiento" o el "acceso" a los dispositivos de los usuarios y la obtención de información a través de cookies y tecnologías similares. También puede tener lugar de forma pasiva, mediante el uso de identificadores "emitidos" por los dispositivos de los usuarios, como el seguimiento wifi o la huella digital de los dispositivos.

7.4.1. *Información almacenada en los equipos terminales de los usuarios*

La regla general del art. 8.1 del Reglamento e-Privacy establece la prohibición de invadir la privacidad de los usuarios a través de tecnologías de rastreo que utilizan los dispositivos como vehículo, como las cookies, pero se prevén excepciones. Se permite el seguimiento cuando sea necesario (por ejemplo, para llevar a cabo la transmisión, o para medir la audiencia web con cookies de origen) o cuando el usuario conceda su consentimiento. Esta disposición tiene como objetivo proteger la información contenida en los dispositivos de los usuarios. Como tal, no solo engloba la instalación de cookies no deseadas o innecesarias en los dispositivos de los usuarios, sino también la instalación de *malware*, huellas digitales de dispositivos o tecnologías que permitan, por ejemplo, que una aplicación active un micrófono o una cámara para recoger información

El cambio más importante que ha sufrido el Reglamento e-Privacy debido a la intervención del Parlamento es la inclusión de una prohibición explícita de las denominadas barreras de rastreadores. Estas últimas presentan a

los usuarios una elección que pueden "tomar o dejar" entre la privacidad y el acceso a un servicio, es decir, cuando los proveedores de servicios deniegan a los usuarios el acceso a un servicio o funcionalidad basándose en que no hayan dado su consentimiento para tratar, almacenar y recoger información que no sea necesaria para la prestación de dicho servicio o funcionalidad. Este rastreo se realiza habitualmente a través de cookies y tecnologías similares para ofrecer una publicidad más dirigida a los usuarios, lo que sin duda es más eficaz que otros tipos de publicidad menos personalizada, generando así mayores ingresos. Existe un debate en torno a la prohibición o no de las llamadas barreras de rastreadores.

7.4.2. *Información emitida por los equipos terminales de los usuarios*

La Directiva e-Privacy no contiene ninguna disposición para proteger la confidencialidad de la información "emitida" por los equipos terminales de los usuarios. El art. 8.2 del Reglamento e-Privacy incluye ahora disposiciones relativas al seguimiento de la información emitida por los dispositivos de los usuarios, como las señales wifi o bluetooth enviadas por smartphones y otros dispositivos, que permiten el seguimiento de la localización. Por lo tanto, esta protección engloba las comunicaciones de máquina a máquina cuando la información está relacionada con un usuario (lo que tiene cada vez más relevancia en la época del Internet de las Cosas).

Esta información solo puede utilizarse en casos excepcionales: cuando sea necesario y cuando los usuarios hayan sido informados. Mientras que la versión de la Comisión solo exige informar a los usuarios y no les otorga un derecho de exclusión voluntaria. Esto habría reducido el nivel de protección establecido en el RGPD, en el que, en una situación similar, debería concederse un derecho de exclusión voluntaria en caso de que no fuera necesario el consentimiento. Por consiguiente, el Parlamento endureció los requisitos para solicitar el consentimiento. Esta adición es importante ya que eleva significativamente los requisitos para que los proveedores puedan tratar los datos de los usuarios. De lo contrario, el mero hecho de

exigir un aviso legitimaría la recogida de información de los usuarios capturada a través, por ejemplo, de señales wifi, que podrían revelar la ubicación y otros datos privados de las personas de forma inadvertida e incentivarían el uso ya de por sí elevado de sensores ubicuos

7.5. La cuestión del consentimiento

El consentimiento es el fundamento jurídico central en el marco de la e-Privacy, que permite varias actividades de tratamiento si los usuarios han dado su consentimiento. Sin embargo, la evaluación REFIT[229] puso de manifiesto que algunas disposiciones han impuesto una carga innecesaria a empresas y consumidores. Por ejemplo, la norma del consentimiento para proteger la confidencialidad de los equipos terminales no logró su objetivo. Existe un amplio reconocimiento de que, hoy en día, los usuarios finales se enfrentan a solicitudes de aceptación de cookies y otras tecnologías de seguimiento que no se leen ni se entienden, lo que conlleva situaciones en las que los usuarios aceptan las condiciones sin darse cuenta de las consecuencias. De esta manera, es posible que el seguimiento se esté llevando a cabo sin el consentimiento legal. La norma relativa al consentimiento de la Directiva de e-Privacy tiene un alcance a veces demasiado amplio, ya que engloba prácticas que no afectan a la privacidad, y a veces demasiado limitado, ya que no abarca claramente algunas técnicas de seguimiento (por ejemplo, la huella digital de dispositivo) que pueden no entrañar el acceso o almacenamiento en el dispositivo.

La Comisión, en su propuesta de Reglamento e-Privacy, pretende abordar estas cuestiones.[230] El art. 9.1 del Reglamento e-Privacy establece que la definición de consentimiento sea la del RGPD. Esto sigue la línea marcada por la Directiva e-Privacy, que también se refiere a la ley de protección de

[229] La evaluación REFIT proporciona los resultados del estudio realizado por el programa de adecuación y eficacia de la reglamentación para evaluar la salud y el estado de las normas actuales e identificar áreas de mejora. Los resultados de este estudio fueron presentados por la Comisión Europea junto con la Propuesta de un nuevo Reglamento e-Privacy. Véase COMISIÓN EUROPEA (2017): *Ex-post REFIT evaluation of the ePrivacy Directive 2002/58/EC* SWD(2017), de 10 de enero.

[230] Exposición de motivos de Propuesta de Reglamento e-Privacy, p. 5.

datos para la definición de consentimiento. Según el RGPD, el consentimiento se define como "toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen" (art. 4.11 del RGPD).

Sin embargo, los usuarios a menudo se enfrentan a solicitudes de consentimiento que no son sencillas y algunas de ellas están diseñadas incluso para ser poco claras. Por esta razón, el art. 9.2 del Reglamento e-Privacy tiene por objeto proporcionar a los usuarios la posibilidad de expresar su consentimiento de manera más sencilla. En concreto, el art. 9.2, tal como ha sido redactado por la Comisión, establece lo siguiente "Sin perjuicio de lo dispuesto en el apartado 1, cuando sea técnicamente posible y factible, a los efectos del artículo 8, apartado 1, letra b), el consentimiento *podrá* expresarse mediante la configuración técnica adecuada de una aplicación informática que permita acceder a Internet" (énfasis añadido).

De esta manera, si es técnicamente factible, el consentimiento para las cookies y otras tecnologías de seguimiento similares reguladas por el art. 8.1.b puede expresarse a través de la configuración técnica del navegador web o de cualquier otra aplicación informática (o software) que proporcione acceso a internet. Estas son las denominadas normas "no realizar seguimiento" (*Do Not Track* o DNT en inglés). Se trata de un mecanismo que permite a las personas expresar su elección sobre las cookies y otras tecnologías de seguimiento configurando su navegador para ello (o utilizando formas similares que se aplican a cualquier otra tecnología para centralizar la configuración del consentimiento). En la práctica, las normas DNT significan que los usuarios pueden decir a su navegador de una sola vez cuáles son sus preferencias de cookies, en lugar de dar su consentimiento cada vez que visitan un sitio web. Esto evitaría que los usuarios recibieran un sinfín de banners de cookies (o solicitudes de consentimiento similares) cada vez que lleven a cabo una acción rutinaria como abrir un sitio web. En cambio, una vez que el usuario haya activado la configuración de DNT, el navegador envía una señal a los sitios web, las

empresas de análisis, las redes publicitarias, los proveedores de *plug-in* y otros servicios web encontrados durante la navegación y solicita que la aplicación web se abstenga de realizar el seguimiento de esa persona.[231]

Sin embargo, según la redacción de la Directiva e-Privacy, algunos sitios web pueden decidir legalmente hacer un seguimiento de los usuarios, ya que no están obligados a respetar esa configuración. O peor aún, algunos sitios web podrían optar por actuar como si las señales DNT significaran "no enviar anuncios" en lugar de "no recoger y tratar datos sobre mí y este dispositivo".[232] Por lo tanto, la Comisión afirma que la centralización del consentimiento en los software, junto con la ampliación de la excepción relativa al consentimiento de las cookies (es decir, la no exigencia de consentimiento para las cookies necesarias o inocuas), reduciría significativamente el número de notificaciones a las que se enfrentan los usuarios, lo que evitaría la actual fatiga de consentimiento y supondría un ahorro en los costes para muchos negocios que podrían trabajar sin banners de cookies.[233]

Sin embargo, el informe LIBE destacó que la redacción de la Comisión tenía el inconveniente de hacer que las normas DNT fueran opcionales y aconsejaba hacerlas obligatorias. También recomendó que las normas DNT se aplicaran a todas las tecnologías de seguimiento para englobar otros contextos como el Internet de las Cosas. Tras dicha recomendación, el texto propuesto por el Parlamento refuerza las disposiciones sobre las normas DNT de varias maneras. En primer lugar, haciéndolas vinculantes en lugar de opcionales. En segundo lugar, pidiendo que la redacción sea más neutra desde una perspectiva tecnológica, ya que ya no se refiere al software, sino a la expresión más amplia de "especificaciones técnicas". En tercer lugar, el consentimiento detallado se proporciona ahora

[231] FUTURE FOR PRIVACY FORUM, *What is Do Not Track*.

[232] EDWARDS, Lilian (2018): “Data Protection and ePrivacy: From Spam and Cookies to Big Data, Machine Learning and Profiling”, en Lilian Edwards (ed.), *Law, Policy and the Internet*, Hart.

[233] Exposición de motivos de de Propuesta de Reglamento e-Privacy, p. 6.

permitiendo "un consentimiento específico para finalidades específicas en relación con proveedores específicos de servicios". Por último, los ajustes pueden utilizarse no solo para conceder el consentimiento, sino también para retirarlo.

No obstante, se observa que las disposiciones relativas a las normas DNT de la Propuesta de Reglamento e-Privacy tanto de la Comisión como del Parlamento se refieren únicamente al art. 8.1.b, por lo que únicamente proponen proteger la información almacenada en los equipos terminales (por ejemplo, las cookies y los rastreadores similares). Esto dejaría a las actividades englobadas en el art. 8.2 del Reglamento e-Privacy, es decir, la información emitida por los equipos terminales (como las señales wifi y similares) sin la protección de las normas DNT. Este hecho se mantiene incluso después de que el Parlamento reformulara el art. 8.2 para exigir el consentimiento informado en lugar de limitarse a dar un aviso claro y prominente para los casos en los que no sea necesario para establecer la conexión. A raíz de estos cambios y en consonancia con la protección concedida en virtud del art. 9, defendemos que esta disposición debería modificarse para incluir el art. 8.2 a fin de dotar de coherencia interna al Reglamento e-Privacy.[234]

Por último, el art. 9.3 del Reglamento e-Privacy establece que a los usuarios finales se les concederá el derecho a retirar su consentimiento. Además, el texto de la Comisión establecía que se recordase a los usuarios cada seis meses su derecho a retirar el consentimiento concedido para el tratamiento del contenido (art. 6.3.a y b) y los metadatos (art. 6.2.c.) de las comunicaciones electrónicas.

A este respecto, el informe LIBE aconsejó que se modificara la disposición para incluir la posibilidad de retirar el consentimiento para utilizar cookies y tecnologías de seguimiento similares, y que el recordatorio también se

[234] A este respecto, los autores del informe LIBE enviaron un comunicado a los diputados al Parlamento Europeo en el que destacaban la necesidad de modificar el art. 9.2 del Reglamento e-Privacy en el sentido en que se ha debatido para garantizar el mismo nivel de protección a la información emitida por los equipos terminales.

aplicara a la configuración del navegador. Por último, el informe también añadió la necesidad de prohibir las barreras de rastreadores. Esta protección integral se considera como una forma de proteger mejor a los consumidores contra la naturaleza intrusiva de la publicidad en línea basada en el comportamiento y las actuales actividades de elaboración de perfiles extendidas.

De hecho, el Parlamento siguió esta recomendación de ampliar el ámbito de aplicación del art. 9.3 y estableció que el derecho a retirar el consentimiento también abarcará el tratamiento de la información almacenada en los equipos terminales, como las cookies (art. 8.1.b) y el tratamiento de la información emitida por los equipos terminales (como wifi y bluetooth) (art. 8.2). El Parlamento también sugiere que se prohíban barreras de rastreadores, aunque esta disposición se incluyó en el art. 8 (como ya se ha visto anteriormente) y no en el art. 9. En cuanto a los recordatorios, el Parlamento eliminó esta obligación de los proveedores. Por último, añadió que el tratamiento basado en el consentimiento no debe ir en detrimento de los derechos y libertades de las personas cuyos datos personales estén relacionados con la comunicación o se transmitan en ella, en particular su derecho a la privacidad y a la protección de los datos personales.

El art. 10 del Reglamento e-Privacy trata la información y las opciones de configuración de la privacidad que deben proporcionarse. La propuesta de la Comisión estableció la obligación de los proveedores de software que permiten comunicaciones electrónicas de ofrecer "la posibilidad de impedir a terceros almacenar información sobre el equipo terminal de un usuario final o el tratamiento de información ya almacenada en ese equipo". Esta disposición está dirigida a los proveedores de software, como navegadores de internet o desarrolladores de aplicaciones. Esto implicaría cambios para los proveedores de navegadores, que deberían desarrollar estas opciones para requerir una acción afirmativa clara por parte del usuario final para establecer el acuerdo. Además, los proveedores de software deberían ofrecer la opción de impedir las cookies de terceros, informando al usuario

y solicitándole que realice una elección sobre la configuración de privacidad deseada antes de finalizar la instalación. De esta manera, los proveedores deberían dar a los usuarios varias opciones entre las que elegir para ajustar sus configuraciones con el fin de aceptar o rechazar ser rastreados por terceros. Esto se puede efectuar dando opciones como:[235]

- Aceptar siempre las cookies.
- No aceptar nunca cookies.
- Rechazar cookies de terceros.
- Aceptar solo cookies de origen.

Por consiguiente, si se adopta la propuesta de la Comisión, más usuarios serían conscientes de las técnicas de seguimiento existentes y de las diferentes opciones para protegerse contra el rastreo de su comportamiento. El problema de esta redacción, tal y como ha sido escrita por la Comisión, es que, en la actualidad, la mayoría de los navegadores actuales configuran por defecto los ajustes de cookies para que acepten todas las cookies. Esto significa que solo ofrecer opciones para cambiar la opción preestablecida de "aceptar todas las cookies" infringe los principios del RGPD de protección de datos desde el diseño y por defecto (véase art. 25 RGPD), ya que, si se siguieran estos principios, la opción preseleccionada debería ser la que ofrezca una mayor protección de la privacidad (es decir, "rechazar todas las cookies").

En vista de estas carencias en la redacción original de la Comisión, el Parlamento sugirió que esta disposición se modificara del siguiente modo. En primer lugar, los proveedores de software que permiten comunicaciones electrónicas deben preconfigurar sus sistemas para que tengan, por defecto, las opciones más protectoras. No se daría ninguna opción (ya que no se requeriría consentimiento) para la información que se recoja de los equipos terminales de los usuarios finales cuando sea estrictamente necesaria para llevar a cabo la transmisión o para prestar un

[235] Véase considerando 23 de Propuesta de Reglamento e-Privacy.

servicio de la sociedad de la información solicitado por el usuario final (por ejemplo, para adaptar el tamaño de la pantalla al dispositivo o para recordar artículos de una cesta de compra). En segundo lugar, el usuario dispondría de opciones detalladas entre las que elegir para consentir distintas categorías de finalidades. Estas opciones se presentarían en el momento de la instalación del software, pero también estarían disponibles tras la instalación. En tercer lugar, se establece que, aunque el usuario haya indicado sus preferencias en la configuración general, se le debería permitir hacer excepciones y dar su consentimiento específico (por ejemplo, permitir el almacenamiento de cookies de un sitio web específico, aunque sus preferencias estén establecidas de manera más protectora para otros sitios web). Por último, la información debe ser accesible fácilmente y permitir a los usuarios dar su consentimiento informado.[236]

Esencialmente, el marco de la e-Privacy se basa en el consentimiento para legitimar el uso de datos que de otro modo no sería necesario. Esto se deriva de las normas europeas tradicionales de protección de datos, basadas fuertemente en el consentimiento como medio para que los usuarios ejerzan su autonomía y muestren su autodeterminación.

Sin embargo, el consentimiento ha mostrado deficiencias en los entornos en línea. Pongamos como ejemplo la ya mencionada "fatiga de consentimiento". Algunos autores incluso han argumentado en contra de mantener el consentimiento como herramienta clave para proteger a los usuarios. En este sentido, uno piensa inmediatamente en Helen Nissebaum y en su declaración "dejen de pensar en el consentimiento: no es posible y no es correcto".[237] Lilian Edwards también ha compartido una opinión similar al declarar que "el consentimiento real puede ser, de hecho, el bien de lujo definitivo de la élite: bien educada, rica en tiempo y con

[236] Sin embargo, el texto del Consejo propone eliminar el art. 10 sobre la configuración de la privacidad, lo que causaría que un número significativamente menor de usuarios fuera consciente de la existencia de una configuración de privacidad más protectora.

[237] NISSEBAUM, Helen (2018): “Stop thinking about consent: it isn’t possible and it isn’t right”, en *Harvard Business Review*.

acceso a diversas opciones".[238] El consentimiento hace que el usuario sea responsable de entender que la información personal está siendo tratada por terceros. Del mismo modo, también proporciona un medio de prueba para el responsable del tratamiento de que la decisión tomada por los usuarios al dar su consentimiento es informada y libre.

Sin embargo, dejar a un lado el consentimiento como forma de reflejar las preferencias propias podría crear unas reglas del juego en las que los responsables del tratamiento traten los datos por defecto, con la seguridad de que pocos usuarios ejercerían sus derechos o proporcionando información insuficiente sobre prácticas oscuras. En las fases preliminares del proceso de redacción del Reglamento e-Privacy, el SEPD alegó explícitamente que el consentimiento como base para el tratamiento de datos proporciona un nivel de protección más elevado que otros fundamentos contemplados en el RGPD: "Al exigir el consentimiento para el tratamiento de datos de tráfico y de localización, la actual Directiva e-Privacy ofrece un nivel de protección más elevado que el del RGPD. El RGPD permite, al menos potencialmente, otros fundamentos jurídicos, como el interés legítimo o la ejecución de un contrato. (...) Para proteger mejor la confidencialidad de las comunicaciones electrónicas, el SEPD recomienda que la Directiva e-Privacy mantenga y refuerce el actual requisito de consentimiento (...)".[239]

En declaraciones más recientes, el SEPD volvió a insistir en esta postura y mostró su preocupación por el hecho de que el acuerdo entre los colegisladores pudiera acabar permitiendo "un tratamiento secundario de metadatos para finalidades compatibles". En sus palabras, esto significaría que los metadatos podrían utilizarse para cualquier finalidad que el proveedor de servicios considere que cumpla la cláusula de

[238] EDWARDS, Lilian (2018): “Data Protection and ePrivacy: From Spam and Cookies to Big Data, Machine Learning and Profiling”, en Lilian Edwards (ed.), *Law, Policy and the Internet*, Hart.

[239] SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS (2016): *Opinion 5/2016, Preliminary EDPS Opinion on the review of the ePrivacy Directive (2002/58/EC)*, de 22 de julio, p. 17.

compatibilidad. Por consiguiente, esto crearía una situación muy cercana a la introducción del interés legítimo como base jurídica para el tratamiento de metadatos, que se ha evitado continuamente desde los comienzos de las normas de e-Privacy. Sin embargo, el SEPD declaró expresamente que el alcance de las negociaciones en este sentido es limitado. Por lo tanto, al final parece que, al menos por el momento, el consentimiento puede determinarse como la única base para permitir los tratamientos de datos de comunicaciones electrónicas que no sean necesarios.

Sea como fuere, al final parece que, al menos por el momento, se puede determinar el consentimiento como base para permitir los usos de datos de comunicaciones electrónicas que no sean necesarios. El CEPD ya mostró que no se habían olvidado en absoluto otras opciones, sino que simplemente no se consideraban viables, al afirmar que "[e]l consentimiento del usuario debía obtenerse antes de tratar los datos de las comunicaciones electrónicas (…). No debería haber ninguna excepción para tratar estos datos basándose en el "interés legítimo" del responsable del tratamiento o en la finalidad general de la ejecución de un contrato".[240] Estas tensiones entre los argumentos a favor y en contra del consentimiento dieron lugar al principio de protección de datos por defecto, previsto en el art. 25 RGPD y reflejado en el art. 10.

8. Impacto de la propuesta de Reglamento e-Privacy en los modelos de negocio de vigilancia

Los modelos de negocio de vigilancia han surgido y han crecido rápidamente en los últimos años. Se basan en el análisis de enormes cantidades de datos, a los que ahora se tiende a denominar como el nuevo petróleo o la nueva moneda. Se pueden considerar ejemplos de ello los productos basados en el reconocimiento facial, la inteligencia artificial o la industria de los drones. En estos modelos de negocio, los usuarios

[240] COMITÉ EUROPEO DE PROTECCIÓN DE DATOS (2018): *Statement on the revision of the ePrivacy Regulation and its impact on the protection of individuals with regard to the privacy and confidentiality of their communications*, p. 3.

intercambian estos datos por bienes y servicios, y los proveedores monetizan dichos datos.

Bruce Schneider ha llegado incluso a afirmar que "la vigilancia es el modelo de negocio de internet",[241] y Shoshana Zuboff ha definido el concepto de capitalismo[242] de la vigilancia como basado en la mercantilización de la realidad y su transformación en datos de comportamiento para el análisis y las ventas. Según Zuboff, el capitalismo de la vigilancia preserva modelos de negocio que se basan en la recolección y el análisis de grandes cantidades de datos, la automatización de contratos, la personalización de servicios y el uso de la tecnología para realizar experimentos con usuarios y consumidores y sus impulsores. Estas actividades tienen un claro impacto en la privacidad.

Las principales características del contexto actual del modelo de negocio basado en la vigilancia se podrían sintetizar de la siguiente manera:

En primer lugar, este modelo de negocio se basa en la recopilación de datos, y se ha beneficiado de una supuesta complejidad impulsada por las numerosas y rápidas operaciones automatizadas que hacen que sea casi imposible que sean totalmente comprendidas por personas ajenas. El funcionamiento real de la industria del corretaje de datos es tan secreto que se podría llegar a pensar que se le ha concedido el estatus de secreto comercial.

En segundo lugar, los modelos de negocio de vigilancia se basan en el análisis de metadatos. Los metadatos se pueden generar en grandes cantidades, casi en tiempo real y de forma relativamente estructurada, lo que favorece la agregación. Por ejemplo, los metadatos pueden ser generados por aplicaciones instaladas en un smartphone, sensores portátiles, etc.

---

[241] SCHNEIDER, Bruce (2017): entrevista en Open Democracy. Disponible en: https://www.opendemocracy.net/en/digitaliberties/surveillance-is-business-model-of-internet/

[242] ZUBOFF, Shoshana (2018): *The Age of Surveillance Capitalism. The Fight for a Human Future at the New Frontier of Power*, Londres, Profile Books.

En tercer lugar, este contexto se caracteriza actualmente por la concentración de los agentes del mercado. Por ejemplo, la industria de la inteligencia artificial está dominada por unos pocos agentes importantes, incluyendo los habituales: Facebook, Amazon, IBM, Siemens, Google, Apple o Microsoft. Estas empresas refuerzan su ya significativo poder de mercado mediante la fusión y adquisición de competidores más pequeños, lo que ya ha suscitado preocupación entre las autoridades de protección de datos. Esto es aún más apremiante desde que el acceso a internet se ha convertido una necesidad en la sociedad actual que los ciudadanos consideran incluso como un derecho humano fundamental.

En cuarto lugar, muchos de los proveedores y servicios que crean y recogen la mayor parte de los datos son hoy en día proveedores OTT, que, como se ha explicado, no se rigen por las mismas normas que los operadores tradicionales y se han beneficiado de los vacíos legales de la Directiva actual en el sentido de que no están obligados a recabar el consentimiento para tratar metadatos de comunicaciones electrónicas. En esta situación, si un usuario envía un SMS, la empresa de telecomunicaciones solo puede utilizar su ubicación para servicios de marketing o de valor añadido con el consentimiento del usuario. Sin embargo, cuando esa misma persona decide enviar un mensaje a través de WhatsApp, la recopilación de datos de ubicación se puede realizar sin consentimiento. De este modo, la empresa OTT puede analizar los datos para luego ofrecer publicidad, por ejemplo, de lugares de comida cercanos, o para crear perfiles que pueden incluir datos sensibles deducidos, como hábitos de salud o prácticas religiosas. Esta información es muy rentable y explica por qué los proveedores de OTT han presionado para retrasar las negociaciones sobre el marco de e-Privacy. Estos datos se utilizaban principalmente para servicios relacionados con la publicidad, una industria relativamente inocua. Sin embargo, esto era solo la punta del iceberg, y ahora se están desarrollando servicios mucho más intrusivos, como el reconocimiento facial, sustentados con datos que sirven para entrenar algoritmos. Se trata de usos secundarios de los datos que no fueron

previstos, comprendidos o acordados por los usuarios cuando se recogieron los datos. Algunos de estos usos pueden incluso haber sido establecidos en políticas de privacidad que no han sido leídas y haber sido consentidos por los usuarios sin darse cuenta.

En este sentido, un reciente estudio publicado por la Autoridad Española de Protección de Datos[243] sobre los flujos de información en sistemas Android ha concluido que existe un alto riesgo de comunicación de datos a terceros sin el conocimiento de los usuarios. El estudio revela el alto número de identificadores únicos de dispositivos que revelan información fácilmente enlazable con el usuario de dicho dispositivo. El estudio también concluyó que muchas de las aplicaciones preinstaladas disfrutan de permisos privilegiados para recopilar datos, sin conceder a los usuarios la opción de desinstalarlas, y que las opciones de privacidad presentadas a los usuarios en la configuración inicial del dispositivo no se corresponden con los permisos reales que se conceden a los proveedores.

Aún más preocupantes son las conclusiones sobre el estudio del software preinstalado en dispositivos Android[244]. El estudio muestra que existen muchas relaciones complejas de intercambio de datos privados entre varias partes interesadas que deciden qué software se preinstalarán en los dispositivos. Muchos de ellos contienen puertas traseras que permiten la monitorización del comportamiento de los usuarios sin que sean conscientes de ello. Y esto es solo la parte superficial de un problema mucho más profundo.

Teniendo en cuenta lo anteriormente expuesto, y con el objetivo de minimizar las actividades basadas en la vigilancia, la Directiva e-Privacy introduce varias disposiciones mencionadas previamente en la presente. Lo más importante a este respecto es la inclusión de los proveedores OTT

[243] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (2019): *Análisis de los flujos de información en Android. Herramientas para el cumplimiento de la responsabilidad proactiva*.

[244] GAMBA, Julián; et al (2019): “An Analysis of pre-installed android software”, en *41th Symposium on Security and Privacy*, IEEE San Fransisco.

en el ámbito de aplicación del Reglamento, la protección de los equipos terminales o las normas explícitas sobre metadatos (es decir, la disposición según la cual solo pueden utilizarse con el consentimiento del usuario para finalidades que no sean necesarias, junto con el requisito de suprimirlos o hacerlos anónimos cuando ya no se necesiten para la finalidad declarada). Muchas de las medidas previstas en la propuesta presentada por la Comisión fueron reforzadas posteriormente por el Parlamento. Por ejemplo, el Parlamento endureció las disposiciones del borrador original para limitar el uso del consentimiento para tratar metadatos, prohibió explícitamente las barreras de rastreadores y reforzó algunas disposiciones de acuerdo con el principio de protección de datos por defecto. Este conjunto de medidas tiene el potencial para imponer limitaciones efectivas a la vigilancia masiva e incontrolada de los usuarios y limitar hasta cierto punto las prácticas comerciales relacionadas.

Sin embargo, estas disposiciones chocan con los modelos de negocio basados en la vigilancia masiva, que están ejerciendo una gran presión para influir en el texto final del Consejo. Uno de los principales desafíos de las negociaciones es la cuestión de hasta qué punto los proveedores pueden seguir tratando metadatos para finalidades compatibles distintas de la original. Varias voces autorizadas se han opuesto firmemente a esta postura, lo que significaría, esencialmente, abrir la puerta a prácticas que de hecho están cerca de permitir el interés legítimo como base legal para el tratamiento de metadatos. Desde el origen de las normas sobre comunicaciones electrónicas en Europa, el consentimiento se ha considerado la base preferente para el tratamiento. Se podría argumentar que estos datos se consideran más sensibles que los datos de otra naturaleza, por lo que se limitan los fundamentos legales en virtud de los cuales pueden ser tratados. De hecho, Brigit Sippel (diputada alemana al Parlamento Europeo) ha declarado públicamente que "para mí, los datos

de las comunicaciones son datos sensibles, y no solo el contenido, sino también los metadatos"[245].

Teniendo esto en cuenta, el acuerdo final para el texto de Reglamento será fundamental para determinar cómo pueden beneficiarse los modelos de negocio de la mercantilización de los datos. Se espera que persistan las tensiones, lo que podrá dificultar que se alcance un acuerdo. Muchos agentes del mercado se benefician de este retraso, ya que, como se ha mencionado anteriormente, muchas de sus actividades están actualmente fuera del ámbito de aplicación de la Directiva e-Privacy. En este sentido, los incentivos para atender las peticiones del SEPD[246] y del CEPD[247] y alcanzar un acuerdo rápido son escasos.

En cualquier caso, el marco normativo del Reglamento e-Privacy no tiene capacidad para abordar plenamente las consecuencias negativas de la nueva economía basada en la vigilancia de las personas. La educación de la sociedad civil es crucial, ya que los usuarios muestran comportamientos contradictorios. Por un lado, expresan su creciente preocupación por el tratamiento de los datos en el entorno digital. En cambio, por otro lado, los usuarios no actúan en consecuencia y entregan sus datos a cambio de servicios gratuitos, algunos de los cuales pueden tener un valor elevado mientras que otros tienen un valor mínimo. La causa puede ser la falta de comprensión de todo el potencial de abusos de los datos y el valor de los mismos. Además, la industria del corretaje de datos no llega a entenderse totalmente, ni siquiera por los reguladores. Por lo tanto, el primer paso puede ser aumentar la transparencia, por ejemplo en forma de registros de los corredores de datos

[245] BRACY, Jedidiah (2017): "Sippel: ePrivacy reg should 'abolish surveillance-driven advertising'", en *Blog de IAPP*.

[246] BUTTARELLI, Giovanni (2018): "The urgent case for a new ePrivacy law", en *Blog del Supervisor Europeo de Protección de Datos*.

[247] COMITÉ EUROPEO DE PROTECCIÓN DE DATOS (2019): *Declaración 3/2019 sobre el reglamento de privacidad y las comunicaciones electrónicas*, de 13 de marzo.

8.1. Conclusión

En lo que se refiere al consentimiento, la propuesta de Reglamento e-Privacy adopta un enfoque más favorable hacia el usuario que aquel de la Directiva. De hecho, el consentimiento se considera la principal herramienta legislativa para dar a las personas el control sobre la forma en la que se utilizan sus datos. El art. 9 del Reglamento e-Privacy permite el uso de las normas DNT. Se trata de mecanismos diseñados para permitir a los usuarios expresar sus opciones de una sola vez, en lugar de requerir un consentimiento diferente cada vez que entran en un servicio. La centralización del consentimiento, junto con la ampliación de la excepción para el consentimiento de las cookies (es decir, no exigir el consentimiento para las cookies necesarias o inocuas), reduciría significativamente la cantidad de notificaciones a las que se enfrentan los usuarios, evitando así la actual fatiga de consentimiento. Sin embargo, todavía no está claro si el cumplimiento de las normas DNT será obligatorio u opcional.

El art. 10 del Reglamento e-Privacy trata las opciones de configuración de privacidad que se presentarán a los usuarios, así como de la información relacionada. Mientras que el borrador de la Comisión únicamente obliga a los proveedores a presentar a los usuarios varias opciones, el borrador del Parlamento además se atiene al principio de protección de datos desde el diseño y por defecto y establece que la opción más protectora deba estar preseleccionada hasta que el usuario la cambie.

Esencialmente, el marco de la e-Privacy se basa en el consentimiento para legitimar el uso de datos que de otro modo no sería necesario. Esto se deriva de las normas europeas tradicionales de protección de datos, basadas fuertemente en el consentimiento como medio para que los usuarios ejerzan su autonomía y muestren su autodeterminación. Esto significa que las normas e-Privacy son más restrictivas que las del RGPD, que permitiría otras bases legales como el interés legítimo. En este sentido, el SEPD también ha solicitado explícitamente que se abandonen las disposiciones que puedan crear una situación que "de facto" pueda ser muy

parecida a la del interés legítimo, como el "tratamiento secundario de metadatos para finalidades compatibles"

La evolución del texto de la versión de la Comisión a la del Parlamento ha puesto de manifiesto un endurecimiento de las obligaciones de los proveedores de proteger los derechos de los usuarios. Aunque todavía no se conoce la redacción final y pueden producirse cambios significativos, consideramos importante que el Reglamento e-Privacy mantenga su actual vocación de sostenibilidad y neutralidad tecnológica, de modo que los avances que se produzcan los próximos años no socaven la protección concedida a los usuarios.

El Parlamento Europeo celebró elecciones del 23 al 26 de mayo de 2019 y designó una nueva Comisión Europea que comenzó su mandato el 1 de noviembre de 2019. Por lo tanto, es probable que la adopción del Reglamento no tenga lugar antes de 2020.

Además, según las versiones actuales del Reglamento, este sería de aplicación dos años después de su entrada en vigor, por lo que parece que la UE tendrá que aprender a convivir por el momento con dos cuerpos normativos complementarios, pero no coherentes entre sí: el RGPD y la desactualizada Directiva e-Privacy.

9. Conclusiones

9.1. Base utilizada por defecto

La práctica indica que el consentimiento era la base de legitimación utilizada por defecto antes de la entrada en aplicación del RGPD. Todo ello ayudado por la popularidad del consentimiento como instrumento ligado a la gran virtud de posibilitar el control de los interesados sobre sus datos personales,[248] así como la facilidad del responsable para legitimar el

[248] A título de ejemplo, María Loza afirma que “es claro que el consentimiento es el instrumento que permite al interesado ejercer el control sobre sus datos personales, el cual constituye precisamente el contenido básico del derecho a la protección de datos”. LOZA CORERA, María (2017): “De los microdatos a los datos masivos. Cuestiones legales”, en *Universitat de València*, p. 113-114.

tratamiento, especialmente cuando el consentimiento era obtenido de modo tácito.

Esta propensión cristalizó en la costumbre de no prestar el mismo grado de atención a otras bases de legitimación, tales como el interés legítimo del art. 6.1.f) RGPD o la ejecución de un contrato del art. 6.1.b). Como consecuencia de ello, también se generó un mayor grado de desconocimiento por las técnicas jurídicas o las posibilidades de estas otras bases de legitimación.

Sin embargo, por otro lado, el uso tan extendido del consentimiento por defecto terminó por potenciar algunas limitaciones de esta base jurídica, que en ocasiones se llegaba a utilizar a pesar de no ser más apropiada[249] o de resultar incluso inválida.

9.2. Las grandes suposiciones del consentimiento

El consentimiento presupone que el individuo ha procesado la información que se le presenta, ha comprendido dicha información y sus posibles consecuencias futuras, se ha formado una decisión autónoma y actúa en coherencia al autorizar una actividad de tratamiento de datos personales. Todo ello, además, numerosas veces por día durante el curso de actividades cotidianas cuyo objetivo principal no está relacionado directamente con el proceso mental de decidir sobre el futuro de los datos personales.

9.3. Los problemas del consentimiento

En este capítulo hemos analizado diversas limitaciones del consentimiento, que en esencia muestran que, en determinadas circunstancias, los usuarios no toman decisiones racionales, informadas y conscientes, sino que únicamente parecen aceptar cuando se les presenta una petición de

[249] Un ejemplo típico de uso del consentimiento de manera incorrecta se ha visto de manera extendida en el entorno laboral, con motivo del tratamiento de datos por parte de una asesoría externa, encargada del tratamiento, para la gestión de las nóminas de los empleados.

consentimiento. De este modo, aunque se preste un consentimiento jurídicamente válido conforme al estándar del interesado medio razonable, su utilidad ha sido opacada y no cumple el estándar subjetivo.[250] En ocasiones, estas deficiencias se manifiestan también desde la perspectiva del responsable, alejando el estándar del responsable del idealmente deseado.

En relación con todo ello, cabe rescatar la afirmación del GT29 (ahora CEPD) por la que manifestaba que "si se utiliza correctamente, el consentimiento es una herramienta que otorga al sujeto un control sobre el tratamiento de sus datos. Si se utiliza de manera incorrecta, el control del sujeto se convierte en ilusorio y entonces el consentimiento constituye una base inapropiada para el tratamiento de los datos".[251]

9.4. Se agudiza en entornos big data

Todo ello se agudiza en entornos técnicamente avanzados en los que concurren diversas características, desde la recolección de grandes cantidades de datos de manera intensiva y en ocasiones desapercibida, el análisis de cantidades masivas de datos para la extracción de nuevo conocimiento, la creación de modelos algorítmicos, la aplicación de dichos modelos al individuo para obtener nuevo conocimiento sobre sus patrones de comportamiento y, finalmente, la realización de acciones con base en dicho nuevo conocimiento. Estos entornos son rápidamente cambiantes y lo suficientemente complejos como para que el interesado medio no sea capaz de mantener un nivel de conocimiento actualizado sobre los potenciales beneficios y riesgos de dichos tratamientos de datos. De este modo, es tanto más complicado poder asumir el rol de decidir de manera convenientemente informada y con consciencia.

---

[250] SCHERMER, Bart W.; CUSTERS, Bart; VAN DER HOF, Simone (2014): “The Crisis of Consent: How Stronger Legal Protection May Lead to Weaker Consent in Data Protection”, en *Ethics and Information Technology*, Vol. 16, No. 2.

[251] GRUPO DE TRABAJO DEL ARTÍCULO 29 (2014): *Dictamen 06/2014 sobre el concepto de interés legítimo del responsable del tratamiento de los datos en virtud del artículo 7 de la Directiva 95/46/CE* (WP 217), de 9 de abril.

Así, incluso cuando el consentimiento cumple con los requisitos formales que la norma exige, en la práctica se ha convertido en un acto irreflexivo y automático,[252] en el que los interesados prestar su autorización cada vez que se enfrentan a una solicitud de consentimiento.[253]

9.5. ¿Continúa siendo la base preferida del legislador?

A pesar de la evidencia de las limitaciones del consentimiento que aquí han sido analizadas, principalmente agudas en entornos de alta complejidad, parece que el legislador comunitario mantiene una fuerte preferencia por el uso de esta base de legitimación. Así lo demuestra el hecho de que, bajo el RGPD, el consentimiento pueda legitimar la toma de decisiones automatizadas,[254] la realización de transferencias internacionales de datos, o que el consentimiento expreso habilite el tratamiento de categorías especiales de datos.[255] Igualmente, ello se aprecia en el hecho de que el consentimiento sea requisito para el ejercicio de derechos como la portabilidad de los datos. Del mismo modo, otros cuerpos normativos también son muestra de ello. La Directiva e-Privacy, e incluso con mayor contundencia los borradores de futuro Reglamento e-Privacy, aquí analizados, otorgan al consentimiento un rol principal.

9.6. Alternativas

Es cierto que el RGPD ha endurecido las condiciones del consentimiento, así como los deberes de información, hecho que ha dado lugar a que algunas voces argumenten que el Reglamento se basa, de hecho, en el

[252] CONTRERAS VÁSQUEZ, Pablo; TRIGO KRAMCSÁK, Pablo (2019): "Interés legítimo y tratamiento de datos personales: Antecedentes comparados y regulación en Chile", en *Revista chilena de derecho y tecnología*, Vol. 8, No. 1.

[253] SCHERMER, Bart W.; CUSTERS, Bart; VAN DER HOF, Simone (2014): "The Crisis of Consent: How Stronger Legal Protection May Lead to Weaker Consent in Data Protection", en *Ethics and Information Technology*, Vol. 16, No. 2.

[254] Además del consentimiento, el art. 22 también permite la toma de decisiones automatizadas sobre la base de la necesidad para la ejecución de un contrato o por habilitación legal en el Derecho de la Unión o de los Estados miembros.

[255] Además del consentimiento, el art. 9 prevé circunstancias en las que dicho tratamiento será lícito, tales como el interés público esencial. Sin embargo, el interés legítimo no se encuentra entre estas.

modelo de información y consentimiento como pieza clave.[256] Sin embargo, la solución a los problemas que el consentimiento ha mostrado tener en los últimos años no debe verse únicamente un mayor o más estricto uso de las condiciones del consentimiento.

Algunas soluciones propuestas son mantener el modelo de consentimiento tácito bajo la premisa de que se solicite para transacciones justas o que atiendan al principio de lealtad.[257] Otros autores se pronuncian a favor de reservar el consentimiento sólo para los usos de los datos que se derivan de lo que es razonable esperar,[258] de modo que las personas presten más atención cada vez que se les pida el consentimiento.

Por otro lado, voces como Adsuara Valera se mantienen firmes defensoras del consentimiento y de la capacidad de autodeterminación de la persona, pero defiende la idea de comenzar a acuñar el concepto de "libertad de datos", en el que toma más importancia el rol proactivo de la persona que el matiz reactivo que en ocasiones tiene (en el sentido de que el interesado tiene una posición pasiva o reactiva respecto de las acciones del responsable).[259]

En todo caso, el consentimiento es, y ha sido siempre de hecho, una alternativa más de entre las bases de legitimación, aunque este hecho no se haya trasladado a la práctica con claridad. Así se refleja incluso en la redacción del art. 8 de la Carta de Derechos Fundamentales de la Unión Europea, quizás la norma de mayor relevancia para la consideración de la

---

[256] Ver, por ejemplo, MC CABE, David (2019): "The sun may be setting on the old privacy rulebook", en *Axios*.

[257] SCHERMER, Bart W.; CUSTERS, Bart; VAN DER HOF, Simone (2014): "The Crisis of Consent: How Stronger Legal Protection May Lead to Weaker Consent in Data Protection", en *Ethics and Information Technology*, Vol. 16, No. 2.

[258] BAROCCAS, Solon; NISSEBAUM, Helen (2014): "Big data´s End Run Around Anonymity And Consent", en *Privacy, big data and the public good. Frameworks for engagement*, Cambridge University Press, p.44-75; FORO ECONÓMICO MUNDIAL, THE BOSTON CONSULTING GROUP (2012): "Rethinking Personal Data: Strengthening Trust", *Proyecto Rethinking Personal Data*.

[259] ADSUARA VALERA, Borja (2016): "El consentimiento", en José Luís Piñar Mañas (dir.), *Reglamento general de protección de datos. Hacia un nuevo modelo europeo de privacidad*, Madrid, Reus, p.151-170.

protección de datos como derecho fundamental en los Estados miembros. Este artículo indica, en su apartado segundo, que los datos personales serán tratados "sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley".[260]

No obstante, el espíritu subyacente del RGPD y de sus principales cambios contradice esta afirmación. De hecho, cada vez son más también las opiniones que invitan a reconsiderar la validez del consentimiento en el caso concreto, así como abrirse a otras opciones como la aplicación del interés legítimo. En este sentido, el entonces Supervisor Europeo de Protección de Datos, Giovanni Buttarelli, manifestaba en la primavera de 2019 que para volver a obtener la confianza de los individuos en los servicios de la sociedad digital, un primer paso es la reconsideración de lo que significa el consentimiento. Así, si la autorización para uso de los datos que lleva a cabo el responsable no puede ser retirado, entonces el consentimiento no es la base jurídica adecuada. Y añadía, si el responsable está seguro de que ha desplegado las medidas de mitigación de riesgos adecuadas, y que ha tomado en consideración los intereses del interesado, entonces, una mejor base de legitimación sería el art. 6.1.f) RGPD que consagra el interés legítimo del responsable.[261] Estas declaraciones resultan cuanto menos llamativas en voz del SEPD, por cuanto la postura tradicional del órgano se había basado en una defensa férrea del consentimiento y, en concreto, en contra del interés legítimo. A título de ejemplo, sirvan las declaraciones del Director del mismo organismo, Leonardo Cervera Navas, quien en 2018 afirmaba que, tras una revisión documental por parte del SEPD del interés legítimo, la postura adoptada por el organismo era la preferencia por el consentimiento, que consideraba "la base de legitimación más protectora" para los derechos de los individuos, y recomendar su aplicación en caso de la existencia de dudas

[260] Carta de los Derechos Fundamentales de la Unión Europea, de 18 de diciembre de 2000 (2000/C 364/01).

[261] BUTTARELLI, Giovanni (2019): "Deception by design?", en *Speech to ISMS Forum Spain: XXI International Information Security Conference*, Madrid.

sobre qué base de legitimación aplicar a un tratamiento de datos, en concreto, por la posibilidad de retirarlo así como la garantía del derecho de portabilidad.[262] Ciertamente, como ya ha sido comentado, el uso del consentimiento -y, cabe añadir, el contrato- como base de legitimación conlleva la posibilidad del interesado de poder ejercer derechos de protección de datos como el de portabilidad, que no son ejercitables si el tratamiento se legitima en otras bases.

9.7. La importancia del consentimiento se reduce

A pesar de los argumentos en defensa de las bondades del consentimiento, numerosas voces de innegable prestigio han cargado contra él. Eleni Kosta indica que "el papel del consentimiento en esta era se reduce, pues el control del individuo sobre su información personal se supera mediante la agilización de las actividades cotidianas en las comunicaciones electrónicas y especialmente en internet, en la medida en que no se infrinja la privacidad del individuo".[263] Sobre esta aseveración, Gabriela Zanfir, añade que, si ciertamente aceptamos que el rol del consentimiento se reduce, los individuos necesitan ser vestidos de otro tipo de garantías alternativas que garanticen la protección de sus datos personales.[264] Por su parte, Susan Morrow afirma que "el consentimiento, es su forma más pura, podría convertirse fácilmente en una vara distópica con la que controlar a los ciudadanos".[265]

---

[262] DIRECTOR DEL SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS (2018): "Data processing beneficial to individuals: the use of legitimate interest", en *Computers, Privacy and Data Protection Conference*, Bruselas.

[263] KOSTA, Eleni (2013): *Consent in European Data Protection Law*, Martinus Nijhoff Publishers, p. 318.

[264] En concreto, la propuesta de Gabriela Zanfir se basa en otorgar importancia a un modelo de "garantías adecuadas" no basado únicamente en la base de legitimación del tratamiento de manera que los interesados obtengan un sistema de protección eficaz frente a las limitaciones que presenta el consentimiento. ZANFIR, Gabriela (2014): "Forgetting about consent. Why the focus should be on "suitable safeguards" in data protection law", en *Reloading Data Protection*, Dordrecht, Springer, pp. 237-257.

[265] MORROW, Susan (2019): "*50 shades of privacy:* Consent and the fallacy that will prevent privacy for all", en *Information Age*.

En términos similares se expresaba Lillian Edwards, quien proponía más recientemente dejar el foco de atención actual, centrado en el consentimiento para la recogida de los datos (esto es, an la Fase 1-Recogida), para focalizarlo en su lugar en consentir a usos concretos de big data (es decir, en lo que parece referirse a lo que aquí ha sido descrito como Fase 2-Análisis y especialmente la Fase 3-Aplicación), o incluso "eliminar por completo el consentimiento como concepto central".[266]

9.8. Cambiar el foco de atención

El consentimiento emplaza el foco de atención y la responsabilidad en el interesado, quien debe manifestar haber leído, comprendido y aceptado determinadas condiciones de uso de sus datos. Sin embargo, en entornos cada vez más complejos, ubicuos, impredecibles y cambiantes, este sistema no garantiza sus derechos. En consecuencia, los derechos de los individuos, y en concreto su derecho a la protección de datos personales, podrían estar mejor garantizados mediante alternativas que pongan el foco de atención en el responsable del tratamiento.

A la luz de todo esto, ¿dejará el consentimiento de ser utilizado como la base de legitimación por defecto, y pasará a ser una más o incluso una opción residual? En las próximas páginas analizaremos el art. 6.1.f), que consagra el interés legítimo del responsable o un tercero como base de legitimación del tratamiento.

[266] EDWARDS, Lilian (2018): "Data Protection and ePrivacy: From Spam and Cookies to Big Data, Machine Learning and Profiling", en Lilian Edwards (ed.), *Law, Policy and the Internet*, Hart.

CAPÍTULO V. INTERÉS ¿(I)LEGÍTIMO?

> "En resumen, el sentido común no es una fuente de derecho. Pero ciertamente debería guiar su interpretación. Sería muy desafortunado que la protección de los datos personales se desintegrara en obstrucción por datos personales".[267]

1. Introducción

El "interés legítimo" es quizás uno de los conceptos más confusos del marco de protección de datos, apreciado, odiado e incomprendido a partes iguales.

En vista de las limitaciones analizadas en relación con el consentimiento, el interés legítimo ha comenzado a ser visto, en determinadas esferas, como el nuevo santo grial del tratamiento de datos personales bajo el RGPD. Parte del motivo del creciente interés en esta base jurídica es la (falsa) concepción de que se trata de un cajón de sastre en el que legitimar prácticas y actividades de tratamiento de datos personales de dudosa licitud y que no tendrían cabida en otra base. Esta concepción entraña el riesgo de usar hasta abusar esta base de legitimación, de la misma manera que ha sucedido con el mal uso dado al consentimiento.

Por ello, en este capítulo trataremos de arrojar algo de luz sobre esta noción.

En esencia, a salvo de algunas aclaraciones, el Reglamento ha mantenido el catálogo de bases jurídicas esencialmente inalteradas respecto de la normativa anterior. No obstante, el modo en que estas disposiciones sean

[267] Conclusiones del Abogado General, Caso Rīgas, párrafo 99. Traducción propia. Original: "*In sum, common sense is not a source of law. But it certainly ought to guide interpretation of it. It would be most unfortunate if protection of personal data were to disintegrate into obstruction by personal data*".

utilizadas sí puede verse alterado en entornos big data para adaptarse a la forma en la que se realizan los procesos analíticos en la práctica.

En lo que aquí respecta, el interés legítimo es una base de licitud del tratamiento de datos personales bajo determinadas circunstancias. El artículo 6.1.f) de RGPD[268] establece la licitud del tratamiento cuando dicho tratamiento "es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño". Asimismo, añade que esta base no es aplicable a los tratamientos efectuados por las autoridades públicas en el ejercicio de sus funciones.

El interés legítimo no es un concepto nuevo introducido por el RGPD, sino que ya estaba incluido en el artículo 7 de la derogada Directiva 95/46. La redacción actual no ha cambiado sustancialmente, lo que significa que la (existente, aunque no abundante) experiencia adquirida durante el período de vigencia de la Directiva, junto con la jurisprudencia del TJUE, es de utilidad en el marco del RGPD.

Asimismo, el carácter continuista del precepto también implica que el RGPD continúa utilizando términos ambiguos que ya aparecían en la Directiva que pueden crear incertidumbre y requerir interpretación. A pesar de ello, la redacción del art. 6.1.f) RGPD incluye algunas aclaraciones novedosas. En primer lugar, la apelación explícita a una protección más estricta cuando el interesado es un niño y, en segundo lugar, la exclusión de esta base para las autoridades públicas para aquellos tratamientos que

[268] El término "interés legítimo" también aparece en el RGPD con finalidades diferentes. En primer lugar, como una de las bases de licitud de los tratamientos de datos personales art. 6.1.f)-, sobre la que se basan otras disposiciones -art. 13.1.d), art. 14.2.b), art. 35.7.a), art. 40.2.b), art. 49.1.g) y considerandos 47-50, 69 y 113-. En segundo lugar, en referencia a la existencia de intereses de diferentes agentes que pueden ser merecedores de protección, ya sean estos de autoridades policiales (considerando 88), los interesados -art. 14.5.b) y c), art. 22.2.b), art. 22.3 y 4, art. 35.7.d), art. 88- o terceros art. 49.1.g), art. 49.2 y considerando 111. Este capítulo se centra en el interés legítimo como base de licitud del tratamiento a la luz del art. 6 RGPD.

se correspondan con el ejercicio de sus funciones. De hecho, uno de los primeros “mitos” en surgir a raíz de esta previsión es que esta disposición impide a las autoridades públicas utilizar sus intereses legítimos como base en cualquier circunstancia. Sin embargo, las autoridades públicas sí pueden seguir utilizando el interés legítimo como base para actividades distintas de sus tareas oficiales.

En esencia, a salvo de algunas aclaraciones, el Reglamento ha mantenido el catálogo de bases jurídicas esencialmente inalteradas respecto de la normativa anterior. No obstante, el modo en que estas disposiciones sean utilizadas sí puede verse alterado en entornos big data para adaptarse a la forma en la que se realizan los procesos analíticos en la práctica. En concreto, el interés legítimo como base de licitud posee determinadas características que justifican su estudio.

1.1. ¿Es un cajón de sastre?

Una de las principales críticas al interés legítimo deviene de considerar que se trata de un cajón de sastre, que confiere la facultad de realizar un tratamiento de datos personales que no sería lícito en otra circunstancia. Ello es debido a que la redacción del precepto es más flexible que aquella de otros párrafos del art. 6 RGPD (y el correspondiente art. 7 de la Directiva 95/46).

Uno de los motivos sobre los que se sostiene esta crítica es el hecho de que el consentimiento aporta la garantía de que el responsable no pueda iniciar el tratamiento salvo que haya obtenido una manifestación de aprobación del interesado. Por contra, si la base jurídica es el interés legítimo, el responsable puede proceder al tratamiento, en la medida en que se cumplan una serie de requisitos, y siempre que el usuario no se haya opuesto.

En línea con ello, ciertamente parece que, en ocasiones, determinados responsables manifiestan que, mientras recabar el consentimiento de los usuarios conforme a los estrictos requisitos del RGPD constituye un

desafío, basar el mismo tratamiento sobre el interés legítimo será una vía más sencilla. Así por ejemplo, en su informe anual de 2017, la autoridad irlandesa de protección de datos manifestaba haber observado una cierta tendencia de los responsables a utilizar el interés legítimo como base de licitud del tratamiento "como una especie de comodín para cubrir una situación en la que los datos personales se han tratado de forma reactiva y sin que se haya considerado de antemano si es legítimo o no llevar a cabo el tratamiento". Desde luego, se trata de un uso fraudulento de la disposición que no legitima el tratamiento que fue declarado contrario a la norma por la autoridad.[269]

Por su parte, el GT 29, en su Dictamen sobre el concepto de interés legítimo ha defendido la utilidad de esta base jurídica, de la que ha señalado que presenta garantías complementarias en relación con otras bases, de modo que no debe considerarse "el vínculo más débil o una puerta abierta para legitimar todas las actividades de tratamiento de datos que no estén comprendidas en cualquiera de los demás motivos de legitimación".[270]

De hecho, del análisis realizado en el capítulo anterior sobre las limitaciones del consentimiento y del que sea realizará en este capítulo sobre el interés legítimo, podría llegar a afirmarse que, en muchas ocasiones, el consentimiento o la justificación por la necesidad de ejecutar un contrato, se utilizan para legitimar tratamientos que no salvarían los requisitos del interés legítimo. Al contrario que ocurre con el interés legítimo, el consentimiento y la ejecución de un contrato no requieren la realización de un ejercicio de ponderación de intereses, la implementación de garantías que minimicen el impacto sobre los individuos o, en esencia, un planteamiento previo del responsable sobre qué efectos puede tener el tratamiento de datos personales más allá de los beneficios que de ello espere obtener el responsable o un tercero.

---

[269] DATA PROTECTION COMMISSION (2017): *Informe Anual 2017*, p. 61.

[270] GRUPO DE TRABAJO DEL ARTÍCULO 29 (2014): *Dictamen 06/2014 sobre el concepto de interés legítimo del responsable del tratamiento de los datos en virtud del artículo 7 de la Directiva 95/46/CE* (WP 217), de 9 de abril, p. 11-12.

1.2. Aplicación más compleja

Tal y como será desarrollado en las próximas páginas, la correcta aplicación del interés legítimo no es ni sencilla ni directa. En efecto, no es suficiente con que el responsable del tratamiento considere que existe un interés legítimo -ya sea propio u ostentado por un tercero- para proceder al tratamiento de los datos. Como indica la autoridad británica de protección de datos, este planteamiento parece ser fruto de no comprender qué requiere exactamente la aplicación del interés legítimo.[271]

Ciertamente, la válida aplicación del interés legítimo en la práctica exige una justificación más elaborada que las demás bases de legitimización, pues requiere sopesar con precisión cuáles son los intereses legítimos del responsable -o una tercera persona- en relación con los intereses, derechos y libertades fundamentales del interesado. En consecuencia, si se aplica correctamente, el interés legítimo no debe servir de base para prácticas obscuras que utilizan el art. 6.1.f) RGPD como base para eludir la protección otorgada por RGPD a los derechos de los usuarios o para tratar datos sin el debido conocimiento del sujeto.

1.3. Estándar del interesado medio razonable

Como introdujimos en el capítulo anterior, el estándar del interesado medio razonable se refiere a los requisitos formales que conforman la base de legitimación, desde el punto de vista del interesado medio razonable sobre cuyos datos se dirija, con carácter general, la actividad de tratamiento.

En relación con el interés legítimo, ello se corresponde con la lectura legalista y formal del art. 6.1.f) RGPD como base legal para el tratamiento de datos personales. Este precepto requiere lo que normalmente se ha establecido como una evaluación en tres fases, que debe realizarse caso por caso. En primer lugar, debe existir un interés del responsable del tratamiento o de un tercero, que deberá ser legítimo. En segundo lugar,

[271] INFORMATION COMMISSIONER'S OFFICE (2019): *Update report into adtech and real time bidding*.

debe superarse un juicio de necesidad. En tercer lugar, debe realizarse una ponderación de intereses o juicio de ponderación que ponga en un lado de la balanza los intereses legítimos del responsable del tratamiento o de un tercero y en el otro los intereses, derechos y libertades de los interesados.[272]

1.4. Test de confianza

En la medida en que el responsable desee argumentar la licitud de una operación de tratamiento sobre un interés legítimo, propio o de tercero, dichos intereses deben ser expresados de conformidad con el art. 13.1.d) RGPD. El modo de dar cumplimiento a esta obligación, leída en relación con el principio de transparencia, es de forma tal que el responsable revele dichos intereses de manera explícita, de modo que el interesado, las autoridades de protección de datos, juristas o cualquier otra persona que acceda a la información, no tengan dificultad de comprender cuál es el objetivo final perseguido por el responsable.

Para ilustrar esto, podríamos recurrir a lo que orientativamente cabe bautizar como una "prueba de confianza". Con arreglo a esta prueba, el responsable del tratamiento debe realizar una autoevaluación previa y dilucidar si se siente cómodo a la hora de revelar, por ejemplo, cuáles son los objetivos del tratamiento, cuál es el interés legítimo aducido, qué datos se utilizarán, cómo o qué repercusiones pueden tener sobre los derechos de los interesados. Si comunicar de manera transparente esta información hace que el responsable no se sienta cómodo, entonces lo más probable es que el interés legítimo no sea una base de legitimación válida, sino que

[272] Esta evaluación ha sido ampliamente reconocida por diferentes agentes. Véase GRUPO DE TRABAJO DEL ARTÍCULO 29 (2014): *Dictamen 06/2014 sobre el concepto de interés legítimo del responsable del tratamiento de los datos en virtud del artículo 7 de la Directiva 95/46/CE* (WP 217), de 9 de abril; SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS (2016): *Developing a toolkit for assessing the necessity of measures that interfere with fundamental rights*; SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS (2017): *Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit*.

se pretenda utilizar para crear una ilusión de legitimación sobre tratamientos obscuros que de otro modo no podrían ser lícitos.

De hecho, la autoridad de control inglesa, el ICO, parece partir de esta aproximación al recomendar no utilizar el interés legítimo como base del tratamiento cuando el responsable pudiera sentirse "avergonzado por la publicidad negativa sobre cómo pretende tratar los datos".[273] En línea con esto, algunos académicos han definido en términos generales que los intereses legítimos serían la base más apropiada para las prácticas comerciales estándar inocuas.[274]

1.5. Carga de la prueba

En el ámbito del uso de tecnologías de análisis masivo de datos, la transparencia y su consideración como principio que trasciende el mero deber de información será de importancia capital, pues el responsable deberá poder demostrar que el interesado conoce y puede razonablemente comprender el contexto que rodea la recogida, análisis y posibles tratamientos posteriores de datos personales. Previsiblemente, esto únicamente puede lograrse mediante el uso de técnicas de información que sobrepasen un formulario de información complejo por naturaleza. En otros términos, el responsable debe ostentar la carga de la prueba de que el interesado medio razonable ha podido adquirir un nivel razonable de comprensión, entre otros, sobre el tratamiento, qué datos serán tratados o los posibles riesgos para el interesado.

En todo caso, lo que parece que el art. 6.1.f) aporta con respecto al art. 6.1.a) es el hecho de que el foco de atención se desplaza del interesado al responsable. Esto trasciende el hecho de que la carga de la prueba recaiga sobre el responsable -lo cual ocurre en otras bases de legitimación, reflejado, por ejemplo, en el hecho de que respecto del art. 6.1.a) el responsable deba guardar evidencia de haber obtenido el consentimiento

[273] INFORMATION COMMISSIONER'S OFFICE: *Guidance on legitimate interest*.

[274] Considerando 30 Directiva 95/46.

y de la información prestada-. El uso del interés legítimo como base del tratamiento conlleva vestir con un grado extraordinario de responsabilidad a quien realice el tratamiento, que debe mostrar un "sentimiento ético".[275] En relación con ello, el ICO también indica que

> [El responsable] "puede preferir considerar el interés legítimo como base de legitimación si desea mantener el control sobre el procesamiento y asumir la responsabilidad de demostrar que está en línea con las expectativas razonables de los interesados y que no tendría un impacto injustificado sobre estos. Por otra parte, si prefiere dar a los interesados el pleno control y la responsabilidad de sus datos (incluida la posibilidad de cambiar de opinión sobre si pueden seguir siendo objeto de tratamiento), puede que desee considerar la posibilidad de basarse en el consentimiento" (énfasis añadido).[276]

En otras palabras, el ICO recuerda algo quizás obvio, pero a la par muy relevante: el art. 6.1.f) como base de legitimación emplaza el foco de responsabilidad en el responsable del tratamiento, alejándolo así del interesado, que, como quedó argumentado en el capítulo anterior, es sobre quien recae la responsabilidad cuando el consentimiento es la base utilizada.

Más recientemente, el ICO ha vuelto a insistir en que el interés legítimo crea un compromiso adicional del responsable, que debe asegurarse de que los intereses, derechos y libertades de los usuarios han sido plenamente tomados en consideración.[277] En un sentido similar, la autoridad italiana ha manifestado que, de hecho, el interés legítimo como base de licitud del tratamiento, y la obligación de llevar a cabo una ponderación de intereses

[275] DIRECTOR DEL SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS (2018): "Data processing beneficial to individuals: the use of legitimate interest", en *Computers, Privacy and Data Protection Conference*, Bruselas.

[276] INFORMATION COMMISSIONER'S OFFICE (2019): *Lawful basis guidance*.

[277] INFORMATION COMMISSIONER'S OFFICE (2019): *Update report into adtech and real time bidding*.

es una de las manifestaciones más claras del principio de responsabilidad proactiva introducido en el Reglamento (art. 5.2).[278]

En todo caso, independientemente de la base de legitimación finalmente elegida, será labor del responsable demostrar que el uso de dicha base es válido y lícito, así como documentarlo.

1.6. Falta de criterios claros

A pesar de todo ello, ni la Directiva 95/46 ni el RGPD proporcionan indicadores o criterios sobre cómo aplicar esta base de legitimación -especialmente sobre cómo realizar el juicio de ponderación-. Esta falta de concreción puede verse como hecho causal que explique el uso reducido que ha recibido esta base de legitimación del tratamiento en la práctica.

Aunque cada vez se publican más comentarios y directrices en torno a esta cuestión, sigue siendo cierto que el interés legítimo no ha recibido ni de cerca tanta atención como otras bases de legitimación tales como el consentimiento, ya sea por parte de las autoridades de protección de datos, los profesionales de la justicia o la doctrina académica, a pesar de su gran relevancia para las organizaciones.

Si bien es cierto que ni la Directiva ni el RGPD proporcionan mucha orientación sobre cómo aplicar esta base de legitimación en lo que respecta a las circunstancias en las que se puede aplicar el interés legítimo, también lo es que el RGPD incorpora un algo más de dirección que la Directiva. Los considerandos 47 a 50 RGPD ofrecen algunos ejemplos de casos en los que puede existir la posibilidad de basar el tratamiento en el interés legítimo, como la prevención del fraude (considerando 47), la transmisión de datos personales entre un grupo de organizaciones con fines administrativos internos -por ejemplo, para el tratamiento de datos de los empleados- (considerando 48), la seguridad de las redes y de las tecnologías de la información (considerando 49) o la indicación por parte

[278] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Guida all'applicazione del Regolamento europeo in materia di protezione dei dati personali*.

del responsable del tratamiento de posibles actos delictivos o amenazas hacia la seguridad pública, junto con la transmisión de los datos personales pertinentes a una autoridad competente (considerando 50).

Asimismo, el RGPD también hace mención a la mercadotecnia directa (considerando 47). Es decir, parece que el Reglamento se abre a la posibilidad de que el interés comercial, del que subyace un interés económico, pueda calificarse de interés legítimo y constituir una base lícita de tratamiento conforme al art. 6.1.f). Sobre la mercadotécnica directa, el considerando 47 parecería referirse únicamente al envío de comunicaciones comerciales por medio postal, pero no por medios electrónicos. En efecto, el envío de comunicaciones comerciales por medios electrónicos se encuentra amparado por *lex especialis*, la Directiva e-Privacy (actualmente en proceso de actualización mediante el futuro Reglamento e-Privacy), y en el ámbito nacional, la Ley 34/2002 de 11 de julio, LSSICE (art. 21). Dichas normas no contemplan el interés legítimo como base de licitud. No obstante, recientemente, el EDPB ha señalado que sería posible basar la publicidad comportamental en interés legítimo.[279]

Por su parte, el GT 29 también aportó en su Dictamen sobre la materia algunos ejemplos de interés legítimo como el ejercicio de la libertad de expresión, la supervisión de empleados con fines de seguridad o de gestión.[280]

En cualquier caso, se trata de ejemplos en los que el interés legítimo "puede" aplicarse. Sin embargo, por un lado, este fundamento no siempre puede considerarse válido para las finalidades mencionadas en los considerandos y no debe aplicarse automáticamente. Incluso en estas circunstancias, el responsable del tratamiento debe llevar a cabo una evaluación para concluir si el art. 6.1.f) se aplica a su situación específica. Por otro lado, no se trata este de un listado cerrado de tratamientos que

[279] JELINEK, Andrea (2019): *IAPP Global Privacy Summit*.

[280] GRUPO DE TRABAJO DEL ARTÍCULO 29 (2014): *Dictamen 06/2014 sobre el concepto de interés legítimo del responsable del tratamiento de los datos en virtud del artículo 7 de la Directiva 95/46/CE* (WP 217), de 9 de abril.

puedan basarse en el interés legítimo, sino que, desde luego, será una evaluación que deba realizarse caso por caso.

2. El desarrollo histórico del interés legítimo en la regulación de la protección de datos personales

En capítulos anteriores hicimos referencia al desarrollo de las principales normas en materia de protección en datos, en relación con el avance tecnológico de la época y el desarrollo de algunas de las provisiones más relevantes sobre el objeto de este trabajo. Sin embargo, no nos referimos expresamente al surgimiento y evolución del interés legítimo como base de licitud del tratamiento en la normativa de protección de datos personales.

En este epígrafe analizaremos los principales hitos histórico-normativos que han dado lugar al actual art. 6.1.f) RGPD.

2.1. Precedentes del interés legítimo

2.1.1. Directrices OECD (1980)

Las Directrices sobre protección de la privacidad y flujos transfronterizos de datos personales de la OECD de 1980,[281] cuyo contenido ya introdujimos en el capítulo II, tenía como objetivo, no solo la protección de los derechos individuales, sino también la libre circulación de datos personales. Recordemos, estas Directrices hacían alusión a la posibilidad de tratar datos "con el conocimiento o consentimiento del sujeto de los datos", dejando ver que, ya desde los años 80, se preveían diversos motivos de licitud del tratamiento. Si bien el texto no menciona el interés legítimo, sí hace referencia en diversas ocasiones a una necesaria ponderación de intereses contrapuestos, redacción que recuerda, tanto en el concepto como en la terminología utilizada, a la actual redacción del art. 6.1.f) RGPD.

[281] ORGANIZACIÓN PARA LA COOPERACIÓN Y EL DESARROLLO ECONÓMICOS (1980): *Directrices sobre protección de la privacidad y flujos transfronterizos de datos personales*, de 23 de septiembre.

2.1.2. *Convenio Nº. 108 (1981)*

Tan solo un año más tarde se publicaba el primer documento internacional jurídicamente vinculante en materia de protección de datos personales.[282] Este documento no hacía referencia a las diferentes posibles bases de legitimación del tratamiento de datos personales.

El Convenio aludía al principio de licitud y lealtad, aunque sin desarrollarlo. Es decir, no reguló cuáles son las bases de licitud del tratamiento de datos personales. Así, no hace mención alguna al consentimiento, al interés legítimo ni a ninguna otra de las bases actuales, limitándose a dejar la cuestión abierta.

El texto fue actualizado en 2018,[283] con el objetivo de disponer de un instrumento adaptado a las realidades de los entornos en línea y las nuevas prácticas de recolección y tratamiento de datos personales. El texto refuerza los principios introducidos por el documento original, e introduce conceptos novedosos, tales como el principio de transparencia, de responsabilidad proactiva o la mención a los mecanismos de privacidad desde el diseño, todo ello en línea con el RGPD. Como novedad, la versión actualizada del Convenio incluye también una referencia a la necesidad de contar con una base de legitimación del tratamiento, que podrá ser el consentimiento u otra base establecida legalmente. Es destacable que el art. 5 del Convenio, en su versión actualizada, indica que el tratamiento deberá ser proporcional y reflejar un balance justo entre los intereses perseguidos y los derechos y libertades en lid, lo que recuerda al balance o ponderación de intereses necesario para aplicar el interés legítimo como base para el tratamiento. En otras palabras, el documento no detalla un listado de posibles alternativas al consentimiento. Sin embargo, este se presenta, de nuevo, como una opción entre las varias existentes y se

[282] CONSEJO DE EUROPA (1981): *Convenio 108, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal*.

[283] CONSEJO DE EUROPA (2018): *"Convenio 108" modernizado de 17 de 2018 para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal*.

reconoce la importancia de realizar un balance de intereses, derechos y libertades como garantía para un tratamiento de datos justo y leal.

2.2. Directiva 95/46. Cómo se creó la receta final del interés legítimo

La regulación del interés legítimo como base de licitud del tratamiento de datos personales en el Derecho comunitario tal y como la conocemos hoy en día surgió con la Directiva 95/46, en un proceso de múltiples cambios y compromisos.

En este apartado desarrollaremos cómo se gestó la redacción final del art. 7.f) de la Directiva, desde la primera propuesta de la Comisión, pasando por los textos de enmiendas del Parlamento y el Consejo.[284]

2.2.1. *Directiva 95/46. Propuesta de la Comisión Europea (1990)*[285]

Después de un estudio profundo en la materia, la Comisión Europea presentó, durante el verano de 1990 la primera propuesta de la que terminó por ser la Directiva 95/46, la norma que ha regulado el tratamiento de datos personales en los Estados miembros durante más de 20 años. En esta primera propuesta, la Comisión ya introduce una lista cerrada de bases de licitud del tratamiento. Como curiosidad, destaca que, en dicha propuesta, se diferenciaban los tratamientos llevados a cabo en el seno del sector privado y del sector público.

---

[284] Para una información pormenorizada sobre los comentarios y el proceso legislativo de la Directiva, véase: *Complete Travaux (English) of the Data Protection Directive*. Disponible en: https://resources.law.cam.ac.uk/cipil/travaux/data_protection/COMPLETETRAVEAU(ENGLISH)DPDIRECTIVE.pdf ; y CENTRE FOR INTELLECTUAL PROPERTY AND INFORMATION LAW, UNIVERSIDAD DE CAMBRIDGE, *Data Protection Directive, Detailed index of article development*. Disponible en: https://www.cipil.law.cam.ac.uk/resourceseuropean-travauxdata-protection-directive/detailed-index-article-development.

[285] COMISIÓN EUROPEA (1990): *Proposal for a Council Directive concerning the protection of individuals in relation to the processing of personal data* COM(90) 314 final – SYN 283, (90/C 277/03), de 27 de julio. Disponible en: https://resources.law.cam.ac.uk/cipil/travaux/data_protection/1%2027%20July%201990%20Proposal.pdf.

En este sentido, los datos contenidos en un fichero de una entidad pública[286] únicamente podrían ser comunicados a un tercero cuando este invocara un interés legítimo que no prevaleciera sobre el interés del interesado. Esto es, ya se introduce el conceto de interés de "tercero a quien se comuniquen los datos", que será el único caso en que una autoridad pública podría basar un tratamiento en el interés legítimo. Asimismo, la autoridad que cediera los datos de un interesado debía informarle de ello.

Por su parte, respecto de la licitud del tratamiento en el sector privado,[287] la propuesta de la Comisión incluía como bases de licitud el consentimiento del interesado, el tratamiento realizado bajo una relación (cuasi)contractual, el interés legítimo del responsable o el tratamiento de datos contenidos en fuentes accesibles al público. En concreto, se indicaba como motivo de licitud la persecución de un interés legítimo del responsable siempre que no prevaleciera el interés del interesado.[288]

En relación con los deberes de información, destaca también la capacidad otorgada a los Estados miembros para exceptuar este deber de información del responsable cuando la obligación "choca con los intereses legítimos superiores del responsable del tratamiento del fichero o con un interés similar de un tercero".[289]

Cabe destacar que esta primera versión exigía únicamente dos de los tres requisitos que finalmente se incluyeron en la versión definitiva de la

[286] Véase art. 6. El tratamiento en el sector público que tenga por objeto la comunicación de datos personales. Apartado 1.b): "Los Estados miembros dispondrán en su legislación que la comunicación de los datos personales contenidos en los ficheros de una entidad del sector público sólo será lícita si (...) es solicitada por una persona física o jurídica del sector privado que invoque un interés legítimo, a condición de que no prevalezca el interés del interesado" (traducción propia).

[287] Véase Capítulo III. Licitud del tratamiento en el sector privado. Art. 8.1.c): "Los Estados miembros dispondrán en su legislación que, sin el consentimiento del interesado, la inscripción en un fichero y cualquier otro tratamiento de datos personales únicamente serán lícitos si se han efectuado de conformidad con la presente Directiva y si (…) el responsable del fichero persigue un interés legítimo, a condición de que no prevalezca el interés del interesado" (traducción propia).

[288] Véase art. 6.3.

[289] Véase art. 10.

Directiva y que han trascendido hasta la actualidad gracias al RGPD. Primero, la existencia de un interés, que debe ser legítimo, y segundo, la obligatoriedad de llevar a cabo una ponderaciónde intereses. De hecho, el balance de intereses es un aspecto clave en la aplicación del interés legítimo y lo que le otorga distintividad a esta base de legitimación respecto de las demás. En este sentido, resulta relevante el hecho de que esta ponderación ya formase parte del contenido del interés legítimo desde la propuesta inicial de Directiva. Cabe apreciar, además, que únicamente se mencionan los "intereses" del interesado, en contraposición con la referencia a los "intereses, derechos y libertades fundamentales" de la redacción final de la Directiva. Por último, no se preveía de manera expresa en este momento el tercer requisito: que dicho interés debiera ser necesario para la finalidad del tratamiento o para la consecución del interés legítimo invocado.

Por último, la propuesta, que ya demuestra un claro desarrollo de los derechos de los interesados, regula un derecho de oposición "por motivos legítimos".[290]

2.2.2. *Directiva 95/46. Enmiendas del Parlamento Europeo (1992)*[***291***]

En su propuesta de enmiendas, el Parlamento realizó modificaciones sustanciales, algunas de las cuales en lo que se refería a la regulación del interés legítimo y las bases de licitud del tratamiento.

En primer lugar, el Parlamento elimina los preceptos que diferenciaban las bases de licitud para la comunicación de datos por parte de autoridades públicas y el tratamiento de datos en el sector privado, unificándolos. Así, un enmendado art. 8 indicaba que únicamente podría llevarse a cabo un tratamiento de datos personales con el consentimiento del interesado, si el

[290] Véase art. 14.

[291] PARLAMENTO EUROPEO (1992): *Proposal for a Council directive concerning the protection of individuals in relation to the processing of personal data* COM(90) 314 final – SYN 287, (C 94/173), de 11 de marzo. Disponible en: https://resources.law.cam.ac.uk/cipil/travaux/data_protection/22%2011%20March%201992%20Proposal.pdf.

tratamiento se realizaba bajo una relación (cuasi)contractual, si los datos provenían de fuentes accesibles al público para determinados tratamientos específicos, como el marketing, o si el interesado había tenido "la oportunidad de oponerse al tratamiento y no lo ha hecho".[292]

Asimismo, el responsable podría comunicar los datos, entre otros motivos, cuando así lo solicitase una persona (ya fuese física o jurídica, de Derecho público o no), que demostrase "de forma convincente que su interés en que los datos fuesen comunicados es justificado",[293] o cuando fuese "necesario" para salvaguardar los intereses legítimos de un tercero o del público general, siempre que no se perjudicasen los intereses del interesado.[294]

En relación con estos cambios caben destacarse diversos aspectos. En primer lugar, extraña el hecho de que el Parlamento dejase de lado el concepto de interés legítimo y lo sustituyese por un modelo de *opt-out*, que aporta menos garantías. La fórmula propuesta por el Parlamento ciertamente resultaba más cercana a la figura del consentimiento implícito, pues no requería que existiera un interés legítimo ni que este debiera ser contrapuesto con los intereses del interesado.

En segundo lugar, desde este conjunto de enmiendas destacaba que el consentimiento no tenía una posición preeminente como título de legitimación, sino que ostentaba igual rango que todas las demás, entre las que se incluía dicho *opt-out*.

En tercer lugar, el Parlamento individualiza las normas respecto de aquellos tratamientos consistentes en la comunicación de datos a un tercero. Respecto de ellos, alude por un lado a un "interés justificado" que debe ser demostrado por quien reclame acceder a los datos objeto de cesión, en una figura que parece abarcar tanto un interés propio como, sobre todo, de tercero. Por otro lado, este precepto alude también al concepto propio de

[292] Art. 8.1.c)(a) (nuevo).

[293] Art. 8.2.b).

[294] Art. 8.2.g).

interés legítimo, con la peculiaridad de que se le añade como garantía adicional el requisito de necesidad.

Lo que en todo caso parece desprenderse de las enmiendas del Parlamento es la creación de un sistema complejo de bases del tratamiento variadas. En concreto, el interés legítimo viró hacia una propuesta de derecho de oposición que no requería la realización de una ponderaciónde intereses. En consecuencia, el Parlamento había rebajado el nivel de exigencia para el tratamiento de datos. Si bien sus propuestas sentaron algunos de los pilares sobre los que descansa el desarrollo actual del interés legítimo, su propuesta aún sufrió cambios de calado.

2.2.3. *Directiva 95/46. Enmiendas del Consejo Europeo (1992)*[295]

En el otoño de 1992 el Consejo adoptó su postura respecto de la propuesta de Directiva de protección de datos, en la que mantiene la postura del Parlamento de eliminar las diferencias en las normas relativas al tratamiento de datos en el sector público y privado.

En el Memorándum explicativo que acompaña el texto del Consejo, este anuncia la existencia de una lista exhaustiva de circunstancias bajo las que puede producirse el tratamiento de datos, que incluyen una cláusula por la que se permite ponderar intereses privados. Esta cláusula de ponderación, detalla el memorándum, está orientada a poder ser utilizada en una gran variedad de tratamientos, desde la publicidad hasta la utilización de datos a los que se refiere como de dominio público. Para ello, otorga libertad a los Estados miembro para desarrollar cómo debiera realizarse el balance de intereses. Este margen de actuación concedido a los Estados no permitía, como fue puesto de manifiesto años más tarde por el TJUE en

[295] CONSEJO DE LA UNIÓN EUROPEA (1992): *Amended proposal for a Council Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data* COM(92) 422 final - SYN 287, de 15 de octubre. Disponible en: https://resources.law.cam.ac.uk/cipil/travaux/data_protection/27%2015%20October%201992%20Proposal%20.pdf

relación con la LOPD española, añadir requisitos adicionales a los que se estableciesen en la versión final de la Directiva.

Por medio del art. 7, el Consejo crea una configuración simplificada y reestructurada de las bases de licitud de datos personales, que no diferenciaba entre tratamientos originarios y otros tratamientos diferentes, o la cesión de datos. El motivo de ello es que el uso de una de las bases de licitud del art. 7 en conjunción con el principio de limitación de la finalidad sería, en opinión del Consejo, suficiente.

Destacaba la explicación expresa de que, bajo la Directiva, el consentimiento no es la base de licitud predilecta sobre la que recaerían excepciones, sino que se trata únicamente de una de las múltiples alternativas. Asimismo, el texto del Consejo aclaraba la redacción relativa a la base contractual, añadía el interés vital como base y, finalmente, aceptaba solo parcialmente la redacción del Parlamento sobre el interés legítimo. La propuesta del Consejo permitía el tratamiento de datos cuando este fuese necesario para la satisfacción de un interés general o un interés legítimo del responsable o un tercero a quien se comuniquen los datos, siempre que no prevalezcan los intereses de los interesados.

En esencia, se mantiene la posibilidad de invocar un interés propio o de un tercero, en dicho caso, para acceder a los datos del interesado y que le sean comunicados. Asimismo, queda claramente establecido el requisito de necesidad y la obligación de realizar una ponderación de intereses. Asimismo, se hace referencia a un “interés general”, cuya referencia no se mantendría en la versión final del precepto, reservado únicamente a los intereses legítimos. Por otro lado, el texto sigue refiriéndose únicamente a los “intereses” del interesado, si bien sabemos que en la versión final de Directiva se alude al interés o los derechos y libertades de este.

También se aumentaron los deberes de información y, siguiendo la estela marcada por el Parlamento, se estableció que el derecho de acceso no podría utilizarse para perjudicar los intereses legítimos del interesado, sino únicamente cuando así lo estableciera una norma, nacional o

comunitaria.[296] Un perjuicio como el comentado podría suceder, por ejemplo, cuando un empleador requiere a sus candidatos ejercer un derecho de acceso a determinada información como condición previa para obtener o continuar el empleo.

Por su parte, se reconoce un derecho de oposición del interesado por razones legítimas, tales como la falta de base de licitud del tratamiento.[297]

Tras los varios años de evolución de las diferentes versiones de Directiva, la norma definitiva terminó por instaurar la figura de interés legítimo en su art. 7.1.f con las tres características esenciales que aún hoy en día le pertenecen: la existencia de dicho interés, que debe ser legítimo; la superación de un juicio de necesidad y la evaluación de un juicio de ponderación. Todo ello acompañado de un derecho de oposición por el que el interesado puede reclamar la terminación del tratamiento para una finalidad concreta.

2.3. Reglamento General de Protección de Datos. Mucho ruido y pocas nueces

Tras más de dos décadas de vigencia de la Directiva 95/46, en 2016 se aprobó el RGPD. El nuevo Reglamento introdujo múltiples y profundos cambios en determinados aspectos normativos. Junto con la primera propuesta de RGPD, la Comisión Europea publicó en 2012 una evaluación de impacto[298] donde ya se identificaba la existencia de fragmentación en el modo en que diferentes Estados miembros habían transpuesto la regla del

[296] Art. 13.2.

[297] Art. 15.

[298] COMISIÓN EUROPEA (2012): *Commission Staff Working Paper. Impact Assessment Accompanying the document Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) and Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data* COM(2012) 10 final, de 25 de enero, p. 27. Disponible en: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012SC0072&from=EN.

interés legítimo de la Directiva en sus normas nacionales. Así por ejemplo, en algunos Estados miembros como Alemania indicaban expresamente que esta base era únicamente aplicable a responsables en el sector privado, otros como Italia añadían asimismo aquellos casos autorizados por la autoridad de control y otros como Finlandia preveían disposiciones sobre casos concretos. Por último, algunos Estados, como España, habían impuesto requisitos adicionales para el tratamiento de datos sobre la base del interés legítimo.

Aunque durante los varios años de procedimiento legislativo se debatió mucho sobre posibles cambios en la redacción de la base jurídica del interés legítimo, la redacción final en el RGPD se mantuvo prácticamente intacta respecto a aquella de la Directiva.

En todo caso, merece la pena observar los cambios propuestos desde la primera versión de RGPD del Consejo en 2012 hasta la aprobación del texto de 2016.

2.3.1. *RGPD. Propuesta de la Comisión Europea (2012)*

La propuesta de Reglamento del Consejo[299] preveía en su art. 6.1.f) modificaciones en la regulación del interés legítimo en relación con la Directiva. Quizás la más relevante fuese la eliminación de los intereses legítimos de terceros. Asimismo, la Comisión conservaba su capacidad para adoptar actos delegados mediante los que especificase las condiciones para la aplicación del interés legítimo, lo que fue criticado y eliminado de versiones posteriores.

En todo caso, mantiene la previsión de que los intereses, derechos o libertades del interesado no prevalezcan sobre los intereses legítimos del responsable. Asimismo, esta propuesta ya contempla la necesidad de

[299] COMISIÓN EUROPEA (2012): *Propuesta de Reglamento del Parlamento Europeo y del Consejo 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)* COM (2012) 11 final – 2012/0011 (COD), de 25 de enero. Disponible en: https://www.europarl.europa.eu/registre/docs_autres_institutions/commission_europeenne/com/2012/0011/COM_COM(2012)0011_ES.pdf.

prestar especial atención a la ponderación cuando el interesado sea un niño, la obligación del responsable de documentar ese ejercicio de ponderación de intereses e informar al interesado cuáles son los intereses perseguidos con el tratamiento, así como la prohibición de que las autoridades públicas acudan a esta base en el ejercicio de sus funciones.

2.3.2. *RGPD. Enmiendas del Parlamento Europeo (2014)*

En primera lectura, el Parlamento Europeo adoptó su posición en relación con la propuesta de RGPD, que contenía grandes cambios en relación con el interés legítimo.[300]

En primer lugar, el Parlamento incorpora de nuevo la referencia a los intereses legítimos de terceros a quien se comuniquen los datos como base jurídica. Además, se introduce, a modo de criterio, que el interés cumpla las expectativas razonables del interesado sobre la base de su relación con el responsable. De hecho, lo configura como el factor más relevante a tener en cuenta en la evaluación del interés legítimo. En relación con ello, el Parlamento expande enormemente los límites de las expectativas razonables al añadir que, siempre que se supere la ponderación de intereses, el tratamiento de datos seudónimos cumplirá las expectativas razonables del interesado. Esta provisión fue posteriormente eliminada debido a que la redacción podría dar lugar a interpretar que el uso de datos seudónimos podría permitir no realizar la ponderación de intereses.[301] Por su parte, el Parlamento indicaba que el tratamiento adicional de los datos puede quedar fuera de lo razonablemente esperado por el interesado. A

[300] PARLAMENTO EUROPEO (2014): *Resolución legislativa del Parlamento Europeo, de 12 de marzo de 2014, sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo 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)* (COM(2012)0011 — C7-0025/2012 — 2012/0011(COD)), de 12 de marzo. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52014AP0212&from=EN.

[301] GRUPO DE TRABAJO DEL ARTÍCULO 29 (2013): *Working Party comments to the vote of 21 October 2013 by the European Parliament's Libe Committee*, Anexo de la Carta a la Presidencia griega, de 11 de diciembre de 2013. Disponible en: https://ec.europa.eu/justice/article-29/documentation/other-document/files/2013/20131211_annex_letter_to_greek_presidency_wp29_comments_outcome_vote_libe_final_en_.pdf.

pesar de la eliminación de este extremo, podría extraerse la idea de que para el legislador el uso de datos seudónimos es un factor de grandísima relevancia durante la realización de la ponderación de intereses. Sin embargo, compartimos la opinión de que equiparar de modo casi automático el uso de datos seudónimos con el cumplimiento de las expectativas razonables del interesado diluiría enormemente las garantías de protección del interesado.

Asimismo, se mantiene el nivel de transparencia por el cual se obliga al responsable informar explícitamente al interesado de cuáles son los intereses legítimos perseguidos, documentarlo e informar sobre el derecho de oposición.

Por último, se mantienen las referencias a la especial atención que merece el interesado cuando este sea un niño así como la exclusión del interés legítimo para autoridades públicas en el ejercicio de sus funciones.

2.3.3. *RGPD. Enmiendas del Consejo (2015)*

Tras los múltiples cambios anteriores, a mediados de 2015 la propuesta de RGPD dada por el Consejo[302] ya contenía los elementos del interés legítimo de manera prácticamente idéntica a la finalmente adoptada.

Así, el criterio de la expectativa razonable de los interesados se traslada a los considerandos, sirviendo de criterio para la realización del balance de intereses, pero no como requisito obligatorio. Asimismo, los considerandos muestran diversos ejemplos de intereses legítimos, aunque ello no implica que el art. 6.1.f) pueda ser la base jurídica del tratamiento de manera automática, pues su aplicación requiere la realización del ejercicio de ponderación.

[302] CONSEJO DE LA UNIÓN EUROPEA (2015): *Propuesta de Reglamento del Parlamento Europeo y del Consejo 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) - Preparación de un planteamiento general*, 2012/0011 (COD) 9565/15, de 11 de junio. Disponible en: http://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/es/pdf.

En lo que resta de capítulo, el análisis del interés legítimo como base del tratamiento será llevaba a cabo tomando como punto de referencia la redacción final del art. 6.1.f) y los correspondientes considerandos.

2.4. Conclusiones

En esencia, después de un largo proceso de debate y diversas modificaciones, la forma final del art. 7 y, en particular, el interés legítimo, nació de la mano del Consejo en 1992 y cristalizó en la Directiva 95/46. Desde entonces, se mantiene esencialmente inalterada en el art. 6 RGPD a pesar de que durante el proceso legislativo[303] se debatieron diversas cuestiones como la eliminación del interés legítimo de terceros, la introducción de la expectativa razonable de los interesados como requisito, o una perspectiva favorable respecto de los datos seudónimos.

A pesar de ello, cabe destacar una importante apreciación. Si bien el art. 7.f) de la Directiva unificaba las bases de licitud independientemente de que el tratamiento fuera realizado en el seno del sector público o privado, el RGPD vuelve a realizar una distinción y restringe su uso al excluir la posibilidad de que las autoridades públicas acudan al interés legítimo en el ejercicio de sus funciones. Ello es debido a que el tratamiento de datos personales por las autoridades, cuando se encuentren ejecutando las funciones que les son propias, deberá contar siempre con una habilitación legal o derivarse de una obligación marcada por el ordenamiento jurídico.

Asimismo, el RGPD introduce el concepto de expectativa razonable de los interesados como criterio de gran importancia en la determinación del resultado del balance de intereses y e incluye en los considerandos algunos ejemplos de intereses legítimos. Estas adiciones pueden verse como resultado de las conclusiones de la evaluación de impacto[304] previa a la

[303] Para una información más detallada sobre los documentos y las discusiones de las diferentes versiones de RGPD durante el proceso legislativo, véase: TROIANO, Guglielmo (2015): *General Data Protection Regulation, a complete link collection*. Disponible en: https://europrivacy.info/2015/12/01/general-data-protection-regulation-a-complete-link-collection/.

[304] COMISIÓN EUROPEA (2012): *Commission Staff Working Paper. Impact Assessment Accompanying the document Regulation of the European Parliament and of the Council on*

terminación del RGPD, que ya identificaba la necesidad de clarificar las condiciones para la realización del ejercicio de ponderación de intereses que es requisito de esta base jurídica.

A pesar de todo ello, los elementos del interés legítimo continúan siendo ambiguos y han sido poco desarrollados en comparación con otros títulos de licitud del tratamiento de datos personales, a pesar del gran potencial de esta base, principalmente, para tratamientos llevados a cabo en el sector privado.

En páginas anteriores hacíamos referencia al estándar del interesado medio razonable en relación con la configuración del interés legítimo como base de licitud del tratamiento. Este estándar se compone de tres elementos. En primer lugar, debe existir un interés, ya sea este del responsable o de un tercero, y ha de ser legítimo. En segundo lugar, el tratamiento debe ser necesario para satisfacer dicho interés. Por último, dicho interés legítimo y necesario debe ponderarse con los intereses, derechos y libertades fundamentales del interesado en un ejercicio de ponderación que, en última instancia, determinará si que el tratamiento sea lícito o no.

En los próximos apartados iremos desgranando estos tres elementos con el fin de comprender mejor cómo se aplican. Se trata este de un comentario con carácter genérico, sin embargo, debemos recordar que la evaluación sobre la idoneidad de basar un tratamiento en el interés legítimo deberá realizarse caso por caso.

---

the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) and Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data COM(2012) 10 final, de 25 de enero. Disponible en: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012SC0072&from=EN.

3. ¿Qué es un interés legítimo?

Ni la Directiva de protección de datos ni el RGPD contienen una definición de qué se entiende por interés ni cuándo este puede ser legítimo. Este concepto resulta bastante flexible y abierto,[305] "elástico"[306] y ningún tipo de interés debe ser excluido *a priori*, sino que debe ser el responsable o encargado del tratamiento junto con los tribunales quienes llenen este término de contenido.

En este apartado haremos un acercamiento a qué debe entenderse por interés y cuándo este puede considerarse legítimo.

3.1. El concepto de "interés"

El concepto de lo que deba entenderse por "interés" resulta complejo por tratarse de un término jurídicamente indeterminado. Sin embargo, podemos esbozar sus contornos y definirlo como el valor o la intención general que el responsable del tratamiento desea cumplir a partir de la actividad de tratamiento. El interés puede entenderse como un beneficio buscado, un provecho, utilidad o ganancia esperada.

Este interés debe ser real y presente -esto es, no especulativo- y, aunque el concepto de interés es amplio en el sentido de que admite muchas categorizaciones, no debe ser demasiado vago en el caso específico, sino lo suficiente y claramente articulado para permitir que se lleve a cabo la ponderaciónde intereses.[307] Sin embargo, puesto que el RGPD no contiene

[305] Véanse las conclusiones del Abogado General presentadas en el asunto Rīgas satiksme (C-13/16, EU:C:2017:43), puntos 64 y 65. El Tribunal de Justicia ya ha reconocido como tales la transparencia (sentencia de 9 de noviembre de 2010, Volker und Markus Schecke y Eifert, C-92/09 y C-93/09, EU:C:2010:662, apartado 77) y la protección de la propiedad, la salud y la vida familiar (sentencia de 11 de diciembre de 2014, Ryneš, C-212/13, EU:C:2014:2428, apartado 34). Véanse también las sentencias de 29 de enero de 2008, Promusicae (C-275/06, EU:C:2008:54), apartado 53, y de 4 de mayo de 2017, Rīgas satiksme (C-13/16, EU:C:2017:336), apartado 29.

[306] TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA (2017): Asunto C-13/16, Rïgas, Opinión del Abogado General, de 26 de enero. ECLI:EU:C:2017:43, párrafo 65.

[307] GRUPO DE TRABAJO DEL ARTÍCULO 29 (2014): *Dictamen 06/2014 sobre el concepto de interés legítimo del responsable del tratamiento de los datos en virtud del artículo 7 de la Directiva 95/46/CE* (WP 217), de 9 de abril.

provisiones legales ni directrices sobre lo que puede considerarse un interés legítimo, más allá de los escasos ejemplos aportados en los considerandos, determinar en cada caso concreto cuándo existe un interés se trata de una cuestión abierta.

Por ejemplo, mientras que existen opiniones que se oponen a que la mera obtención de un beneficio económico pudiera considerarse un interés válido,[308] otras fuentes sí consideran que el crecimiento del negocio o el incremento de las ventas -que en últimos términos se traduce en un beneficio económico- sí serían ejemplos de interés legítimo.[309] Del mismo modo, el responsable o un tercero pueden tener, por ejemplo, interés en la protección de su propiedad intelectual o de la seguridad de sus sistemas. Por su parte, el interés de establecer una relación comercial o el envío de comunicaciones comerciales de un cliente también podría ser un interés del responsable del tratamiento, así como la prevención del fraude o la seguridad física/informática. ¿Y el interés en la elaboración de perfiles de clientes con el objetivo de conocerlos mejor para llevar a cabo acciones posteriores (que pueden incluir actividades de mercadotecnia o no)? En este caso, es posible que el responsable en realidad esté frente a diferentes fases del tratamiento que no deben ser unificadas bajo la definición de un único interés.

Del mismo modo, la naturaleza propia de los intereses también es amplia. Un interés legítimo puede estar directamente relacionado con el núcleo de actividad y de generación de valor del responsable, por ejemplo, cuando una aseguradora trata datos personales de su cliente y de una contraparte para solucionar una reclamación por daños. Otros intereses legítimos no forman parte del núcleo de la actividad del responsable, pero sí proporcionan una utilidad innegable, como por ejemplo el envío de

[308] DATA PROTECTION NETWORK (2018): *Guidance on the use of legitimate interests under the EU General Data Protection Regulation (v.2.0)*, p. 6.

[309] INFORMATION COMMISIONER'S OFFICE: *Guidance on legitimate interest*.

propaganda, la prevención del fraude o la implantación de medidas de seguridad.

Por otro lado, el interés puede ser comercial, individual o un beneficio social más amplio.[310] Es decir, no es necesario que el interés sea únicamente propio o de un solo tercero, sino que este puede ser colectivo o extenderse a la sociedad. De hecho, la existencia de un interés social general servirá de peso cuando se realice el juicio de ponderación contra los intereses individuales de los interesados.

Imaginemos, por ejemplo, el interés de una entidad bancaria en realizar un tratamiento de datos a gran escala para detectar fraude, blanqueamiento de capitales o pagos no autorizados por el titular de la cuenta. Para ello, la entidad utiliza datos provenientes de una gran variedad de fuentes, los analiza en tiempo real y crea un modelo algorítmico que detecta patrones de comportamiento sospechosos, tales como la retirada de dinero en un cajero automático en un país lejano o el desvío de pequeñas cantidades de dinero a cuentas opacas. Dicha entidad tendría un interés legítimo propio en detectar operaciones fraudulentas. Adicionalmente, existe un interés de la sociedad en sentido amplio la prevención del blanqueo de capitales o la implantación de medidas que impidan acceder o utilizar fondos no autorizados.

Por último, la definición de interés en el sentido del art. 6.1.f) no precluye *a priori* siquiera intereses que puedan ser vistos como banales o triviales. No obstante, este hecho sí pueda ser considerado durante la realización del juicio de ponderación o conllevar una mayor facilidad para ejercitar el derecho de oposición de los interesados.

3.2. El concepto de "legítimo"

El interés del responsable o un tercero será legítimo cuando respete todas las normas pertinentes (no sólo las leyes de protección de datos) y así lo

[310] INFORMATION COMMISSIONER'S OFFICE (2018): *Guide to the General Data Protection Regulation (RGPD)*, p. 81.

permita la legislación de la UE y nacional.[311] En dicha definición deben considerarse, asimismo, no solo normas comunitarias y leyes de aplicación nacional, sino también, cuando corresponda, normas de menor rango o jurisprudencia. Sin embargo, esto no quiere decir que tal interés se derive en gran medida de un instrumento jurídico. La naturaleza del interés no importa a la hora de evaluar su legitimidad, aunque, de nuevo, sí será importante durante la ponderación de intereses.[312]

Por esta razón, una actividad ilegal o prohibida no podrá considerarse un interés legítimo y no puede basarse en esta disposición.[313] Por ejemplo, imaginemos el caso de una red social profesional que construye un motor de recomendaciones con el objetivo de perfilar a los usuarios para que discriminen a las mujeres ofreciéndoles trabajos con menores ingresos. Existe un interés del responsable en crear un servicio de conexión de ofertantes y demandantes de empleo en función de características, entre las que se incluye el sexo del candidato. Sin embargo, en la medida en que parte del objetivo del responsable se sustente en características discriminatorias, dicho interés será ilegítimo. El tratamiento de datos personales referentes al sexo de los usuarios de la red social o incluso de categorías de datos respecto de los cuales se pueda inferir el sexo, para dicha finalidad no podría estar basado en el art. 6.1.f) RGPD.

Por su parte, opiniones destacadas como la de la oficina de protección de datos del Principado de Liechtenstein, ha destacado que la legitimidad es un concepto relacionado con la aceptabilidad social de determinada conducta, señalando como potenciales intereses legítimos el ejercicio de

[311] CONSEJO DE LA UNIÓN EUROPEA (1992): *Amended proposal for a Council Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data* COM(92) 422 final - SYN 287, de 15 de octubre, Comentarios a los artículos, p. 15.

[312] KAMARA, Irene; DE HERT, Paul (2018): "Understanding The Balancing Act Behind The Legitimate Interest Of The Controller Ground: A Pragmatic Approach", Rochester Institute of Technology, New York, Jules Polonetsky, Omer Tene (eds.), *The Cambridge Handbook of Consumer Privacy*, Cambridge University Press, pp. 321-352.

[313] ZUIDERVEEN BORGESIUS, Frederik J. (2015): *Improving Privacy Protection in the Area of Behavioural Targeting*, Kluwer Law International BV, p.155.

derechos fundamentales específicos como la libertad de opinión, prensa y difusión, el ejercicio de reclamaciones legales o tratamientos realizados en el contexto de la libertad ocupacional. En este sentido, el tratamiento de datos personales no solo no debería ser contrario a las normas jurídicas, sino además, tampoco debería ser contario a los valores sociales predominantes.[314]

Así, parece que el concepto de interés es amplio y puede incluir cualquier bien jurídico reconocido como tal por un sistema, ya sea este económico, legal, de hecho, o moral.[315]

En conclusión, parece que la definición legal de lo que pueda considerarse interés legítimo es amplia y abarca un gran rango de intereses. Por este motivo, se hace relativamente sencillo invocar la existencia de dicho interés legítimo.

No obstante, ello no implica asumir que es igualmente sencillo invocar el art. 6.1.f) como base de legitimación válida para el tratamiento de datos personales, pues este debe superar un balance de intereses, que puede de hecho ser complejo de superar, tal y como analizaremos en epígrafes posteriores.

3.3. Algunos ejemplos dudosos

A pesar de todo lo anteriormente dicho, ello no obsta para que determinados intereses pudieran encontrarse en zonas grises en tanto dieran generar dudas sobre si el nivel de especificidad requerido para definir el interés para el tratamiento de datos es suficiente. Veamos algunos ejemplos de servicios de la sociedad de la información utilizados por una gran masa de usuarios.

---

[314] BYGRAVE, Lee A. (2002): *Data Protection Law: Approaching Its Rationale, Logic and Limits*, Kluwer law international, p. 61.

[315] DATENSCHUTZSTELLE FÜRSTENTUM LIECHTENSTEIN, *Berechtigtes Interesse gem. Art. 6 Abs. 1 Bst. f DSGVO*. Disponible en: https://www.datenschutzstelle.li/datenschutz/themen-z/berechtigtes-interesse-gem-art-6-abs-1-bst-f-dsgvo.

1. *Criptomoneda*

La política de privacidad de la asociación que gestiona una criptomoneda indica: "[c]ontamos con una variedad de bases de legitimación del tratamiento, incluyendo (…) en la medida en que sea necesario para nuestros (u otros terceros) intereses legítimos, *incluido* nuestro interés en prestar un servicio innovador, personalizado, seguro y rentable a nuestros usuarios y socios, a menos que sobre esos intereses prevalezcan tus intereses o derechos y libertades fundamentales que requieren de una protección de datos personales".

Diversos comentarios podrían hacerse de esta aseveración en relación con la falta de especificidad de los intereses legítimos invocados, pero nos centraremos en dos principales. En primer lugar, la mención a la existencia de intereses legítimos varios, para después concretar únicamente algunos de ellos a modo meramente ejemplificativo -tal y como se desprende del término "incluido"-. En segundo lugar, la referencia concreta a la prestación de un servicio innovador como interés legítimo, sobre el que concurre un elevado nivel de vaguedad y falta de concreción.

2. *Aplicación de citas*

En modo similar, la política de privacidad de una conocida aplicación de citas indica, en términos faltos de especificidad, "podemos utilizar su información cuando tengamos intereses legítimos para hacerlo", a lo que se añade, a título ejemplificativo, "por ejemplo, analizamos el comportamiento de los usuarios en nuestros servicios para mejorar continuamente nuestras ofertas, sugerimos ofertas que creemos que pueden interesarle y procesamos la información para fines administrativos, de detección de fraude y otros fines legales". Así pues y con la información facilitada, ¿puede interpretarse que se cumple la necesaria especificidad en la determinación de las finalidades del tratamiento? ¿Existe dicha especificidad respecto de la indicación de los intereses legítimos alegados por el responsable? Y por último ¿es el interesado capaz de conocer sobre qué base de legitimación se tratan sus datos personales, a los efectos, por

ejemplo, de poder conocer si cabe la posibilidad de ejercer su derecho de oposición?

Bien es cierto que, en ocasiones, la redacción y la delimitación exacta de las finalidades del tratamiento podrán no ser sencillas. Ello no obsta, sin embargo, para que el responsable no realice un ejercicio exhaustivo de transparencia que concluya con un nivel de determinación, al menos, adecuado para hacer saber a los interesados sobre qué tratamientos pueden ejercer derechos tales como el de oposición.

3. *Medidor de actividad física*

Otro ejemplo interesante es un dispositivo que, entre otras funcionalidades, mide el nivel de actividad física del usuario. En su política de privacidad se realiza una somera identificación de sus finalidades del tratamiento, tales como proporcionar y mantener los servicios; mejorar, personalizar y desarrollar los servicios; comunicación con el usuario; fomento de la seguridad y protección. A continuación, únicamente se indica que se utilizan diversas bases de legitimación entre las que "se incluyen" el consentimiento del usuario e "intereses comerciales legítimos, como mejorar, personalizar y desarrollar los Servicios, comercializar nuevas funciones o productos que podrían interesarle y promover la seguridad y la protección". Es decir, parece que en este caso ni tan siquiera se liga una actividad concreta de tratamiento con su base de legitimación correspondiente.

4. *Motor de búsqueda*

Por su parte, la política de privacidad de un gran motor de búsqueda con fecha de junio de 2019 detallaba entre las finalidades de los tratamientos basados en interés legítimo la de personalizar servicios para ofrecer una mejor experiencia de usuario, así como la de ofrecer publicidad para que los usuarios puedan acceder gratuitamente a diversos servicios. Esta redacción podría ser considerada adecuada de no ser porque en el párrafo previo se informa de que el responsable utiliza consentimiento para ofrecer

al usuario servicios personalizados, tales como anuncios basados en los intereses del usuario.

De este modo, al interesado medio no le resulta sencillo conocer qué base de legitimación se utiliza, de hecho, cuando recibe publicidad. Una posibilidad de entender esta redacción es que Google basara en su interés legítimo la oferta de publicidad, por ejemplo, contextual, y únicamente después de haber obtenido consentimiento, se haría un tratamiento más extenso de datos personales para perfilar al usuario y presentarle publicidad personalizada. Sin embargo, este hecho no queda claramente especificado.

3.4. Los terceros

El RGPD se refiere a los intereses legítimos tanto del responsable del tratamiento como de un tercero. Si bien el concepto de responsable del tratamiento parece claro a este respecto, lo que constituye un tercero puede resultar problemático. Esto se debe a que la definición de "tercero" dispuesta en RGPD excluye a diversas partes.

En concreto, el art. 4.10 RGPD define al tercero como "persona física o jurídica, autoridad pública, servicio u organismo distinto del interesado, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas para tratar los datos personales bajo la autoridad directa del responsable o del encargado" (énfasis añadido).[316] Ejemplos de quiénes podrían considerarse terceros cuyo interés legítimo podría ser objeto de protección y configurar la base del tratamiento podrían ser un cliente de una entidad o un individuo que desee presentar una queja o acción legal contra una persona, para lo cual puede necesitar acceso a algunos datos personales de dicha persona. Asimismo, los terceros pueden ser el conjunto de ciudadanos con carácter genérico, en relación, por

[316] Por su parte, el GT 29 también definió el concepto de tercero en GRUPO DE TRABAJO DEL ARTÍCULO 29 (2010): *Dictamen 1/2010 sobre Dictamen 1/2010 sobre los conceptos de «responsable del tratamiento» y «encargado del tratamiento»* (WP 169), de 16 de febrero.

ejemplo, al interés que estos ostentan en conocer información sobre los sueldos de directivos, la lucha contra el blanqueo de capitales o la pornografía infantil.

Por ejemplo, una entidad aseguradora puede tener un interés legítimo en reducir el fraude entre sus asegurados. Ante la sospecha de fraude en un caso particular, podría solicitar a la entidad telefónica del asegurado acceder a la grabación de todas las llamadas realizadas en el último mes, con el objetivo de conocer si el asegurado ha confesado el fraude a sus allegados. La entidad telefónica, responsable del tratamiento de dichos datos, deberá analizar la posible existencia de un interés legítimo de tercero -la compañía aseguradora-. En este caso, la detección del fraude constituye un interés claro de la aseguradora. Además, la finalidad de obtener una posible confesión del fraude es específica, real y actual. Sin embargo, el acceso al contenido de las comunicaciones electrónicas no es legítimo en virtud de la Directiva e-Privacy (y el futuro Reglamento e-Privacy). En conclusión, la solicitud no superaría el primer requisito para aplicar el art. 6.1.f) RGPD y ni siquiera sería preciso proseguir a analizar si el tratamiento es necesario para la finalidad deseada o a realizar una ponderación de intereses.

En el asunto Rīgas, el Abogado General recoge en sus conclusiones una defensa de una aproximación razonable al uso del art. 6.1.f). Así, aquél tercero que solicite información a un responsable alegando un interés legítimo, debe aportar toda la información relevante para permitir analizar la existencia de su interés legítimo, que servirá de base para que el responsable del tratamiento le proporcione los datos solicitados sin necesidad de tener que realizar diferentes peticiones a otros interesados. En concreto, el Abogado General del caso Rīgas indicaba a este respecto que “[e]n lenguaje metafórico, la aplicación del criterio de necesidad no puede convertir la realización de un interés legítimo en una búsqueda del tesoro kafkiana que se parezca enormemente a un episodio de Fort Boyard, en el que los participantes son enviados de una habitación a otra a fin de

recabar pistas parciales que les permitan saber finalmente dónde deberían ir".[317]

Es decir, el hecho de que los datos solicitados al responsable puedan ser también obtenidos de otras fuentes no debe jugar en contra de considerar que existe un interés legítimo del tercero para obtener los datos directamente del responsable, sin embargo, el tercero que alegue dicho interés legítimo para que le sean cedidos determinados datos de un interesado debe esforzarse por mostrar la información relevante que sostenga su invocación del interés.

Por otro lado, la concreción de quiénes pueden ser considerados terceros se ve influida por la definición de otras figuras. Especialmente destacable es la corriente jurisprudencial del TJUE, que en los últimos años ha realizado una interpretación amplia del concepto de responsable del tratamiento (más concretamente, de la figura de la corresponsabilidad) en diversas resoluciones (véanse los casos Fashion ID,[318] Wirtschaftsakademie[319] o Testigos de Jehová)[320]. Así por ejemplo, destaca el caso FashionID. El caso transcurre en torno a la distribución de responsabilidad entre dos entes diferentes. Por un lado, el administrador de un sitio web de venta de moda FashionID. Por otro lado, la red social Facebook, que recoge datos de usuarios de páginas webs de terceros administradores cuando estos insertan en su página web el botón "Me gusta" de Facebook. Tras analizar el tratamiento de datos, el Tribunal determinó que los administradores que deciden incluir dicho botón en su sitio web están tomando la decisión de utilizar medios que permiten que Facebook recopile datos. Por este motivo, no son en realidad terceros, sino

[317] TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA (2017): Asunto C-13/16, Rïgas, Opinión del Abogado General, de 26 de enero. ECLI:EU:C:2017:43, párrafo 75.

[318] TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA (2019): Asunto C-40/17, Fashion ID GmbH & Co. KG vs Verbraucherzentrale, de 29 de julio. ECLI:EU:C:2019:629.

[319] TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA (2018): Asunto C-210/16, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein vs Wirtschaftsakademie Schleswig-Holstein GmbH, de 5 de junio ECLI:EU:C:2018:388.

[320]TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA (2018): Asunto C–25/17, Tietosuojavaltuutettu vs Jehovan todistajat, de 10 de julio. ECLI:EU:C:2018:551.

corresponsables de la recogida de los datos y deben por tanto tener una base jurídica propia y cumplir con las obligaciones del RGPD, tales como el deber de informar. Es decir, ambos responsables, Facebook y el administrador de la página web, deben poder alegar un interés legítimo propio para el tratamiento.

En otro orden de cosas, pensemos también en aquellos terceros, corredores de datos y otros intermediarios del mercado de datos cuyo modelo de negocio se basa en acceder y posteriormente analizar datos de los usuarios de una página web. En caso de que estos agentes sean considerados terceros, y no corresponsables en función de la doctrina Fashion ID, dichos terceros tienen un interés en poder recopilar los datos del mayor número de usuarios de internet, y además, dicho interés es comercial y por tanto legítimo. Asimismo, se podría argumentar que, al menos para algunos de dichos terceros, el tratamiento es necesario para desplegar su modelo de negocio. Así, el administrador de una determinada página web podría analizar si el interés legítimo de cada uno de los terceros puede servir de base del tratamiento consistente en recopilar información rica y en tiempo real sobre todos los usuarios de la página web. Este tratamiento parece desproporcionado y no superaría un juicio de ponderación de intereses. Conceder acceso a cientos de terceros con los que el interesado no tiene relación a los datos personales de miles de usuarios en cada interacción con un sitio web para tratamientos que el propio responsable (administrador web) no puede ver, no superaría el ejercicio de ponderación. En consecuencia, tratamientos cada vez más comunes en nuestro día a día, tales como permitir cookies de terceros, deberán ser consentidas por el usuario.

4. El concepto de “necesidad”

El segundo paso de los tres necesarios para la evaluación de los intereses legítimos es la valoración de si el tratamiento es "necesario" para los fines previstos.

La redacción del art. 6 revela que, con excepción del art. 6.1.a) (consentimiento), todas las demás bases de legitimación exigen expresamente que el tratamiento sea "necesario". No obstante, incluso aunque el consentimiento pudiera parecer la única base de legitimización que no requiere necesidad, sí implica necesidad hasta cierto punto, ya que un consentimiento válido en términos del RGPD se da para un propósito o finalidad específica, y dicho tratamiento debe ser necesario en relación con la finalidad de acuerdo con el art. 5.1.c).[321] Esto muestra la centralidad del concepto de necesidad en el art. 6 para el tratamiento legal de los datos personales.

En este sentido, el TJUE ha señalado que las derogaciones y limitaciones del derecho a la protección de datos únicamente deben aplicarse cuando sea estrictamente necesario. Por ello, la cantidad y naturaleza de los datos objeto de tratamiento no deben ser mayores de lo necesario para la finalidad del tratamiento. [322] Sin embargo, la necesidad es un concepto más amplio que el de estrictamente "esencial" para la finalidad. En el asunto Huber, el TJUE argumentó que el concepto de necesidad "tiene su propio significado en el Derecho comunitario".[323]

Para evaluar la necesidad, debe tenerse en cuenta si el responsable del tratamiento puede lograr razonablemente el mismo objetivo sin dicho

[321] HILDEBRANDT, Mireille (2019): "Privacy as protection of the incomputable self: From agnostic to agonistic machine learning", en *Theoretical Inquiries in Law*, Vol. 20, No. 1, pp. 83-121.

[322] Sirvan, por todas, TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA (2010): Asuntos acumulados C-92/09 y C-93/09, Volker und Markus Schecke y Eifert, de 9 de noviembre. ECLI:EU:C:2010:662, párrafo 86; y TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA (2014): asunto C-212/13, Ryneš, de 11 de diciembre. ECLI:EU:C:2014:2428, párrafo 28.

[323] TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA (2008): Asunto C-524/06, Huber, de 16 de diciembre. ECLI:EU:C:2008:724, párrafo 52. "Por consiguiente, habida cuenta del objetivo consistente en equiparar el nivel de protección en todos los Estados miembros, el concepto de necesidad, tal como resulta del artículo 7, letra e), de la Directiva 95/46 – cuyo objeto es delimitar con precisión uno de los supuestos en los que resulta lícito el tratamiento de datos personales, no puede tener un contenido variable en función de los Estados miembros. Por lo tanto, se trata de un concepto autónomo del Derecho comunitario que debe recibir una interpretación idónea para responder plenamente al objeto de dicha Directiva, tal como se define en el artículo 1, apartado 1, de la misma", esto es, la defensa del derecho a la intimidad, la protección de datos personales y las libertades y derechos fundamentales de las personas físicas.

tratamiento o por medios menos intrusivos, equilibrando la proporcionalidad entre el tratamiento y la finalidad. Si tal es el caso, la base legal no puede considerarse necesaria y, por lo tanto, no será aplicable.[324] En otras palabras, “el fin no justifica los medios”, pues el tratamiento no puede ir más allá de lo necesario para la finalidad. Además, esta relación también debe funcionar a la inversa: los medios del tratamiento deben ser capaces de conseguir el objetivo perseguido.

El requisito previo de la necesidad también aparece en la Carta de los Derechos Fundamentales de la UE y en el Convenio Europeo de Derechos Humanos (CEDH), que exigen que cualquier interferencia o limitación del derecho a la intimidad y a la protección de datos sea "necesaria". Algunos autores afirman que el concepto de "necesario" en la ley de protección de datos debe interpretarse en línea con la jurisprudencia del Tribunal Europeo de Derechos Humanos (TEDH). Así, merece la pena señalar que el TEDH se ha pronunciado sobre lo que implica la necesidad, y ha establecido este término no es sinónimo de "indispensable", pero tampoco tiene la flexibilidad de expresiones como "admisible", "normal", "útil", "razonable" u "oportuno".[325]

Por contra, el Supervisor Europeo de Protección de datos (SEPD) ha declarado que el concepto de necesidad utilizado por el TEDH no es equivalente al concepto de necesidad que sirve de requisito para las bases de licitud del art. 6 RGPD. Concretamente, el SEPD alega que "la necesidad de las operaciones de tratamiento en el Derecho derivado de la UE y la necesidad de las limitaciones al ejercicio de los derechos

[324] Así lo han interpretado diversos agentes. Véase GRUPO DE TRABAJO DEL ARTÍCULO 29 (2014): *Dictamen 06/2014 sobre el concepto de interés legítimo del responsable del tratamiento de los datos en virtud del artículo 7 de la Directiva 95/46/CE* (WP 217), de 9 de abril; INFORMATION COMMISSIONER’S OFFICE (2017): *Big data, artificial intelligence, machine learning and data protection* (versión 2.2); DATENSCHUTZSTELLE FÜRSTENTUM LIECHTENSTEIN, *Berechtigtes Interesse gem. Art. 6 Abs. 1 Bst. f DSGVO*.

[325] TRIBUNAL EUROPEO DE DERECHOS HUMANOS (1983): Sentencia 5947/72, Silver y otros v Reino Unido, de 25 de marzo, párrafo 97.

fundamentales se refieren a conceptos diferentes".[326] En consecuencia, el SEPD ha establecido que el conceto de necesidad del art. 6 RGPD debe entenderse en el sentido de que cualquier dato que no esté directamente relacionado con la obtención, realización o cumplimiento del interés legítimo perseguido no se basa en un tratamiento lícito. En consecuencia, el concepto de necesidad implica la necesidad de una evaluación que tenga en cuenta, tanto la eficacia del tratamiento de los datos para el fin específico, como la evaluación de si existe una forma menos intrusiva de que los derechos de las personas logren el mismo objetivo.[327]

Asimismo, la red Data Protection Network (Red de Protección de Datos) ha proporcionado orientación a este respecto afirmando que el concepto necesidad no requiere una carga tan elevada como la de indispensabilidad, pero tampoco tan baja como la de utilidad o deseabilidad.[328] Por ejemplo, si existe otra manera de perseguir el mismo objetivo, pero esta requiere un esfuerzo desproporcionado, entonces el tratamiento tal como se concibe puede considerarse necesario.

Ahora bien, la autoridad inglesa de protección de datos parece abrir la concepción de lo que debe considerarse necesario. El ICO afirma en sus directrices sobre interés legítimo que algunas prácticas como la elaboración de perfiles o la publicidad no son esenciales para el tratamiento, pero sí pueden ser necesarias para las finalidades del responsable.[329] De este modo, en la medida en que el responsable defina los fines del tratamiento y sus intereses de manera claramente específica, sin “esconderse tras objetivos comerciales vagos que podrían lograrse de otro modo”, podría

[326] SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS (2016): *Developing a toolkit for assessing the necessity of measures that interfere with fundamental rights*; SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS (2017): *Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit*.

[327]SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS (2017): *Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit*.

[328] DATA PROTECTION NETWORK (2018): *Guidance on the use of legitimate interests under the EU General Data Protection Regulation (v.2.0)*.

[329] INFORMATION COMMISSIONER’S OFFICE: *Guidance on legitimate interest*.

satisfacer este requisito de la evaluación del interés legítimo. Así, parece que una concreción clara de los fines del tratamiento, los intereses y una aplicación estricta del principio de limitación de las finalidades puede ayudar a llenar de contenido el test de necesidad.

Por otro lado, como ya señalaba el GT29, el concepto de interés está estrechamente relacionado con aquél de finalidad, y por tanto, con el principio de limitación la finalidad del actual art. 5.b RGPD. Curiosamente, de hecho, el propio GT29 parece asemejar ambos términos cuando señala como ejemplos de interés legítimo, entre otros, los tratamientos "con *fines* históricos, científicos o de investigación". Sin embargo, se trata de nociones diferentes, en el sentido de que el de interés es un concepto más amplio que el de finalidad.

De hecho, cabría incluso llegar a entender que la noción de interés puede incluir el propósito de alcanzar un fin determinado a través de un medio concreto, por ejemplo, a través de medios técnicos específicos -siempre, eso sí, que se cumplan los demás requisitos legales-. En este sentido, podría delimitarse como un interés del responsable la persecución de un fin utilizando tecnologías de tratamiento y análisis de datos masivos con la finalidad de obtener conocimiento de otro modo oculto en las bases de datos. De este modo, cabría preguntarse a continuación si el tratamiento es necesario para conseguir la finalidad de descubrir información a partir de datos primarios -es decir, durante la Fase 2-Análisis-. En caso de que pudiese argumentarse que no existe otro medio para conseguir razonablemente este interés u objetivo, el responsable superaría el test de necesidad. A pesar de todo, recordemos que deberá seguir teniendo en cuenta las circunstancias del caso concreto para justificar la superación o no del ejercicio de ponderación.

Se trata, en esencia, de encontrar un medio apto en Derecho para permitir al responsable o a un tercero exigir el cumplimiento del ordenamiento jurídico para obtener un beneficio o alcanzar una utilidad, a través del

tratamiento de datos de los interesados, siempre que ello no sea desproporcionado.

De hecho, la necesidad de un tratamiento también depende, en gran medida, de las circunstancias del caso concreto e implica un cierto grado de subjetividad. En todo caso, los límites externos de lo que es necesario en cada caso deben ser establecidos por los principios relativos al tratamiento de datos personales previstos en el art. 5, tales como la licitud, lealtad, la minimización de datos o la integridad y confidencialidad.[330] Especial importancia reciben en este sentido el principio de calidad de los datos, según el cual estos deben ser adecuados, pertinentes y no excesivos en relación con los fines para los que son recogidos y utilizados posteriormente.

Así por ejemplo, pensemos en el caso de un responsable que alega un interés legítimo para el tratamiento de datos personales con la intención de mostrar publicidad personalizada al usuario este accede a una página web. Dependiendo de cómo se defina la finalidad del tratamiento, el requisito de necesidad adquiere matices. Un responsable que defina su finalidad del tratamiento -concepto relacionado, aunque no necesariamente coincidente con la definición de su interés legítimo- como la presentación de publicidad comportamental podría argumentar que la realización de perfiles ricos de cada usuario es necesaria para la presentación de publicidad individualizada para sus gustos. En todo caso, a continuación, el responsable debería demostrar que, además, supera el balance de intereses, lo cual se dificulta.

Por su parte, si la finalidad del tratamiento se describe de manera más amplia como la presentación de publicidad, se podría concluir que no es necesario llevar a cabo un tratamiento de datos tan intenso como el descrito en el caso anterior, sino que bastaría con una observación de datos

[330] KAMARA, Irene; DE HERT, Paul (2018): "Understanding The Balancing Act Behind The Legitimate Interest Of The Controller Ground: A Pragmatic Approach", en Rochester Institute of Technology, New York, Jules Polonetsky, Omer Tene (eds.), *The Cambridge Handbook of Consumer Privacy*, Cambridge University Press, pp. 321-352.

contextual y no comportamental para poder adecuar el contenido publicitario a la persona, sin llegar a realizar una total personalización. En este caso, además, el responsable tendrá más facilidad para superar la posterior prueba de ponderación de intereses.

En relación con todo ello, es de señalar que los arts. 13 y 14 RGPD imponen al responsable la obligación de informar de que la base de licitud de una actividad concreta es el art. 6.1.f, y en su caso, qué intereses legítimos específicos sostienen el tratamiento. Sin embargo, no se encuentran compelidos a justificar por qué el tratamiento se vincula por un nexo de necesidad o de causalidad con el interés perseguido. En otras palabras, no existe obligación de publicitar la justificación del test de necesidad.

5. El otro lado de la balanza: los intereses, derechos y libertades del interesado

Los responsables del tratamiento están acostumbrados a tomar en consideración, medir y evaluar sus propios intereses y riesgos. Sin embargo, además del interés legítimo perseguido por el responsable del tratamiento, ya sea propio o de terceros, el art. 6.1.f) establece que en el lado contrapuesto de la balanza deban tomarse en consideración los intereses, derechos y libertades fundamentales del interesado y el impacto que el tratamiento tenga sobre estos.

5.1.1. *Inversión de la carga de la prueba*

Unas líneas atrás decíamos que la obligación de llevar a cabo un balance de intereses es el factor más distintivo del interés legítimo como base de licitud. Ello es debido, en realidad, a la necesidad de tomar en consideración al interesado, que constituye uno de los principales factores diferenciadores, al menos en lo que respecta a tratamientos realizados en un entorno privado. En este sentido, podría incluso hablarse de una suerte de inversión de la carga de la prueba.

En efecto, en el capítulo anterior argumentábamos cómo el consentimiento supone emplazar el foco en la responsabilidad del interesado de manifestar

la aceptación del tratamiento y comprender sus implicaciones. En cambio, el interés legítimo deposita sobre el responsable el deber de demostrar que, previo al tratamiento, se lleva a cabo un análisis minucioso, no únicamente sobre los intereses y beneficios propios, sino también sobre aquellos del interesado. Estos, además, deben ser comprendidos por el propio responsable -e igualmente informados al interesado conforme a los arts. 13 y 14 RGPD-. Adicionalmente, el responsable debe ser capaz de medir el riesgo, el posible impacto, la naturaleza de los riesgos y beneficios del tratamiento para los individuos y realizar una ponderación.

5.1.2. *No necesariamente legítimos*

Es destacable que la norma no exige que los intereses, derechos y libertades del interesado sean legítimos. Esto es relevante en la medida en que este resulta un alcance más amplio que aquel concedido a los intereses del responsable o terceros.[331]

Ello explica, por ejemplo, que un interesado puede alegar que la utilización de su imagen obtenida por una cámara de vigilancia en un comportamiento incorrecto no puede utilizarse para despedirlo. En otras palabras, incluso aunque el responsable o un tercero tengan un interés claramente legítimo, su fin no justifica cualquier medio.

Ello no obstante, el balance de intereses debe tomar en consideración, en primer lugar, los efectos del tratamiento sobre el derecho de los interesados a su protección de datos personales y privacidad, que conforme a los art. 7 y 8 de la Carta adquieren la categoría de fundamentales. [332]

---

[331] GRUPO DE TRABAJO DEL ARTÍCULO 29 (2014): *Dictamen 06/2014 sobre el concepto de interés legítimo del responsable del tratamiento de los datos en virtud del artículo 7 de la Directiva 95/46/CE* (WP 217), de 9 de abril.

[332] TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA (2011): Asuntos acumulados C-468/10 y 469/10 ASNEF y FECEMD, de 24 de noviembre. ECLI:EU:C:2011:777, párrafos 38 y 40; TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA (2017): Asunto C-131/12, Google Spain y Google, de 13 de mayo. ECLI:EU:C:2014:317, párrafo 74; TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA (2017): Asunto C-13/16 Rīgas, de 4 de mayo. ECLI:EU:C:2017:336.

5.1.3. *¿Más allá de la protección de datos?*

Asimismo, en relación con la ponderación de intereses, existen un matiz que diferencia la redacción dada por la Directiva y aquella elegida por el RGPD. El art.7.f) de la Directiva 95/46 hacía alusión al interés o los derechos y libertades fundamentales del interesado que requieran protección con arreglo al apartado 1 del artículo 1 de la presente Directiva, es decir, "libertades y de los derechos fundamentales de las personas físicas, y, en particular, del derecho a la intimidad, en lo que respecta al tratamiento de los datos personales". Así, el juicio de ponderación se refería de modo genérico a los derechos y libertades del interesado, tras lo cual concretaba, el derecho a la intimidad y a la protección de datos.

Por su parte, el art. 6.1.f) RGPD menciona "los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales". Es decir, de una lectura de la literalidad de lo dispuesto en el RGPD en relación con lo que preveía la Directiva parecería que el Reglamento acotase el ámbito de protección de los intereses, derechos y libertades fundamentales a aquello que tenga relación directa, o al menos, más directa, con la protección de los datos personales del interesado. Esta interpretación podría no incluir intereses más amplios como la confidencialidad de comunicaciones, comunicaciones de (meta)datos *machine-to-machine*, el honor, la intimidad en un sentido más amplio que la protección de datos personales, la privacidad, la información, la transparencia o el acceso a documentos públicos, entre otros.

A pesar de ello, consideramos que el objetivo del RGPD es la protección del derecho a la protección de datos en armonía y equilibro con otros intereses y derechos e intereses fundamentales.

Así, en orden a garantizar estos intereses, el RGPD debe ser interpretado de manera amplia y en relación con lo dispuesto en el considerando 4 del propio RGPD. En él se indica, por un lado, que el derecho a la protección de los datos personales no es un derecho absoluto, sino que debe considerarse en relación con su función en la sociedad y mantener el

equilibrio con otros derechos fundamentales, con arreglo al principio de proporcionalidad.

Por otro lado, el considerando realiza una afirmación de amplio alcance cuando indica que el RGPD respeta todos los derechos fundamentales, libertades y principios reconocidos en la Carta conforme se consagran en los Tratados. En particular, el Reglamento pretende tomar en consideración "el respeto de la vida privada y familiar, del domicilio y de las comunicaciones, la protección de los datos de carácter personal, la libertad de pensamiento, de conciencia y de religión, la libertad de expresión y de información, la libertad de empresa, el derecho a la tutela judicial efectiva y a un juicio justo, y la diversidad cultural, religiosa y lingüística".[333, 334]

Aunque no mencionado expresamente en esta lista incluida en el RGPD, no debemos olvidar que en la Carta también se reconoce como derecho fundamental aquel de libertad de empresa (art. 16). Es posible argumentar por tanto que los responsables del tratamiento, en ejercicio de este derecho, deban encontrar un punto de equilibro con los interesados en el ejercicio de su derecho a la protección de datos. El reconocimiento de este derecho, supliría, en parte, algunos de los argumentos que reducen la ponderación de intereses a la presunción de que un mero interés económico del responsable no podrá nunca superar un derecho fundamental. De manera proporcional, leal y ponderada, ambos derechos revisten de carácter fundamental y deben ser atendidos.

No solo eso, sino que el derecho a la protección de datos personales debe ponderarse con otros intereses o derechos que, sin ser fundamentales,

[333] Para ampliar en la relación entre el derecho a la protección de datos personales y otros derechos véase AGENCIA DE LOS DERECHOS FUNDAMENTALES DE LA UNIÓN EUROPEA Y CONSEJO DE EUROPA (2019): *Manual de legislación europea en materia de protección de datos*, Ed. 2018, Luxemburgo, p.61 y ss.

[334] El contenido de este considerando también ayuda a poner de manifiesto que, además del derecho a la protección de datos personales, el tratamiento de datos tiene una incidencia innegable en otros muchos derechos. PIÑAR MAÑAS, José Luís (2016), "El objeto del Reglamento", en José Luís Piñar Mañas (dir.), Reglamento General de Protección de Datos: Hacia un nuevo modelo europeo de privacidad, Madrid, Reus, p. 56.

sean legítimos, sean estos de otras personas (esto es, intereses privados) o de la sociedad en su conjunto (es decir, intereses públicos).[335]

En este sentido, resulta interesante lo dispuesto en el considerando 75 del RGPD, que le otorga relevancia a cualquier potencial impacto o consecuencia que recaiga sobre el interesado, entre los que cita riesgos como la discriminación, la elaboración de perfiles o cuando el tratamiento se refiera a cantidades masivas de datos o de interesados.

> "Los riesgos para los derechos y libertades de las personas físicas, de gravedad y probabilidad variables, pueden deberse al tratamiento de datos que pudieran provocar daños y perjuicios físicos, materiales o inmateriales, en particular en los casos en los que el tratamiento pueda dar lugar a problemas de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, reversión no autorizada de la seudonimización o cualquier otro perjuicio económico o social significativo; en los casos en los que se prive a los interesados de sus derechos y libertades o se les impida ejercer el control sobre sus datos personales; en los casos en los que los datos personales tratados revelen el origen étnico o racial, las opiniones políticas, la religión o creencias filosóficas, la militancia en sindicatos y el tratamiento de datos genéticos, datos relativos a la salud o datos sobre la vida sexual, o las condenas e infracciones penales o medidas de seguridad conexas; en los casos en los que se evalúen aspectos personales, en particular el análisis o la predicción de aspectos referidos al rendimiento en el trabajo, situación económica, salud, preferencias o intereses personales, fiabilidad o comportamiento, situación o movimientos, con el fin de crear o utilizar perfiles personales; en los casos en los que se traten datos personales de personas vulnerables, en particular niños; o en

[335] AGENCIA DE LOS DERECHOS FUNDAMENTALES DE LA UNIÓN EUROPEA Y CONSEJO DE EUROPA (2019): *Manual de legislación europea en materia de protección de datos*, Ed. 2018, Luxemburgo, p.42-43.

los casos en los que el tratamiento implique una gran cantidad de datos personales y afecte a un gran número de interesados"(énfasis añadido).

En su jurisprudencia, el TJUE ha reconocido la existencia de un interés en la búsqueda de transparencia,[336] la protección de la propiedad[337] la protección de la salud y la familia, la obtención de información personal de un tercero con el objeto de iniciar un acciones legales contra él (en consonancia con el art. 8.2 Directiva).[338] De hecho, como argumentó el Abogado General en el asunto Rīgas, si el ejercicio de una acción legal puede justificar el tratamiento de categorías especiales de datos, no existe motivo para desechar automáticamente la idea de la existencia de un interés legítimo en el tratamiento de datos de categoría no especial.

El planteamiento anterior trasciende la normativa comunitaria y tiene su reflejo en nuestro orden constitucional interno. De acuerdo con el art. 10 de nuestra Constitución, los derechos fundamentales y las libertades deben ser el fundamento de la paz social. En este sentido, De la Quadra-Salcedo hace hincapié en la necesidad de reconocer una dimensión holística del Derecho, que no limite sus soluciones a la aplicación de cada rama del Derecho a parcelas diferenciadas, sino vistas en su conjunto.[339]

Bajo esta percepción, el derecho a la protección de datos personales sería un elemento más de un grupo más amplio y diversos de derechos y libertades objeto de protección que deben ser observados de manera conjunta, concepción que tiene un perfecto encaje con el ámbito de protección amplio que otorga el RGPD y, más concretamente, la necesidad

[336] TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA (2010): Asuntos acumulados C-92/09 y C-93/09 Volker und Markus Schecke and Eifert, de 9 de noviembre. ECLI:EU:C:2010:662, párrafo 77.

[337] TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA (2014): asunto C-212/13, Ryneš, de 11 de diciembre. ECLI:EU:C:2014:2428, párrafo 34.

[338] TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA (2017): Asunto C-13/16 Rīgas, de 4 de mayo. ECLI:EU:C:2017:336.

[339] DE LA QUADRA-SALCEDO FERNÁNDEZ DEL CASTILLO, Tomás (2018): "Retos, riesgos y oportunidades de la sociedad digital", en Tomás de la Quadra-Salcedo y José Luis Piñar (dirs.), Sociedad digital y Derecho, Madrid, BOE-Red.es, p. 64.

de considerar derechos y libertades en sentido amplio durante la realización de un ejercicio de ponderación. Así, la aplicación de las tecnologías de análisis de datos masivos no debería limitarse cuando el riesgo sobre los derechos y libertades es nimio.[340]

En esencia, parece razonable concluir que los intereses, derechos y libertades del interesado que deben ponderarse al realizar el balance de intereses se refieren a un espectro muy amplio.

5.1.4. *Naturaleza heterogénea*

Tal y como defendía Hondius, la libertad personal y la información son factores que influyen en la consecución de un balance entre el individuo y su contexto social, lo que a su vez es condición necesaria para alcanzar creatividad individual y capacidad de expresión como grupo.[341]

De este modo, los intereses a proteger no deben ser vistos únicamente bajo el prisma del interesado medio en cuanto persona individual, sino de la sociedad en su conjunto. Así, por un lado, la creación de un impacto colectivo positivo que trasciende al propio individuo será un factor a tener en cuenta en la realización del balance de intereses. Por otro lado, la protección intrínseca de la dignidad y la consideración de que esta solo puede desarrollarse en sociedad en la medida en que los datos personales de los ciudadanos sean tratados de manera justa y proporcional deberá también ser un factor de consideración. Es decir, el interés consistente en la garantía de un espacio de desarrollo personal de cada individuo, visto desde un prisma colectivo, genera un interés que resulta ser objeto de protección en sí mismo.

Ello porque, entre otros motivos, precisamente las consecuencias más perjudiciales de los tratamientos nocivos de datos personales son más visibles a gran escala. El impacto colectivo es además superior y de

[340] DE LA QUADRA-SALCEDO FERNÁNDEZ DEL CASTILLO, Tomás (2018): "Retos, riesgos y oportunidades de la sociedad digital", en Tomás de la Quadra-Salcedo y José Luis Piñar (dirs.), Sociedad digital y Derecho, Madrid, BOE-Red.es, p. 64.

[341] HONDIUS, Frits (1975): *Emerging Data Protection in Europe*, North-Holland.

diferente naturaleza a la suma de los impactos negativos individuales que el tratamiento causa sobre cada persona. Ello emplaza al responsable a tomar en consideración los efectos de sus actividades del tratamiento en relación con el entorno y el contexto completo en el que se desarrollan, y no como actividades desconectadas del ambiente o únicamente contextualizadas en un entorno limitado, como un sector de actividad específico o en relación únicamente a los competidores comerciales.

Por último, los intereses, derechos o libertades fundamentales del interesado sobre el interesado pueden verse afectados de manera negativa por el tratamiento pretendido, pero también de manera positiva. Así, como conclusión preliminar, cabe afirmar que un impacto positivo en los intereses del sujeto facilitará la aplicación del art. 6.1.f) como base del tratamiento. Por su parte, el impacto negativo pesará en la ponderación en el sentido contrario al tratamiento, si bien no de modo definitivo. Ciertamente, el proceso de aplicación del interés legítimo ha de verse como un método dinámico y en etapas, en el que cabe la posibilidad de revertir o minimizar el impacto mediante diversos mecanismos, tales como implementar garantías específicas.

6. El ejercicio de ponderación de intereses

El último paso del análisis para concluir si el interés legítimo puede ser el título de legitimación sobre la que se asiente el tratamiento de datos es la ponderación entre los intereses legítimos del responsable o un tercero, por un lado, y los intereses, derechos y libertades fundamentales de los interesados, por otro lado, que, como hemos visto, no tienen por qué ser legítimos.[342]

Es, de hecho, la necesidad de llevar a cabo y documentar la realización de una ponderación de intereses donde reside el potencial del art. 6.1.f) de

[342] En aras de la simplicidad, utilizaremos la referencia genérica a los “intereses” del interesado cuyos datos se encuentran en lid, en lugar de “intereses, derechos y libertades fundamentales”.

aportar un grado cualitativamente superior en la protección de los individuos que otras bases.

6.1. Consideraciones generales

La realización de dicho balance de intereses es el único criterio que aporta el RGPD en relación con la metodología de aplicación del art. 6.1.f) cuando establece que sobre los intereses legítimos del responsable "no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño". Se trata pues de un criterio amplio y ambiguo. A mayor abundamiento, el RGPD no contiene un conjunto de directrices sobre cómo efectuar dicha ponderación.[343]

La ponderación de intereses es clave en la aplicación del interés legítimo y es lo que otorga distintividad a esta disposición respecto de las demás bases de licitud. Es por ello que el TJUE ha establecido en diversas ocasiones que los Estados miembros no puedan prescribir con carácter definitivo el resultado de dicho balance de intereses, pues en todo caso habrá de tenerse en cuenta las circunstancias concretas del caso,[344] sino únicamente especificar situaciones en las que exista una presunción de legitimidad. Este extremo será tratado con detalle más adelante.

Cabe traer a colación la reflexión de Piñar Mañas de que, si bien el espíritu del RGPD es consciente y sensible al valor económico de los datos -lo que puede trasladarse directamente en la concreción de un interés legítimo del responsable-, "en todo caso el derecho fundamental a la protección de datos prevalece sobre el interés económico de los responsables y encargados, como ya ha puesto de manifiesto el Tribunal de Justicia en su

[343] Algunas directrices pueden encontrarse en GRUPO DE TRABAJO DEL ARTÍCULO 29 (2014): *Dictamen 06/2014 sobre el concepto de interés legítimo del responsable del tratamiento de los datos en virtud del artículo 7 de la Directiva 95/46/CE* (WP 217), de 9 de abril, pero es necesaria una mayor concreción.

[344] TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA, (2011): Asuntos acumulados C-468/10 y 469/10 ASNEF y FECEMD, de 24 de noviembre. ECLI:EU:C:2011:777, párrafo 47; TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA (2016): Asunto C-582/14 Patrick Breyer v Germany, de 19 de octubre. ECLI:EU:C:2016:779, párrafo 62.

Sentencia de 13 de mayo de 2014, *Google Spain y Agencia Española de Protección de Datos (AEPD)*, asunto C 131/12".[345]Cierto es que precisamente el ejercicio de realizar un balance de intereses responde al hecho de que el derecho a la protección de datos no es absoluto, sino modulable. Sin embargo, esta consideración no debe servir para menoscabar un derecho individual fundamental.

La falta de desarrollo del precepto hace necesario acudir a fuentes externas el RGPD para encontrar claves sobre cómo realizar la ponderación de intereses. Este ejercicio de ponderación puede ser visto como una "evaluación de impacto ligeramente simplificada" para comprobar que los riesgos para los intereses de las personas son proporcionales,[346] tomando en consideración las circunstancias del caso concreto y el contexto que lo rodea. En parte, es precisamente la necesidad de realizar este análisis que el interés legítimo puede ser, en la práctica, más complejo que cualquiera de las demás bases de legitimación, a pesar de que en un primer momento pudiera parecer la opción más flexible y abierta.

Otro aspecto que destacar del ejercicio de ponderación es que, en principio, será una valoración que realizará inicialmente el responsable del tratamiento. Únicamente en un momento posterior esta decisión podrá ser revisada, por ejemplo, en el caso de que el responsable sea inspeccionado, auditado o sometido a un procedimiento sancionador. Este es, de hecho, uno de los aspectos que más suspicacia puede despertar, por cuanto el responsable actúa como juez y parte en la ponderación.[347]

Por otro lado, a pesar de la falta de orientación del RGPD sobre cómo llevar a cabo la ponderación de intereses, un punto de partida de utilidad podría

---

[345] PIÑAR MAÑAS, José Luís (2016), "El objeto del Reglamento", en José Luís Piñar Mañas (dir.), *Reglamento General de Protección de Datos: Hacia un nuevo modelo europeo de privacidad*, Madrid, Reus, p. 52 y ss.

[346] INFORMATION COMMISSIONER'S OFFICE, *Guidance on legitimate interest*.

[347] Es también lo que, en términos informales, pero más que auto explicativos, Ruth Benito ha explicado de la siguiente manera: "en toda ponderación, suele suceder que, antes o después hay que chuparse el dedo y ponerlo al viento". BENITO, Ruth (2017): "Examen del interés legítimo como base del tratamiento de datos", en *Con la Venia, Señorías*.

ser tomar en consideración el propósito primario (que no único) del RGPD. Dicho propósito primario, es, de hecho, tratar de limitar los posibles abusos sobre el tratamiento de datos personales producidos por actividades automatizadas, las transferencias de cantidades masivas de datos y la posibilidad de obtención de información a partir de todo ello. Es decir, el legislador tenía en mente responsables que cuentan con medios tecnológicos cuya actividad principal estuviera relacionada con el tratamiento de cantidades cada vez mayores de datos de manera continua. Por su parte, aquellas situaciones en las que, por ejemplo, un responsable unipersonal lleva a cabo un tratamiento de datos de una persona específica para una finalidad clara y sencillamente comprensible, podrán requerir una aplicación más liviana de la norma.

6.2. Interés contra interés

La realización de una Evaluación del Interés Legítimo (LIA por sus siglas en inglés) debe tener en cuenta, en particular, la naturaleza de los intereses de ambas partes (como los tipos de intereses y datos, la vulnerabilidad de los interesados), el impacto del tratamiento y las medidas de salvaguarda aplicadas por el responsable del tratamiento.[348] En consecuencia, algunos juristas sostienen que el interés legítimo es la base más apropiada para las prácticas comerciales inocuas estándar.

En este momento, la atención se centra sobre las circunstancias específicas del tratamiento tal y como el responsable es capaz de conocerlas en relación con el interesado medio razonable. Es decir, responsable no está obligado a poder prever los factores que afectan a las circunstancias específicas de cada interesado (que sí pueden ser alegadas y tenidas en cuenta en un momento posterior a través del ejercicio del derecho de oposición). En consecuencia, el responsable tiene el deber de actuar de manera diligente para identificar los intereses del responsable medio y posibles consecuencias previsibles, e incluso puede considerarse

[348] DATA PROTECTION NETWORK, (2018): *Guidance on the use of legitimate interests under the EU General Data Protection Regulation (v.2.0)*.

que sobre el responsable pesa la carga de llevar a cabo una labor de investigación que asegure que no se pasa por alto ningún factor del tratamiento relevante para la ponderación.

Al tratarse de un derecho relativo, el derecho a la protección de datos personales interactúa con otros derechos e intereses y existirán situaciones en las que diferentes derechos entren en conflicto. Sin embargo, esta relación es ambivalente, de modo que el amparo al derecho de protección de datos puede ayudar a garantizar otros derechos o intereses.

Asimismo, al realizar la ponderación de intereses (así como en cualquier otra actividad que requiera datos personales), el responsable del tratamiento debe seguir cumpliendo los principios del RGPD. Esto significa que el responsable debe abstenerse, por ejemplo, de intentar ofrecer un resultado injusto del equilibrio y actuar de forma sesgada para favorecer sus propios intereses. Por consiguiente, incluso si el tratamiento resulta necesario para el responsable, éste no puede proceder automáticamente a llevarlo a cabo. Así, especial relevancia cobra el principio de lealtad (establecido en el art. 5.1.a) RGPD).

6.2.1. *La naturaleza de los intereses*

El primer factor que tomar en cuenta en la ponderación de intereses es la naturaleza de los intereses en juego. Se trata de un concepto amplio que abarca aspectos como los tipos de datos (especialmente el hecho de que puedan ser datos de categoría especial, datos hechos públicos por el interesado o mantenidos totalmente en su esfera íntima),[349] si los intereses añaden un valor a los interesados o la sociedad, y no únicamente al responsable o un tercero a quien se comuniquen los datos, o el origen de los datos (por ejemplo, los datos obtenidos de terceros pueden tener mayores implicaciones para los derechos del interesado que aquellos otros

[349] En este sentido se manifiesta, por ejemplo, la autoridad de Liechtenstein de Protección de Datos.

obtenidos de manera directa por el responsable en su relación con el interesado).

Por su parte, el objetivo de la actividad de tratamiento también podrá determinar el balance de intereses, y así, aquellas prácticas que se inscriban en cuestiones aceptadas socialmente y que gocen de amplio reconocimiento y comprensión tendrán más peso en la ponderación. Por ejemplo, el uso de un conjunto de datos y técnicas con la finalidad de investigación del blanqueo de capitales por parte de una entidad bancaria tendrá mayor legitimación que la utilización de los mismos datos y técnicas con la finalidad de personalizar el precio de un producto o de extracción de nuevo conocimiento mediante inferencias con el objetivo de vender la información.

En relación con la utilización de tecnologías big data, otros factores que definitivamente influirán en la ponderación deben ser el volumen de datos tratados, la capacidad analítica del responsable y la posibilidad de obtener nuevos datos personales o información sobre los sujetos. En definitiva, el uso de la tecnología y sus consecuencias sobre los individuos. En este sentido, será también necesario valorar la capacidad de reidentificación de datos no personales o previamente anonimizados.

6.2.2. *La publicidad de los datos*

Respecto del hecho de que el interesado haya podido hacer públicos ciertos datos, este aspecto es relevante en la sociedad actual, caracterizada por la presencia de los usuarios en redes sociales, donde se comparte contenido personal. La publicación de una información en redes sociales no puede, por sí sola, legitimar el tratamiento de datos personales subsiguiente, menos aún sin una finalidad específica. Sin embargo, la difusión entre lo público y lo privado parece estar contribuyendo a modificar la percepción de los interesados y parece estar tomando un rol en la ponderación de intereses.

En relación con ello, también conviene recordar que, en el ordenamiento jurídico español, los datos personales hechos públicos por el interesado a

través de internet no se incluyen en las consideradas fuentes accesibles al público.[350]

6.2.3. *Expectativa razonable del interesado*

El considerando 47 RGPD menciona las expectativas razonables del interesado como un factor distinguido para la determinación del resultado del balance de intereses, donde la relación entre el responsable del tratamiento y el interesado es relevante.

De acuerdo con esto, el responsable del tratamiento debe evaluar si la persona puede prever de forma plausible que determinados datos se recogerán para los fines previstos en el momento y en el contexto de la recogida. Como ha sido mencionado en trabajos anteriores por Irene Kamara y Paul de Hert,[351] una expectativa razonable tiene una fuerte relación con las circunstancias previas al tratamiento, incluyendo proporcionar información a su debido tiempo al interesado.

Factores de expectativa razonable

Algunos factores que pueden influir en las expectativas razonables del interesado son el tiempo por el que se mantienen los datos, la fuente de los datos, la naturaleza precisa de cualquier relación preexistente entre el individuo y cómo se han tratado sus datos con anterioridad. Por último, el uso de nuevas tecnologías o el tratamiento de datos de formas novedosas que el interesado pueda no haber anticipado.

RELACIÓN ENTRE RESPONSABLE E INTERESADO**.** Por su parte, la relación entre el responsable y el interesado también juega un papel en

[350] A pesar de ello, resulta paradigmático que la redacción del art. 58 bis apartado segundo de la Ley Orgánica de Protección de Datos incluya, sea confusa en el sentido de que parece equiparar las páginas webs a las demás fuentes de acceso público: "[l]os partidos políticos, coaliciones y agrupaciones electorales podrán utilizar datos personales obtenidos en páginas web y otras fuentes de acceso público para la realización de actividades políticas durante el periodo electoral".

[351] KAMARA, Irene; DE HERT, Paul (2018): "Understanding The Balancing Act Behind The Legitimate Interest Of The Controller Ground: A Pragmatic Approach", en Rochester Institute of Technology, New York, Jules Polonetsky, Omer Tene (eds.), *The Cambridge Handbook of Consumer Privacy*, Cambridge University Press, pp. 321-352.

determinar si el individuo podría razonablemente esperar el tratamiento. El considerando 47 indica que es más probable que el interés legítimo pueda ser la base del tratamiento cuando el responsable tiene una "relación pertinente y apropiada", por ejemplo, como cuando el interesado es un cliente o empleado. Si el responsable no tiene una relación preexistente, es más difícil que un interesado pueda esperar que sus datos sean tratados.

Por ejemplo, un cliente de un restaurante de comida a domicilio podría esperar que el restaurante conservara su nombre y dirección para futuras entregas de pedidos. Los datos de clientes pueden conservarse en la base de datos en virtud del interés legítimo del propietario del restaurante de guardar los datos correctos y actualizados de sus clientes con el objetivo de automatizar el proceso de entrega para que la persona que realiza el reparto sepa dónde dirigirse, eliminando así posibles errores resultantes de preguntar la dirección en cada orden de compra. Para esta finalidad, es necesario guardar la información en el sistema y no existe una forma alternativa fácil y menos intrusiva de proceder. Por último, los datos tratados no son de carácter sensible, el cliente puede esperar de forma razonable que su dirección pueda ser guardada, y no se deriva ningún impacto negativo relevante de ello. Por lo tanto, el art. 6.1.f) del RGPD constituye un fundamento jurídico idóneo para este tratamiento.

En cambio, si el responsable obtiene los datos de un tercero, debe tener la confianza de que el interesado fue informado sobre la posibilidad de transmitir sus datos para su uso por terceros, es decir, que la cesión de datos está legitimada para la finalidad del tratamiento. A pesar de ello, el uso de datos provenientes de terceros, especialmente cuando se trata de múltiples partes, así como la cesión de datos a terceros, debe ser un extremo del tratamiento de datos restringido. En este sentido, el responsable que compre datos de terceros debe, en primer lugar, analizar conforme al principio de minimización de datos la necesidad real de tratar datos personales en lugar de anonimizados.

INTERESADO MEDIO RAZONABLE. El ejercicio de ponderación de intereses, y con ello el análisis de las expectativas razonables del interesado debe tener pretensión de ser objetivable. En otras palabras, debe referirse a los intereses y expectativas del interesado medio razonable al que se dirija el tratamiento y bajo las circunstancias del tratamiento. Por el contrario, el responsable no tiene obligación -ni capacidad- de ponderar las circunstancias de una persona en particular o sus expectativas.

Si el tratamiento de datos tiene como interesado un grupo específico de población de características singulares, el responsable deberá tomar en consideración tales características en la definición del interesado medio razonable para dicho tratamiento. Quizás el ejemplo más claro de ello sean los niños, pero desde luego, también se pueden pensar otros casos. Así por ejemplo, un producto o servicio que conlleve un tratamiento de datos personales y dirigido a personas "mayores" -entendido en sentido amplio, no necesariamente referido a personas de tercera edad- que no se han desarrollado en entornos tecnológicos rápidamente cambiantes y que, a pesar de gozar de plena capacidad y entendimiento, no puede presuponérseles una capacidad elevada de conocimiento sobre los procesos de tratamientos de datos personales ni sus consecuencias.[352]

TRANSPARENCIA**.** Otro de los factores que también deberá ser considerado en la balanza y que podrá influir sobre las expectativas razonables de los interesados en determinados casos, así como en su capacidad posterior de ejercer sus derechos, es la transparencia. Ello es porque los interesados podrán razonablemente esperar un tratamiento de datos si este les ha sido avisado.

Se trata de un criterio generalmente ligado a la capacidad de control de los individuos sobre la utilización de los datos personales que se refieran a ellos. De este modo, aportar información conforme al principio de

[352] De hecho, junto con el reconocimiento de la especial importancia de los derechos del menor en al art. 24 de la Carta de Derechos Fundamentales, la Carta también reconoce expresamente en su art. 25 el derecho de las personas mayores a participar en la vida social y cultural.

transparencia, desde la Fase 1, en el momento de la recogida de los datos, será un factor favorable al tratamiento durante la realización del balance de intereses. En consecuencia, la forma en que se aporte dicha información, así como el modo y la facilidad para ejercer los derechos por parte del interesado podrán influir en sus expectativas razonables.

La expectativa razonable no es un factor determinante

A pesar de todo lo anterior, aunque las expectativas razonables son un factor importante, no determinan automáticamente el resultado del balance de intereses. El mero hecho de haber advertido previamente a la persona que sus datos serán tratados de cierta manera no significa necesariamente que los intereses legítimos del responsable prevalezcan, independientemente del potencial perjuicio para el interesado. Tal afirmación equivaldría a poner, de nuevo, la carga sobre el interesado de modo tal que una expectativa razonable de tratamiento, que podría ser no deseada, podría llegar a justificar la licitud del tratamiento.

Asimismo, en algunos casos, será posible para el responsable justificar un tratamiento de datos inesperado si tiene una razón convincente para ello. Esta aproximación goza de toda lógica en tanto el avance de la técnica dificulta que el interesado se mantenga actualizado y pueda razonablemente esperar determinados tratamientos que, por ejemplo, puedan generar un impacto positivo sobre estos o superar la ponderación de intereses.

Limitaciones de la expectativa razonable como factor en el ejercicio de ponderación

Existen algunas limitaciones relacionadas con las expectativas razonables del interesado medio cuando las actividades de tratamiento utilizan nuevas tecnologías, procesos complejos y cambiantes. En primer lugar, no siempre queda claro en qué sentido influye la transparencia en relación con procesos tecnológicamente complejos. ¿Sería posible deducir que el interesado puede razonablemente esperar un tratamiento por el hecho de que le ha sido presentada determinada información, siendo ampliamente

aceptado que en muchas ocasiones no la comprenderá? O por el contrario ¿será que en escenarios de uso de herramientas de análisis masivo de datos dicha expectativa se nubla debido a la impredecibilidad del proceso, a pesar de los esfuerzos del responsable por respetar aportar garantías a los interesados?

Por otro lado, la expectativa razonable del interesado es un factor dinámico que puede modificarse con el paso del tiempo. Bien es cierto que tomar en consideración los cambios en la percepción del uso y tratamiento de datos personales es positivo. No obstante, otorgar un énfasis excesivo en las expectativas del interesado podría llegar a facilitar la realización de un balance de intereses para tratamientos de datos invasivos por el solo hecho de que los ciudadanos puedan llegar a acostumbrarse a un estado de tratamiento intensivo de los datos que se generan en actividades.[353] Por ejemplo, en la actualidad, cualquier usuario medio de un sitio web o una aplicación móvil tiene una expectativa de que sus datos serán tratados. ¿Hace ello que el responsable pueda utilizar este hecho de manera favorable a sus intereses en la ponderación?

Es lo que podríamos bautizar como la paradoja de las expectativas. Si el interesado medio razonable se hace cada vez más consciente de la existencia de prácticas ubicuas de recolección y análisis de datos, e incluso de vigilancia, pueden llegar a asumir que es razonablemente esperado que un nivel tan intenso de monitorización continúe existiendo. De este modo, prácticas que se sitúan en áreas grises de la norma, que de otro modo no contarían con el factor de la expectativa razonable, y que podrían incluso llegar a considerarse no lícitas por ser inesperadas, llegarían a poder legitimarse por el solo hecho de continuar existiendo. Por su parte, la existencia de estas prácticas se consolida por el hecho de que las prácticas empresariales evolucionan a un ritmo más veloz que los pronunciamientos de las autoridades de control o, en última instancia, los tribunales. Es decir,

[353] Bien es cierto que en dichos casos resultará útil el hecho de que el RGPD aporta como instrumento adicional de control la obligación de cumplir con los principios del tratamiento como la licitud, lealtad o transparencia.

el sistema jurídico puede no ser capaz de actuar a la velocidad suficiente para paralizar ciertas prácticas sectoriales que hacen uso de técnicas y tecnologías de tratamientos de datos antes de que estas hayan evolucionado y cristalizado hasta crear una expectativa sobre las personas. Como consecuencia, el mero paso del tiempo podría hacer que ciertas prácticas, con independencia de su naturaleza o consecuencias, fueran más esperadas y por tanto propensas a superar la ponderación de intereses.

De este modo, la utilización de este factor, pensado originariamente como elemento de contrapeso, se convierte de repente en un nuevo elemento de peso en el lado de la balanza que ocupan los intereses del responsable.

De hecho, sería sencillo imaginarse que una cada vez mayor penetración de técnicas y tecnologías de recogida y análisis de datos, así como de toma de decisiones, podría hacer cambiar las expectativas razonables de los interesados a lo largo del tiempo, en el sentido de hacer más predecible un análisis intenso de los datos.

De este modo, aunque la expectativa razonable del interesado medio deba ser un factor adicional que tomar en consideración en el balance de intereses, podría argumentarse que no debería ser el factor más relevante, hasta el punto de ser prácticamente la única directriz que menciona el RGPD, aunque sea en sus considerandos. Serviría mejor al espíritu del RGPD y a su objeto de protección la concreción de un factor de ponderación más objetivable.

6.2.4. *Impacto sobre el interesado y medidas de seguridad ¿Una alternativa a la expectativa razonable?*

Por todo lo anterior, el impacto del tratamiento sobre los intereses, derechos y libertades fundamentales del interesado puede tornarse como un factor de ponderación más afinado. Bajo esta aproximación, el posible impacto que el tratamiento de los datos personales pueda tener sobre los interesados sería uno de los criterios que con más fuerza determinarían el sentido de la balanza, por encima incluso de la expectativa del interesado

o su relación con el responsable. Esto es, las consecuencias que se puedan derivar de un uso informatizado de la información sobre la vida real del individuo, tanto impactos positivos como riesgos derivados de ello y su probabilidad de materialización.

El RGPD no señala expresamente el impacto como factor de especial relevancia en la evaluación del interés legítimo, aunque es posible entrever que sí se trata de un elemento al que el legislador ha otorgado importancia a lo largo de todo el texto de la norma. De hecho, la consideración del impacto como factor del interés legítimo está ligada a la aproximación basada en riesgos del RGPD. Por otro lado, opiniones como la de la autoridad de control irlandesa hacen mención al impacto sobre el individuo como un componente del balance de intereses.[354]

Por su parte, el GT29 ya dejaba ver que el impacto podría ser un elemento de importancia en el ejercicio de ponderación cuando establecía que "al interpretar el alcance del artículo 7, letra f), se aspira a un enfoque equilibrado que garantice la flexibilidad necesaria a los responsables del tratamiento de datos en situaciones en las que no exista un impacto indebido sobre los interesados, mientras que, al mismo tiempo, estos disfruten de una seguridad jurídica y unas garantías suficientes".[355]

Los responsables del tratamiento están acostumbrados a analizar los riesgos que una operación tiene sobre el propio responsable, ya sean estos riesgos financieros, reputacionales, ambientales, de fraude, etc. Sin embargo, la práctica de analizar subsiguientemente los riesgos de una operación para el interesado medio es una práctica menos común.

Por ello, si bien la consideración del impacto de manera preferente a la expectativa del interesado puede ayudar a resolver ciertas limitaciones, la determinación y ponderación de tal impacto no es una tarea sencilla.

---

[354] DATA PROTECTION COMMISSION, (2019): *Guidance Note: Legal Bases for Processing Personal Data*, p. 24.

[355] GRUPO DE TRABAJO DEL ARTÍCULO 29 (2014): *Dictamen 06/2014 sobre el concepto de interés legítimo del responsable del tratamiento de los datos en virtud del artículo 7 de la Directiva 95/46/CE* (WP 217), de 9 de abril, p. 12.

MEDIDAS DE SEGURIDAD. En este punto también son muy relevantes las medidas de seguridad jurídico-organizativas que el responsable implemente con el objetivo de reducir el posible riesgo remanente que el tratamiento de datos implique para los sujetos. De hecho, estas medidas de seguridad pueden ser determinantes para impulsar la balanza en uno u otro sentido en la medida en que garanticen que los intereses de la organización no supondrán un riesgo desproporcionado para los individuos.

Estas medidas pueden consistir, entre otras,[356] en la minimización de datos, seudonimización, anonimización,[357] aumentar los niveles de transparencia, estándares de privacidad desde el diseño y por defecto,[358] métodos de

[356] DATA PROTECTION NETWORK (2018): *Guidance on the use of legitimate interests under the EU General Data Protection Regulation (v.2.0)*, p. 6.

[357] Seudonimizar datos consiste en reemplazar los atributos que permiten identificar a la persona por un "seudónimo", y mantener ambos datos, el personal y su seudónimo, separados con medidas técnicas y organizativas. AGENCIA DE LOS DERECHOS FUNDAMENTALES DE LA UNIÓN EUROPEA Y CONSEJO DE EUROPA (2019): *Manual de legislación europea en materia de protección de datos*, Ed. 2018, Luxemburgo, p.132.

Este proceso no debe confundirse con la anonimización, que implica romper todas las relaciones que identifiquen a la persona. Así, el responsable que utiliza el dato seudónimo mantiene, por lo general, capacidad para saber a qué persona se refieren los datos, pues se conservan los datos adicionales que permiten la identificación. Sin embargo, el usuario de la información dentro de la organización -por ejemplo, un empleado de un determinado departamento que accede a los datos, los analiza y realiza actividades de tratamiento- no tiene acceso a los datos directamente identificativos. Por ello, el dato seudónimo otorga una mayor garantía de seguridad que el uso de datos directamente identificables, a pesar de que ambos tipos de datos sigan siendo personales.

Este tipo de datos se utilizan en muchos contextos con el objetivo de proteger la identidad de la persona frente a usuarios no autorizados, pero manteniendo, al mismo tiempo, la certeza de que los datos pertenecen a la misma persona. Así por ejemplo, la seudonimización se utiliza ampliamente en estudios médicos en los que se observa la evolución de una enfermedad a lo largo del tiempo. El investigador debe tener la certeza de que los datos de cada visualización pertenecen a la misma persona para ser capaz de analizar la evolución de cada constante, aunque no necesita conocer quién es la persona a la que se refiere el conjunto de datos. Únicamente el hospital donde se realizan las visitas conoce la identidad del paciente, que después enmascara para obtener historiales seudoanonimizados.

La seudoanonimización es así una medida de incrementar la seguridad. En efecto, el art. 25 RGPD, sobre protección de datos desde el diseño, menciona la seudoanonimización como ejemplo de medida técnica y organizacional para salvaguardar los principios de protección de datos.

[358] Resulta muy interesante encontrar en la doctrina española una referencia a lo que parecía ser la idea temprana sobre la que posteriormente se construyó el concepto de protección de datos desde el diseño. Ya en 2007, Murillo de la Cueva reflexionaba sobre la importancia de adoptar medidas que garantizasen que los equipos terminales estén "fabricados de manera compatible con el derecho de los usuarios de proteger y controlar el uso de sus datos personales". MURILLO DE LA CUEVA, Pablo Lucas (2007):

autenticación por factores múltiples unido a la estricta concesión de derechos de acceso para reducir a lo rigurosamente necesario quiénes pueden acceder a la información dentro de la organización. Asimismo, la reducción de los plazos de conservación de datos, el cifrado o cualquier otra medida técnica u organizativa. Estas medidas deben referirse, no solo a las bases de datos utilizadas de manera cotidiana por el responsable, sino también, por ejemplo, a las copias de seguridad, que susceptibles de sufrir brechas de seguridad.

Del mismo modo, otras medidas pueden incluir la reducción de las finalidades del tratamiento, la utilización de medios técnicos lo menos intrusivos posibles para la finalidad, así como la concesión de medios sencillos y directos para que los interesados puedan oponerse al tratamiento en el momento de la recogida, de modo que dicho tratamiento no llegue a tener lugar con sus datos personales. Igualmente, especialmente útiles pueden ser las medidas orientadas a limitar el uso de los datos personales o el nuevo conocimiento que de ellos pueda obtenerse durante la Fase 2, cuando son sometidos a procesos de combinación de bases de datos, análisis y descubrimiento de patrones. Ello es debido a que, en la medida en que se restrinja la posibilidad de que los datos puedan ser utilizados para la toma de decisiones (esto es, Fase 3), el potencial impacto del tratamiento sobre los interesados se minimiza al tiempo que se mantiene la capacidad de innovación del responsable y de experimentación durante la Fase 2.

El tipo de medidas, la naturaleza o su robustez dependerán del caso concreto. Sin embargo, el establecimiento de medidas de seguridad de acuerdo con el estado del arte[359] es especialmente importante cuando se lleven a cabo tratamientos de carácter sensible o de mayor impacto potencial, por ejemplo, cuando se utilicen tecnologías big data para el

"Perspectivas del derecho a la autodeterminación informativa" en *Revista de Internet, Derecho y Política*, No. 5

[359] Más detalles sobre el estado del arte en materia de protección de datos desde el diseño en el Seminario de IPEN 2019 (Internet Privacy Engineering Network).

tratamiento de datos a gran escala con la finalidad de análisis y descubrir patrones e inferencias basados en interés legítimo.

La determinación de las medidas de seguridad que deben recaer sobre el tratamiento es también un proceso dinámico. Así, el responsable podrá prever unas determinadas medidas y, a pesar de ello, concluir que el resultado del balance de intereses aquellos de los interesados prevalecen. Un motivo de ello podría ser que, a pesar de las medidas establecidas, el riesgo potencial y el impacto negativo del tratamiento sobre los interesados es aun suficientemente elevado como para no justificar el tratamiento. Ante esta situación, el responsable puede implementar medidas de seguridad adicionales en orden a minimizar el impacto, lo que, eventualmente, puede llegar a virar la balanza en favor del responsable.

El objetivo final de estas medidas de salvaguarda es, por lo tanto, limitar el impacto del tratamiento sobre los interesados, fomentando prácticas lo más inocuas posibles. Asimismo, el hecho de que los intereses legítimos del responsable del tratamiento o de un tercero prevalezcan sobre aquellos del interesado, incluso desde un primer momento, no implica la liquidación las garantías y medidas de seguridad del tratamiento,[360] por lo que, aunque la ponderación de intereses concluya a favor del tratamiento, siempre deben adoptarse medidas paliativas.

6.2.5. *Tratamientos para fines secundarios como la realización de perfiles*

Como destaca el considerando 47, también es de gran importancia el tratamiento posterior de los datos con fines secundarios distintos de los que motivaron la recogida de los datos, por ejemplo, para llevar a cabo actividades de análisis y descubrimiento de nueva información o para la elaboración de perfiles. En esta línea, el concepto de finalidades no

[360] KAMARA, Irene; DE HERT, Paul (2018): "Understanding The Balancing Act Behind The Legitimate Interest Of The Controller Ground: A Pragmatic Approach", en Rochester Institute of Technology, New York, Jules Polonetsky, Omer Tene (eds.), *The Cambridge Handbook of Consumer Privacy*, Cambridge University Press, pp. 321-352.

incompatibles es crucial, junto con los principios de transparencia y limitación de la finalidad.

En concreto, el principio de limitación de la finalidad (art. 5.1.b) RGPD) establece que los datos no deben ser tratados posteriormente de forma incompatible con las finalidades iniciales especificadas, explícitas y legítimas. Para ello, el tratamiento posterior con fines de archivo de interés público, de investigación científica o histórica o con fines estadísticos no se considerará incompatible con los fines iniciales y, por lo tanto, no necesitará una nueva base jurídica para el tratamiento. Un análisis profundo del concepto de limitación de la finalidad está fuera del alcance de este trabajo. Baste decir que, para determinar la compatibilidad de los fines originales y secundarios de los datos, el RGPD orienta al responsable del tratamiento para que tenga en cuenta factores tales como la relación entre los fines, el contexto en el que se recogieron los datos, las expectativas razonables del interesado, la naturaleza de los datos y la existencia de salvaguardias (considerando 50). Estos factores recuerdan algunos de los utilizados en la ponderación de intereses para la evaluación del interés legítimo.

A ello se añade la obligación del responsable de especificar cuáles son las finalidades del tratamiento y su interés legítimo en el momento de la recogida de los datos (esto es, al inicio de la Fase 1) o en todo caso antes del inicio del tratamiento, de modo que la reutilización de datos personales para finalidades no previstas en un primer momento puede encontrar dificultades. Para ello, el proceso de anonimización, cuando sea posible, resulta de gran utilidad.

Asimismo, la diferenciación de las finalidades y las diversas fases del ciclo de vida de los datos es relevante. En efecto, en el momento de la recogida de los datos (Fase 1), el responsable puede prever y por tanto informar de manera transparente y específica sobre la finalidad de análisis de los datos (Fase 2), por ejemplo, para la búsqueda de patrones que permitan elaborar relaciones entre variables y crear modelos de perfilado, que, recordemos, en esta fase no son aplicados sobre personas concretas. Más complejo

será, no obstante, que el responsable se encuentre en posición de informar modo completo sobre las posibles finalidades que puedan idearse para la Fase 3, consistentes en la aplicación del conocimiento de la Fase 2 para la toma de decisiones, como por ejemplo, la realización de perfiles de personas concretas y la realización de inferencias de información personal.

Recomendaciones del Consejo de Europa pre-RGPD

El análisis de datos permite conocer la personalidad de un individuo, o al menos, la proyección de dicha personalidad en el mundo digital y ello ha sido objeto de análisis desde hace años. Antes de la creación del RGPD, durante la vigencia de la antigua Directiva 95/46, el Consejo de Europa publicó recomendaciones sobre el tratamiento de datos automatizados o con finalidades de elaboración de perfiles.[361] En dichas recomendaciones, el Consejo reconoce, por un lado, la posibilidad de que la elaboración de perfiles pueda basarse en el consentimiento, le ejecución de un contrato, un interés público, vital o un interés legítimo del responsable o un tercero. Sin embargo, a renglón seguido el Consejo a se refiere específicamente a aquellas personas que, por su condición, no puedan expresar su consentimiento libremente, tales como personas incapaces o niños, respecto de los cuales indica que, en principio, las actividades de perfilado deben estar prohibidas debido al posible peligro de manipulación o discriminación. Esta aproximación parece considerar el consentimiento como un modo más seguro o garantista de tratamiento de datos frente a otras opciones como el interés legítimo de modo que, ante la imposibilidad de manifestar un consentimiento, el tratamiento no puede llevarse a cabo. Dicha prohibición, destacaba el documento, podría ser levantada en dos circunstancias por los Estados miembros: cuando existiese un "interés general superior" y así lo estableciese una ley con las garantías adecuadas

[361] CONSEJO DE EUROPA, COMITÉ DE MINISTROS (2010): *Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling (Profiling Recommendation)*, de 23 de noviembre, p. 10 y 46.

o cuando el tratamiento tuviera como objetivo proteger el interés legítimo del interesado, ya fuese para beneficiarle o protegerle frente a un peligro.

Esta afirmación sorprende por varios motivos. En primer lugar, parece haber una contradicción entre el reconocimiento de que la elaboración de perfiles puede llevarse a cabo bajo diversas bases jurídicas y la apariencia de que, en realidad, el consentimiento es la única base deseable, de modo que la imposibilidad de manifestar un consentimiento libre debe conlleva la prohibición del tratamiento. En segundo lugar, el levantamiento de la prohibición puede responder a dos causas, ninguna de las cuales se corresponden con una base de licitud. La primera de ellas, el interés general superior, recuerda a una suerte de interés público que parece requerir ser reforzado, aunque si tal era la intención del órgano, no se comprende bien el cambio de terminología. La segunda causa del levantamiento de la prohibición es la protección del interés legítimo del interesado, que en realidad no se trata de la aplicación de la base jurídica del interés legítimo, pensada para preservar el interés del responsable o un tercero.

De hecho, la recomendación de prohibición del tratamiento cuando el interesado sea una persona incapaz parece indicar que, en todo caso y sin tener en cuenta las circunstancias del caso, la condición de incapaz o niño de una persona conlleva irreflexivamente la no superación de un hipotético balance de intereses. Es decir, se establecería una presunción que no admite prueba en contrario de que el solo hecho de que el interesado sea un niño o una persona incapaz vicia el interés legítimo como base del tratamiento. Todo ello, aunque el tratamiento pudiera ser no lesivo para el sujeto y por tanto, evitando reconocer que el ordenamiento jurídico también desea proteger el interés del responsable o de un tercero en una situación de equilibro de intereses.

A pesar de todo, no puede negarse que la condición de incapaz o niño del interesado deberá tenerse en cuenta sea cual sea la base jurídica del tratamiento, y así ha quedado expresamente reconocido con posterioridad

a este informe, tanto respecto del consentimiento (art. 8 RGPD), como del interés legítimo (art. 6.1.f) RGPD) y por la jurisprudencia (véase TJUE, caso Rīgas). Sin embargo, tanto la Directiva como el RGPD y el TJUE han manifestado, con posterioridad a dicho informe, que la condición de niño -a la que se podría asimilar la de incapaz- de una persona no puede determinar por sí solo el resultado de la ponderación de intereses.

Directrices del Comité Europeo de Protección de Datos post-RGPD

Por su parte, el sucesor del GT29, el CEPD, parece tener una perspectiva más abierta sobre el interés legítimo, pues ha reconocido que las actividades de tratamiento consistentes en el perfilado de interesados individuales (Fase 3) pueden basarse en el art. 6.1.f) RGPD siempre que no se base en un tratamiento que sea únicamente automatizado y que tenga efectos significativos o legales (en otras palabras, actividades de elaboración de perfiles que no estén comprendidas en el ámbito de aplicación del art. 22 RGPD).[362]

En aquellos casos donde el RGPD lo permita, algunos de los factores a considerar en la ponderación de intereses requerido para aplicar el interés legítimo son el nivel de detalle del perfil (es decir, desde los más generales hasta aquellos más detallados), la exhaustividad del perfil (esto es, si permite describir un aspecto concreto de la persona o múltiples aspectos de modo que puede crearse una imagen más completa del interesado), los efectos sobre los interesados (con especial atención al impacto negativo), así como las medidas de salvaguarda (por ejemplo, para evitar la discriminación, la imparcialidad o la exactitud).[363]

Si bien siempre será necesario analizar el caso concreto antes de poder llegar a una conclusión, sí es posible establecer parámetros generales. En

[362] GRUPO DE TRABAJO DEL ARTÍCULO 29, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679* (WP 251 rev.01), de 6 de febrero. Adoptadas por el Comité Europeo de Protección de Datos.

[363] GRUPO DE TRABAJO DEL ARTÍCULO 29, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679* (WP 251 rev.01), de 6 de febrero. Adoptadas por el Comité Europeo de Protección de Datos.

esta línea, el documento asegura, que aquellas actividades que, por sus características, conlleven prácticas muy intrusivas de tratamiento, como, por ejemplo, el seguimiento a través de múltiples sitios web, dispositivos, localizaciones o mediación de datos con finalidades de marketing, serán difícilmente lícitas bajo el interés legítimo.[364]

Por su parte, la versión actualizada del Convenio 108 también reconoce la posibilidad de acudir al interés legítimo como base para el tratamiento de datos en el contexto de actividades de perfilado.

Discrepancias en la doctrina y autoridades de control

El estudio de esta cuestión por parte de la doctrina, así como las opiniones de las autoridades de control reflejan diferentes opiniones. Por ejemplo, Frederik Z. Borgesius argumenta en contra de la posibilidad de basar en el interés legítimo actividades de seguimiento -que conllevan perfilado de los usuarios en la Fase 3- para finalidades de personalización de publicidad.[365] En una línea similar, Irene Kamara y Paul de Hert muestran reticencias, de modo más genérico, para la utilización de tecnologías big data con finalidades de perfilado, a pesar de reconocer las limitaciones de otras bases como el consentimiento en entornos big data.[366]

Por el contrario, otra parte de la doctrina académica defiende la utilidad de aplicar el interés legítimo a actividades de tratamiento que conlleven el uso de nuevas tecnologías como big data o el Internet de las Cosas como medio de aportar mayores garantías. En un interesante estudio, las autoras Lokke Moerel y Corien Prins proponen aplicar la evaluación que sirve de base para la aplicación del interés legítimo en relación con el tratamiento de

[364] GRUPO DE TRABAJO DEL ARTÍCULO 29, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679* (WP 251 rev.01), de 6 de febrero. Adoptadas por el Comité Europeo de Protección de Datos.

[365] ZUIDERVEEN BORGESIUS, Frederik J. (2015): "Personal Data Processing for Behavioural Targeting: Which Legal Basis?", en *International Data Privacy Law*, Vol. 5, No 3, pp. 163-176.

[366] KAMARA, Irene; DE HERT, Paul (2018): "Understanding The Balancing Act Behind The Legitimate Interest Of The Controller Ground: A Pragmatic Approach", en Rochester Institute of Technology, New York, Jules Polonetsky, Omer Tene (eds.), *The Cambridge Handbook of Consumer Privacy*, Cambridge University Press, pp. 321-352.

datos personales incluso para finalidades secundarias incompatibles -entre las que cabría incluir aquella de elaboración de perfiles- abandonando la aplicación del principio de limitación de la finalidad como criterio independiente de la normativa de protección de datos.[367] Asimismo, las autoras reniegan de la utilidad de que el consentimiento o la necesidad para la ejecución de un contrato deban seguir siendo consideradas bases de licitud del tratamiento. En cambio, estos principios pueden ser sustituidos por una evaluación previa que determine si el responsable ostenta un interés legítimo en la recogida de datos y su tratamiento.

Entre las autoridades de control también pueden surgir diferentes aproximaciones, aunque con carácter general estas destacan la posibilidad de poder recurrir al interés legítimo como base del tratamiento para la realización de perfiles. El ICO inglés ha manifestado que la base jurídica del interés legítimo puede ser aplicada a cualquier tipo de tratamiento para cualquier finalidad razonable y menciona la elaboración de perfiles entre los intereses legítimo de un responsable.[368] Asimismo, en la décima sesión abierta de la AEPD española se indicaba que el perfilado puede, en principio, llevarse a cabo bajo cualquier base jurídica en la medida en que la base elegida en cada caso sea adecuada y cumpla con todos los requisitos del RGPD. En el caso concreto del interés legítimo, la autoridad señalaba la importancia de una ponderación de intereses correcta.

En resumen, puede observarse como el interés legítimo es una base de licitud que se encuentra en el centro deun debate intenso en el que no parece existir un gran consenso. A pesar de ello, parece que el paso del tiempo está jugando en favor de este título de licitud, en la medida en que las algunas autoridades de control van manifestando posturas más abiertas hacia la idea de basar en un interés legítimo actividades de perfilado.

---

[367] MOEREL, Lokke; PRINS, Corien (2016): “Privacy for the homo digitalis: Proposal for a new regulatory framework for data protection in the light of Big Data and the internet of things”, en *SSRN Electronic Journal*, 2784123: 1-98.

[368] INFORMATION COMMISSIONER’S OFFICE, *Guidance on legitimate interest*.

6.3. Resolviendo la ecuación

En esencia, en la ponderación de intereses entran en juego, por un lado, los intereses legítimos del responsable, que en numerosas ocasiones se podrán resumir en la esperanza de obtener un beneficio como conocer mejor a los clientes, ser más eficiente en la asignación de recursos o tener mayores ventas; y por otro lado, los intereses, derechos y libertades fundamentales de los sujetos, que en numerosas ocasiones se resumirán en un posible riesgo o la limitación de algún modo de la protección de su esfera más íntima y personal, que, recordemos, está configurada como un derecho fundamental de la persona en la Unión Europea.

6.3.1. *Posibles sesgos*

Una vez tomados en cuenta todos los factores, el responsable debe otorgarles un valor y determinar qué lado de la balanza pesa más. Sin embargo, el proceso no es directo y en todo caso conllevará un grado de parcialidad por parte del propio responsable.

En lo que se refiere a la evaluación de impactos negativos o riesgos, ya existen diversas metodologías para enumerarlos, evaluar su gravedad, la posibilidad de que ocurran y planificar acciones para abordarlos. Deberá prestarse atención al hecho de que el responsable no minimice la magnitud real de aquellos riesgos con la pretensión de distorsionar el balance de intereses. Por su parte, la evaluación del impacto positivo resulta también compleja debido a la subjetividad del análisis y a la naturaleza del impacto en los derechos y libertades de las personas.[369]

Este es quizás el factor por el que el interés legítimo recibe sus mayores críticas, en el sentido de que esta subjetividad pudiera ser utilizada por el responsable para proceder a legitimar falazmente un tratamiento aun cuando los intereses, derechos y libertades fundamentales de los

[369] KAMARA, Irene; DE HERT, Paul (2018): “Understanding The Balancing Act Behind The Legitimate Interest Of The Controller Ground: A Pragmatic Approach”, en Rochester Institute of Technology, New York, Jules Polonetsky, Omer Tene (eds.), *The Cambridge Handbook of Consumer Privacy*, Cambridge University Press, pp. 321-352.

interesados debieran pesar más que los intereses legítimos del responsable. Es decir, en la medida en que el responsable actúa como juez y parte en el juicio de ponderación, existen incentivos para actuar en beneficio propio de manera desleal.

No obstante, el deber de documentar le evaluación de todos los requisitos del interés legítimo del responsable debe permitir determinar cuál fue el camino argumentativo por el que este concluyó que el interés legítimo sería la base de legitimación más apropiada, y por tanto, auditable en cualquier momento posterior. De este modo, el responsable tiene también incentivos para situarse en una posición lo más objetiva posible y llegar a una conclusión del juicio de ponderación acorde con los principios y obligaciones del Reglamento, y muy especialmente el principio de responsabilidad proactiva y de transparencia.

Es de hecho, la obligación de realizar una ponderación de intereses y documentarlo lo que aporta un mayor grado de garantía al interesado respecto de utilizar una base de legitimación alternativa como el consentimiento. Como ya fue detallado en el capítulo anterior, la petición de consentimiento se inicia presentando al usuario una solicitud que en muchas ocasiones no lee o comprende, en la que se le pide autorización para llevar a cabo un tratamiento que pudiera ser abusivo o impactar sobre sus intereses, derechos y libertades. Por el contrario, el interés legítimo requiere una cuidad atención a los intereses, derechos y libertades de los interesados sin necesidad de abrumar al usuario con todo tipo de decisiones complejas y constantes.

6.3.2. *Dónde se encuentra el equilibrio*

La redacción de RGPD (y antes que este, de la Directiva) establece que el interés legítimo será una base de licitud apropiada cuando sobre los intereses del responsable o un tercero “no prevalezcan los intereses o los derechos y libertades fundamentales del interesado”. Es decir, el legislador opta por una redacción en negativo, según la cual no se exige que el interés del responsable prevalezca sobre aquellos del interesado, sino que no sea

prevalecido por ellos. Esto plantea algunas cuestiones. ¿Es necesario que los intereses, derechos y libertades fundamentales del interesado predominen en todo caso? ¿Es suficiente con que los intereses del responsable o un tercero tengan un peso equivalente a los intereses, derechos y libertades fundamentales del interesado? ¿Quiere esto decir que el impacto sobre los interesados deba ser nulo, o existe un margen de apreciación razonable? ¿Es posible realizar un segundo ejercicio de ponderación si el resultado primero se torna en favor del interesado?

Quizás la cuestión más relevante para decidir sobre la validez del interés legítimo como base del tratamiento de datos personales sea cuál debe ser el resultado del ejercicio de ponderación que debe realizarse para considerar que se ha alcanzado un equilibro que permita utilizar el art. 6.1.f). El RGPD no exige que el impacto sobre el interesado sea nulo o inexistente, sino que admite la posibilidad de la existencia de cierto nivel de impacto negativo sobre el interesado, siempre que este sea mínimo, justificado y mitigado.[370] De este modo, la existencia de un impacto sobre los interesados como consecuencia del tratamiento no invalida de manera directa la utilización de la base del art. 6.1.f) RGPD. Sin embargo, este impacto no podrá ser elevado, sino que deberá mantenerse en un umbral razonable.

Por todo lo anterior, cuantos mayores indicios existan de que el tratamiento de datos resulta inocuo o poco intromisivo, y de que dicho interés puede aportar un beneficio tangible, tanto para el interesado a nivel individual como para la sociedad, mayor justificación habrá para poder concluir que el tratamiento está justificado.

6.3.3. *Resultado preliminar y reevaluación*

Si el juicio de ponderación diera como resultado un alto riesgo para los intereses, derechos y libertades fundamentales de los interesados, el

[370] A pesar de ello, la autoridad de protección de datos de Liechtenstein, en sus directrices sobre el interés legítimo establece que "los intereses del interesado no deben predominar de ninguna manera". DATENSCHUTZSTELLE FÜRSTENTUM LIECHTENSTEIN, *Berechtigtes Interesse gem. Art. 6 Abs. 1 Bst. f DSGVO*.

responsable deberá lleva a cabo una nueva evaluación que evalúe en mayor detalle el posible impacto, así como medidas de mitigación de los riesgos, con el objeto de concluir si dichas acciones pueden permitir utilizar el interés legítimo como base del tratamiento.

Por otro lado, como la lógica indica, cabe la posibilidad de que del ejercicio de ponderación diera como resultado que los intereses legítimos del responsable o tercero no prevalecen sobre aquellos de los interesados. En dicho caso, el resultado puede tomarse como provisional por parte del responsable, y el responsable podrá adoptar medidas y garantías adicionales que permitan minimizar el impacto del tratamiento sobre los interesados antes de repetir el balance de intereses.

De este modo, el responsable podrá introducir nuevos elementos en el balance en favor del interesado y repetir el ejercicio de ponderación de manera subsecuente. En todo caso, y obviamente, ello no podrá servir para falsear un resultado positivo del balance con el objeto de aplicar el interés legítimo como base para un tratamiento sobre el que en realidad prevalezcan los intereses, derechos y libertades fundamentales del interesado.

La elección de las garantías pertinentes deberá especificarse en el caso concreto. Un buen punto de partida es el reforzamiento de aquellas medidas señaladas en el RGPD. Adicionalmente, el responsable puede incrementar la facilidad para el ejercicio de los derechos del interesado, con especial énfasis en el derecho de oposición, llegando incluso a la consideración de conceder el ejercicio de este derecho por defecto, salvo fundadas excepciones. Asimismo, garantizar la portabilidad de los datos podrá ser otro factor que ayude a re-calcular el resultado del ejercicio de ponderación, pues recordemos, este derecho no se garantiza en el RGPD para tratamientos basados en el interés legítimo.

6.3.4. *Proceso vivo en el tiempo*

La ponderación de intereses es un proceso vivo y dinámico, no solo en el momento de la realización del análisis para determinar la base del

tratamiento, sino también a posteriori, en la medida en que el responsable debe garantizar que no han devenido circunstancias que invaliden en resultado del ejercicio de ponderación -lo que en última instancia equivaldría a no disponer a partir de ese momento de una base de legitimación del tratamiento, lo que a su vez desataría el mayor nivel de sanciones que el RGPD establece-.

Así por ejemplo, si un cambio de circunstancias, como el enriquecimiento de la base de datos con nuevos datos, hace que el impacto sobre los interesados pueda ser mayor, será necesario que el responsable vuelva a analizar de nuevo si el interés legítimo sigue siendo una base válida para el tratamiento, o si en su caso, necesita paralizarlo o buscar medidas que reduzcan dicho impacto.

6.3.5. *Cuestiones abiertas*

A pesar del análisis y las indicaciones aquí aportadas, la naturaleza propia de esta base de legitimación, caracterizada por la flexibilidad, resulta en la irremediable subsistencia de cuestiones que quedan abiertas. Así por ejemplo, y quizás la más relevante, será tomar en consideración en qué medida las autoridades de protección de datos se muestran conformes con el uso de esta base de legitimación para tratamientos de datos masivos con técnicas intensivas y complejas. En este sentido, será imprescindible que el responsable sea capaz de demostrar la solidez del proceso que le llevó a concluir que el interés legítimo sería una base de licitud del tratamiento conforme a Derecho.

Otro factor a tomar en consideración en la aplicación de una disposición tan abierta como el art. 6.1.f) RGPD es la posibilidad de que lo que se considere interés legítimo, así como el modo de realizar la ponderación de intereses puede ser diferente entre Estados miembros. En este sentido, la creación de directrices sectoriales a nivel comunitario podría arrojar mayor luz.[371]

[371] CONSEJO DE LA UNIÓN EUROPEA, SECRETARÍA GENERAL (2019): *Preparation of the Council position on the evaluation and review of the General Data Protection Regulation*

6.4. Conclusiones

En este epígrafe hemos analizado la ponderación de intereses, tercer requisito de licitud del interés legítimo como base del tratamiento de datos personales.

Este paso constituye un momento único que obliga al responsable a profundizar sobre si la actividad de tratamiento es capaz de lograr su objetivo y cumplir con sus intereses, pero también, y sobre todo, cuáles son los intereses, derechos y libertades de los interesados que puedan verse afectados. Si bien el responsable está generalmente habituado a llevar a cabo un análisis de sus intereses y riesgos, ponderarlos, tomar medidas de mitigación y actuar en consecuencia, quizás ese hábito no sea tan extendido cuando se refiere a los intereses y riesgos de aquellos cuyos datos desea tratar.

Se trata por tanto de un ejercicio de madurez y sinceridad que debe quedar documentado por escrito. De hecho, la necesidad de realizar y evidenciar documentalmente la ponderación de intereses es lo que otorga un gran potencial al art. 6.1.f) de aportar un grado cualitativamente superior en la protección de los individuos que otras bases.

A pesar de que aún es necesario ampliar el número de referentes doctrinales en favor del interés legítimo, máxime para tratamientos que implican la utilización de tecnologías de datos masivos, los postulados en favor del interés legítimo han comenzado a aparecer. Por ejemplo, Borgesius destaca la importancia del balance de intereses indicando que "la diferencia entre el marketing directo que se basa en el balance de intereses (a través de la exclusión voluntaria u *opt-out*) y el marketing directo que se basa en el consentimiento (*opt-in*) no es meramente teórica. La obligación de realizar la ponderación permite a veces a las empresas tratar datos personales para marketing directo basándose en la exclusión voluntaria, pero en tales casos se exige que la empresa sopese los

(GDPR) - Comments from Member States, de 9 de octubre. Comentarios de Alemania, p. 14.

intereses involucrados. Al confiar en un consentimiento ficticio de exclusión voluntaria, las empresas podrían tratar de eludir la responsabilidad de encontrar un balance entre sus intereses y los del interesado" (traducción propia).[372]

7. Estándar subjetivo. El derecho de oposición

Como se adelantaba en el capítulo anterior, el estándar subjetivo del interesado había quedado definido como aquellos aspectos que afectan a un interesado específico y que afectan al modo de dar cumplimiento a los requisitos necesarios para la validez de la base de legitimación del tratamiento. En relación con la aplicación concreta de la base jurídica del interés legítimo, el estándar subjetivo hace referencia a aquellos extremos que, por afectar de manera particular a un interesado, no hayan sido tenidos en cuenta por el responsable en la realización de la evaluación de interés legítimo -y más concretamente durante la ponderación de intereses-, pues en dicho ejercicio el responsable únicamente considera los aspectos del tratamiento desde la perspectiva genérica del interesado medio.

Cuando la base jurídica del tratamiento fuese el interés público o el interés legítimo, los interesados disponen de un derecho de oposición conforme al art. 21 RGPD, que permite al interesado prevenir el inicio del tratamiento o detenerlo en determinadas circunstancias.

7.1. Derecho absoluto solo para mercadotecnia

En concreto, el individuo goza bajo el RGPD de un derecho de oposición absoluto cuando el tratamiento tuviera por objeto la mercadotecnia directa. En dicho caso, es importante destacar que la oposición se referirá, no solo al tratamiento de datos para la presentación de publicidad por medios electrónicos, sino también a la elaboración de perfiles y otras actividades destinadas a la personalización del contenido publicitario.

[372] ZUIDERVEEN BORGESIUS, Frederik J. (2015): *Improving Privacy Protection in the Area of Behavioural Targeting*, Kluwer Law International BV, p.180.

7.2. Situación particular

En relación con otras finalidades del tratamiento, el derecho de oposición del interesado debe basarse en “motivos relacionados con su situación particular”, que serán analizados por el responsable caso por caso. Esto es, el derecho de oposición otorga al interesado la oportunidad de contactar al responsable para alegar circunstancias personales o apreciaciones subjetivas y que el responsable pudo no tener en cuenta durante la consideración del interés legítimo y la ponderación de intereses realizada teniendo en mente al interesado medio razonable.

Es relevante ser conscientes de que el responsable no podrá conocer *a priori* las circunstancias individuales de cada uno de los interesados cuyos datos puedan ser objeto de tratamiento. Sin embargo, el individuo sí podrá cuestionar el resultado del balance de intereses conforme a circunstancias que formen parte de su contexto individualizado y que no hayan sido tenidas en cuenta, o no lo hayan sido de manera debida en la ponderación realizada por el responsable.

Por ejemplo, la percepción de intimidad y el interés en proteger dicha esfera privada puede ser muy diferente para dos personas. Ello se refleja, por ejemplo, cuando una persona que ha decido no tener un perfil en redes sociales mientras otra sí tiene una presencia amplia en redes. En ese caso, los interesados deben tener mecanismos para expresar sus intereses y preferencias subjetivas y cuestionar la ponderación que el responsable realizó con carácter genérico y objetivable. Un medio para ello es el derecho de oposición. De este modo, el ejercicio extenso del derecho de oposición permite al interesado manifestar su voluntad cuando así lo desee.

7.3. Detención del tratamiento con excepciones

Como regla general, tras el ejercicio de un derecho de oposición, el responsable del tratamiento debe dejar de tratar los datos personales para la finalidad concreta para la que se ha manifestado oposición. En este sentido, cabe hacer diversas apreciaciones.

Es necesario recordar que el derecho de oposición se refiere a una finalidad del tratamiento específica pero no a los datos personales *per se*, y por tanto no conlleva necesariamente la supresión de los datos personales,[373] que podrán seguir siendo tratados para otras finalidades en función de las circunstancias del caso (véase art. 17.1.c). Sin embargo, este matiz no es ampliamente conocido por el interesado medio -ni, probablemente por el interesado concreto que ejerce su derecho-. Así, el interesado podría por ejemplo obtener la impresión de sus datos han sido eliminados de la base de datos del responsable tras ejercer un derecho de oposición. De hecho, algo similar ocurre cuando el interesado ejerce un derecho de supresión. En este caso, el derecho sí se refiere a los datos *per se*, pero a pesar de ello, en la medida en que el responsable siga teniendo una base de licitud del tratamiento de esos mismos datos para otra finalidad, la supresión no podrá hacerse efectiva.[374]

Por otro lado, existen excepciones en las que será posible continuar el tratamiento y denegar el ejercicio del derecho de oposición, tal y como se expone en los párrafos siguientes. Asimismo, en virtud del art. 18.1.d, el responsable debe paralizar el tratamiento hasta que haya resuelto sobre el derecho de oposición.

7.4. Los motivos legítimos imperiosos

La primera excepción al ejercicio del derecho de oposición es aquella por la cual el responsable acredite motivos legítimos "imperiosos" para el tratamiento que prevalezcan sobre los intereses, los derechos y las libertades del interesado, o para la formulación, el ejercicio o la defensa de reclamaciones. Es decir, parece que, a pesar de conceder al interesado un derecho de oposición, el RGPD otorga la última palabra al responsable para

[373] AUSLOOS, Jeff (2016): "The Interaction between the Rights to Object and to Erasure in the GDPR", en *KU Leuven Centre for IT & IP law (CiTiP)*.

[374] AUSLOOS, Jeff; MAHIEU, René; VEALE, Michael (2019): *Getting Data Subject Rights Right, A submission to the European Data Protection Board from Data Protection Academics (v.1)*.

que, tras realizar un nuevo ejercicio de ponderación de intereses, valore si la oposición debe ser atendida.

Aplicada de manera laxa, esta excepción podría suponer una puerta trasera para que, de facto, el responsable pudiera justificar con carácter reiterado que su interés prevalece contra aquellos de los interesados y en consecuencia no atender aquellas circunstancias subjetivas que concurren sobre quienes ejercitan el derecho y que les diferencian del interesado medio razonable. En esta situación, el valor del derecho de oposición se vería desvirtuado y la aplicación del interés legítimo generaría situaciones abusivas para los interesados.

Sin embargo, el espíritu de la norma parece exigir una interpretación especialmente estricta de esta excepción que garantice la efectividad del derecho de oposición. Así lo demuestra la exigencia de que, en este caso, el interés del responsable no deba ser solo legítimo sino también imperioso, término que no se define en el RGPD pero que se utiliza en repetidas ocasiones. Adicionalmente, es el responsable quien asume la carga de la prueba de que el tratamiento de los datos personales puede continuar para la finalidad frente a la que se ha ejercido la oposición.

Así, la interpretación del precepto debe suponer que, salvo situaciones en las que el tratamiento se hubiera basado en intereses excepcionalmente relevantes, cualquier derecho de oposición debe ser atendido y el tratamiento de datos personales debe paralizarse. De este modo, se podría incluso decir que una interpretación garantista daría lugar a concluir que prácticamente cualquier alegación por parte de un interesado sobre sus motivos subjetivos debe conducir a la paralización del tratamiento a pesar de que dichos motivos no sean relevantes. De hecho, el TJUE ha aclarado que los derechos del interesado deben prevalecer con “con carácter general” sobre aquellos intereses económicos del responsable.[375]

[375] TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA (2014): Asunto C-131/12, Google Spain SL, Google Inc v Agencia Española de Protección de Datos (AEPD), Mario Costeja González, de 13 de mayo, apartado 81.

Es decir, aunque el derecho de oposición sea relativo en cualquier tratamiento que no tenga por finalidad la mercadotecnia, la interpretación restrictiva de las excepciones a este derecho debe hacer que funcione con carácter cuasi-absoluto. De hecho, el compromiso del responsable de optar por considerar los derechos de oposición de esta manera cuasi-absoluta podrá ser un elemento de peso a tomar en cuenta durante la realización de la ponderación de intereses en relación con el cumplimiento del estándar del interesado medio razonable y, por tanto, en favor del tratamiento.

7.5. Protección de terceros

En segundo lugar, como excepción a la norma general de paralización del tratamiento cabe atender a lo dispuesto en el art. 18.2, sobre la limitación del tratamiento. Este precepto establece que el tratamiento de datos puede continuar "con miras a la protección de los derechos de otra persona física o jurídica". Esto es, parece que el RGPD permite apreciar una suerte de interés legítimo de terceros que justificaría continuar con el tratamiento de datos personales.

Esta previsión no coincide, sin embargo, con la existencia de un interés legítimo de tercero en sentido propio. En primer lugar, el precepto únicamente hace referencia a la existencia de derechos de otra persona, pero no de intereses. De este modo, parece que la limitación del tratamiento únicamente puede tener lugar cuando se pretenda proteger un bien jurídico expresamente protegido por el ordenamiento jurídico, y, en esencia, con categoría de derecho. Por otro lado, este derecho puede pertenecer, no solo a una persona física, sino también a una persona jurídica, que no ostentan derechos de protección de datos personales.

En todo caso, en dicho caso, parece claro que el tratamiento sí debe limitarse en todo aquello que no entre en conflicto con la defensa de los derechos de un tercero.

7.6. Capacidad de disposición

En atención a todo lo dicho, puede concluirse que, interpretado de manera estricta, el art. 21 RGPD permite al interesado manifestar su postura contraria al inicio o continuidad del tratamiento de sus datos personales y solicitar su finalización. La interpretación de los términos ambiguos utilizados por la norma respecto de las excepciones previstas en el RGPD puede condicionar la efectividad de este derecho de oposición.

Así, el derecho de oposición se trata, en realidad, de un medio voluntario de exclusión del tratamiento, que, como tal, permite que el interesado mantenga un poder de disposición sobre los datos personales a pesar de que la elección de las bases jurídicas de interés legítimo o interés público no parte, inicialmente, de dicha expresión de la voluntad. En consecuencia, no puede sostenerse que la utilización de una base de legitimación del tratamiento diferente del consentimiento o la aceptación de condiciones contractuales que hagan necesario el tratamiento implique no tomar en consideración la capacidad de disposición y decisión del interesado.

7.7. Dificultad para ejercitar el derecho

El derecho de oposición parte de la premisa de que el interesado tiene conocimiento suficiente de las circunstancias del tratamiento como para comprender sus implicaciones y ser capaz de argumentar qué circunstancias relacionadas con su situación particular le avalan. Para ello, deben cumplirse diversas condiciones.

En primer lugar, el interesado debe conocer qué intereses legítimos han servido de base jurídica del tratamiento -lo cual en teoría debería ser posible, pues el responsable está obligado a informar de ello-. Sin embargo, la especificación de los intereses legítimos no siempre es clara en la información aportada por el responsable, y en ocasiones la información sobre el tipo de datos personales tratados, los fines del tratamiento, la base jurídica (y en su caso, los intereses legítimos concretos), así como los derechos aplicables, no está ligada. Como medida de salvaguarda frente a

responsables que deseen hacer un uso poco transparente de la información en aras de crear dificultad para los interesados en el ejercicio de sus derechos, y en atención al principio de responsabilidad proactiva, sería útil exigir que el responsable esté vinculado a aquellos intereses manifestados de manera clara y transparente de modo que no pudiera alegar motivos legítimos imperiosos que no hubieran sido previamente expuestos.

En segundo lugar, el interesado debe conocer el concepto jurídico de interés legítimo y de oposición. Sin embargo, este conocimiento no puede suponerse siempre y en todo caso. De hecho, parece que la realidad indica que el interesado medio no tiene un conocimiento profundo sobre sus derechos en materia de protección de datos. Es razonable pensar que esto sea incluso más acuciante en el concreto caso español en relación con el interés legítimo, por cuanto esta ha sido tradicionalmente una base jurídica poco utilizada sobre la que el interesado medio razonable no ha tenido la oportunidad de ser concienciado. A mayor abundamiento, no debemos olvidar todo lo ya argumentado en relación con la especial dificultad que supone para un interesado medio comprender los factores que intervienen en aquellos tratamientos en los que se utilizan tecnologías big data y caracterizados por la complejidad o la imprevisibilidad.

En tercer lugar, el interesado debe ser capaz de identificar y comunicar qué circunstancias personales conforman su estándar subjetivo de modo tal que el tratamiento deba paralizarse. Todo ello sin conocer qué derechos, intereses y libertades sobre los interesados han sido tomados en consideración por el responsable en la realización del balance de intereses ni qué valor o peso se le ha otorgado a cada uno en relación con los intereses del responsable.

Es esencia, llevar a cabo un ejercicio de oposición requiere un nivel de esfuerzo por parte de los interesados relativamente elevado. De este modo, la falta de directrices, concienciación y educación del interesado medio dificulta el ejercicio de sus derechos y podría cuestionar los efectos favorables del uso del art. 6.1.f) como base de legitimación del tratamiento.

En este sentido, la construcción de un mecanismo sólido y directo de oposición por parte del responsable juega un papel especialmente relevante en el funcionamiento de esta base jurídica.

Por ejemplo, la creación de medios de oposición a través de sistemas conocidos como *opt-out* por los que el usuario puede manifestar de modo sencillo que no desea que sus datos sean objeto de determinado tratamiento serán un modo de elevar las garantías al interesado. De hecho, la creación de modos de oposición sencillos por parte del responsable, incluso aportando mayores garantías y facilidades que aquellas a las que el RGPD obliga, será otro factor a considerar en favor del tratamiento durante la realización del balance de intereses.

7.8. Transparencia en el ejercicio del derecho de oposición

Por otro lado, sería de gran utilidad poder disponer de medios que permitan conocer si un responsable detiene el tratamiento de datos personales con carácter general cuando un interesado ejercita un derecho de oposición y si, por el contrario, existen responsables cuya reacción automática es la alegación de intereses imperiosos que justifican que el tratamiento deba continuar.

Dicha práctica sería de pleno contraria al RGPD en la medida en que la argumentación del responsable atendiera a parámetros y argumentos genéricos, pues la ponderación de intereses requerido durante el ejercicio de un derecho de oposición debe llevarse a cabo, en todo caso, tomando las circunstancias específicas del interesado que ejerce el derecho.

Para ello, ciertas medidas de transparencia aportarían seguridad jurídica. Así, por ejemplo, la publicación por parte de los responsables de datos anuales sobre la cantidad de derechos -y más concretamente, derechos de oposición- han sido ejercidos y cuántos han sido efectivamente atendidos arrojaría luz. Esta medida de transparencia cumpliría un doble objetivo. En primer lugar, el hecho de conocer que determinada información será pública desincentiva que los responsables actúen de modo oscuro. En

segundo lugar, el acceso a dicha información publicada permitiría que la sociedad, investigadores, activistas, expertos o la propia autoridad de control pudieran conocer si existen prácticas que, bajo un supuesto amparo normativo, en realidad escondan incumplimientos como la creación de barreras al ejercicio del derecho de oposición de los interesados.

8. Deber de información al interesado

Una vez que el responsable ha identificado un interés legítimo, ha realizado el juicio de necesidad y por último ha llevado a cabo y documentado la ponderación de intereses, y en la medida en que este último sea favorable en el sentido de que los intereses, derechos y libertades fundamentales de los interesados no prevalezcan, está en posición de realizar un tratamiento de datos conforme al art. 6.1.f) RGPD.

Al inicio de este capítulo hablamos del “test de confianza” como aquella prueba por la que el responsable analiza si se siente cómodo revelando los objetivos del tratamiento, sus intereses legítimos, qué datos se utilizarán o qué repercusiones puede todo ello tener en el interesado. Si comunicar de manera transparente esta información hace que el responsable no se sienta cómodo, entonces lo más probable es que el interés legítimo no sea una base de legitimación válida, sino que se pretenda utilizar para crear una ilusión de legitimación sobre tratamientos obscuros que de otro modo no podrían ser lícitos.

8.1. Transparencia e incongruencias de la norma

Lo que subyace a esta aproximación no es otra cosa que el principio de transparencia, que, en materia de protección de datos, aparece por primera vez recogido de manera expresa en el RGPD. Este principio, que debe observarse cualquiera que sea la base del tratamiento, se liga en ocasiones -y de forma errónea- al requisito de que el consentimiento sea informado. De hecho, la experiencia indica que una de las mayores críticas al interés legítimo deviene precisamente de considerar que la aplicación de una base de legitimación diferente al consentimiento conlleva una falta de

transparencia, control y conocimiento por parte del individuo. Esta afirmación es, no obstante, falaz. En efecto, realizar un tratamiento de datos sin consentimiento no implica, en ninguna circunstancia, realizarlo sin conocimiento del interesado o sin aportar toda la información relevante en relación con el tratamiento, en cumplimiento, ya no solo del principio de transparencia, sino de las obligaciones de información de los arts. 12-14 RGPD.

En este sentido, el RGPD aporta, además, mejoras respecto de la Directiva 95/46. Bien es cierto que la Directiva ya contenía un deber de información, de modo que el concepto de transparencia no es totalmente novedoso. Sin embargo, el RGPD además de haber ampliado el contenido de las obligaciones de información del responsable (arts. 13 y 14), incorpora, como ya se ha expresado, el principio de transparencia (art. 5.1.a)). Y lo hace nada menos que compartiendo cabeza de lista de principios relativos al tratamiento con aquellos de licitud y lealtad. Así, el principio de transparencia debe entenderse ligado al deber de información del responsable -manifestados como derechos de los interesados- pero sin embargo trasciende de este deber. De este modo, se puede entender que un responsable podría cumplir con el contenido de su deber de información, pero infringir, a pesar de ello, con el principio de transparencia.[376]

Asimismo, en observancia de los principios de transparencia y licitud, cuando el responsable del tratamiento aplica el interés legítimo como base del tratamiento, este debe informar al interesado sobre cuáles son los intereses legítimos que persigue él mismo o el tercero con base en los arts. 13.1.d) y 14.2.b) de modo que contribuya a que el interesado obtenga predictibilidad en lo referente a la actividad del tratamiento.

[376] A modo de ejemplo, sirva la sanción de 250.000 euros impuesta por la Agencia Española de protección de datos a LaLiga por incumplimiento del principio de transparencia a pesar de considerar que el consentimiento obtenido fuera válido, y por tanto, deducimos que correctamente informado. AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (2018): Resolución Nº: PS/00326/2018, de 11 de junio de 2019.

Sin embargo, curiosamente, esta información no es necesaria cuando el sujeto ejerce su derecho de acceso en virtud del art. 15. En efecto, al igual que otras cuestiones cubiertas por los derechos de información, la revelación de los intereses legítimos concretos del responsable del tratamiento no forma parte del contenido del derecho de acceso. Esto podría potencialmente perjudicar la capacidad del usuario para impugnar la decisión del responsable del tratamiento de actuar de acuerdo con el arte. 6.1.f) o para ejercer su derecho de oposición (art. 21) y puede terminar por crear asimetrías de información por la dificultad de un usuario de obtener a través de un único medio toda la información relevante.

8.2. Transparencia de procesos big data

A pesar de los esfuerzos de transparencia del responsable, la complejidad de ciertos tratamientos y la velocidad del cambio tecnológico puede provocar que para el interesado medio razonable los medios de recolección de datos (Fase 1), la intensidad del análisis posterior (Fase 2) o la toma de decisiones (Fase 3) pasen desapercibidos o resulten oscuros e incomprensibles. Como ya fue señalado en el capítulo anterior, este problema se aprecia independientemente de la base de legitimación de dichos tratamientos, y tanto en el sector privado como en el sector público.[377]

Por otro lado, el ecosistema de datos no es únicamente complejo en lo que se refiere a la actividad de tratamiento de un responsable concreto. Los datos y metadatos, sean personales o anonimizados, son objeto de cesión y llegan a un número potencialmente ilimitado de partes. Incluso aunque dichos flujos de datos cuenten con base de legitimación y cumplan con otras obligaciones establecidas en el RGPD, ello no siempre conlleva la defensa de las garantías del usuario. Pensemos, por ejemplo, en una

[377] Durante el mes de noviembre de 2019, por ejemplo, la falta de transparencia en relación con un estudio sobre movilidad anunciado por el Instituto Nacional de Estadística español, realizado a partir de datos presuntamente anonimizados de las principales operadoras telefónicas, despertó alarma social motivada, entre otros motivos, por el desconocimiento de las tecnologías y procesos técnicos utilizados.

política de privacidad transparente, completa y sencilla de uno de los cientos de intermediarios o corredores de datos que reciben datos del interesado. Su nombre aparece en un listado de terceros a los que se cederán los datos en una primera política de privacidad, aquella que se le presenta al interesado al acceder a un servicio online determinado. No es razonable pensar que el interesado haya comprendido las implicaciones de que sus datos sean cedidos a dicho corredor, que actúa como tercero, ni es en cualquier modo juicioso suponer que todos los interesados vayan también a acceder a las políticas de privacidad de cada uno de dichos terceros para comprender el alcance una cesión de datos de tan amplio espectro. Así, en entornos en los que interactúan un número elevado de partes, la transparencia no se traduce en que el interesado pueda realmente hacerse cargo de las consecuencias de sus decisiones. En términos similares, el hecho de que exista información transparente disponible para los usuarios, no debe conllevar la obligación de estos de comprenderla. Llanamente, el interesado no debe ser compelido a actuar como ente de control para detectar y paralizar usos de los datos y tratamientos dañinos o abusivos. El uso de los datos de manera, no solo transparente, sino también leal y ponderada debe ser obligación inherente a la actividad del responsable.

En otras ocasiones, este mismo resultado se produce incluso aunque los datos no sean cedidos a un número elevado de terceros intermediarios en el mercado de los datos. En todo caso, prácticamente en cualquier interacción del usuario, existirán diversas partes que actuarán como corresponsables de, al menos, alguna de las actividades del tratamiento. Así por ejemplo, en el caso de un sensor embebido en un dispositivo común como una camiseta, es posible pensar que intervienen, como mínimo, un desarrollador del software y la organización que comercializa las camisetas. De modo similar, en el caso de una aplicación móvil, el usuario interactúa con el desarrollador de la aplicación, así como el vendedor del teléfono o dispositivo móvil donde la instala. En estos casos, incluso aunque el número de responsables que tienen acceso directo a los datos personales

del interesado y que pueden hacer uso de estos sea más limitado, no existe un único punto de contacto que le permita a dicho interesado acceder de manera transparente a toda la información relevante. La última jurisprudencia del TJUE en la materia, entre la que destaca la resolución en el caso Fashion ID,[378] destaca por ampliar el concepto de corresponsabilidad así como los deberes de información del primer responsable, aquél con el que el interesado interactúa de manera directa en una primera instancia. A pesar de ello, el esfuerzo que debe hacer el usuario para comprender las relaciones y responsabilidades de cada parte, así como los aspectos relativos al tratamiento, es desproporcionado.

En este sentido, la legitimación de los tratamientos a través de mecanismos que no se basen en la premisa de que el interesado haya comprendido todos los elementos del tratamiento pueden resultar en un mayor nivel de protección de estos. Por ello, el interés legítimo como base jurídica puede ser capaz de suplir esta limitación, gracias a la realización de la ponderación de intereses que el responsable realiza con toda la información de la que este dispone, siendo que él es quien más conocimiento debe tener sobre el contexto completo del tratamiento.

9. Interés legítimo en la práctica: jurisprudencia. Especial referencia al TJUE

Como ya ha sido mencionado, el análisis sobre la validez del interés legítimo como base del tratamiento debe ceñirse al caso concreto y no es posible adelantar, con carácter genérico, un resultado. A pesar de todo, resulta de utilidad analizar los casos estudiados por el TJUE y que conforman su línea jurisprudencial.

La jurisprudencia del TJUE no prevé directrices u orientaciones extensas sobre la interpretación del interés legítimo como fundamento jurídico. Una de las razones de ello es que el TJUE no ha tratado muchos casos que

[378] TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA (2019): Asunto C-40/17, Fashion ID GmbH & Co. KG vs Verbraucherzentrale, de 29 de julio. ECLI:EU:C:2019:629.

exigiesen la interpretación de la disposición sobre el interés legítimo (art. 7.f)Directiva). Otra causa es que, incluso en los casos en los que se solicitó al Tribunal que aclarase el concepto de interés legítimo o sus pasos, este se ha quedado corto a la hora de proporcionar orientaciones concretas (por ejemplo, dejando a los tribunales nacionales la posibilidad de llevar a cabo el ejercicio de ponderación y de equilibrar los intereses y los derechos).

En los epígrafes siguientes analizaremos la jurisprudencia llevada ante el conocimiento del TJUE en relación con la aplicación del interés legítimo como base del tratamiento. Los casos se presentan en orden cronológico inverso (es decir, de más reciente a más antiguo).

9.1. Asunto TK (2019)[379]

TK es residente en un apartamento que forma parte de una comunidad de vecinos. Tras aprobarse la decisión, se instalaron varias cámaras de videovigilancia en zonas comunes del edificio con el objetivo de prevenir actos vandálicos como los que ya se habían producido. Frente a ello, TK consideró que dichas cámaras vulneraban sus derechos e inició acciones legales.

El caso trata la cuestión de una ley nacional que permite actividades de videovigilancia sin consentimiento, para proteger intereses legítimos y garantizar la guarda y protección de personas, bienes y valores. El Tribunal es preguntado acerca de si esta restricción del derecho a la protección de datos personales contraviene el art. 7.f) de la Directiva. El Tribunal nacional también planea si dicha habilitación es proporcional, necesaria y responde a intereses generales de la Unión o si hay otras alternativas con las que el responsable puede proteger su interés legítimo. Asimismo, se plantea la cuestión de si el responsable debe probar la existencia de un interés legítimo actual en el momento del tratamiento de los datos. Por último, se

[379] TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA (2019): Asunto C-708/18, TK vs Asociaţia de Proprietari bloc M5A-ScaraA, de 19 de diciembre. ECLI:EU:C:2019:1064.

plantea si el tratamiento es excesivo o no adecuado conforme al principio de conservación de los datos.

En lo que aquí interesa, el TJUE concluye que existe un interés legítimo consistente en garantizar la protección de los bienes, de la salud y de la vida de los copropietarios del inmueble. En respuesta a la cuestión del tribunal nacional, el TJUE aclara que el interés legítimo debe existir y ser actual en el momento del tratamiento de los datos, y no meramente hipotético. Sin embargo, esto no exige que necesariamente haya existido previamente un daño a la seguridad de bienes y personas. En este caso, el TJUE aprecia la existencia y actualidad del interés en el momento del tratamiento. Asimismo, el TJUE recalca que el requisito de necesidad debe interpretarse en un sentido de "estricta necesidad". El TJUE indica que el tratamiento es considerado necesario para la satisfacción de dicho interés, pues la prevención de delitos no puede alcanzarse de manera eficaz por otros medios. Sin embargo, en atención al principio de minimización de datos, el TJUE invita al responsable a plantearse si su interés pudiera conseguirse si la videovigilancia funciona únicamente de noche, o a través de la difuminación de imágenes. En la ponderación de intereses, que será tarea del tribunal nacional, deberán tenerse en cuenta factores como el carácter potencialmente sensible de los datos, el número de personas que tienen acceso a ellos, las expectativas razonables de los interesados.

9.2. Asunto Fashion ID (2019)[380]

Fashion ID es una empresa de comercio electrónico de moda, que insertó en su página web a modo de plug-in el botón «Me gusta» de Facebook para obtener un beneficio comercial derivado de la optimización publicitaria. De esta manera, cuando un usuario accede a la página web de Fashion ID, se transfiere automáticamente a Facebook información sobre la dirección IP del usuario y datos técnicos del navegador, con independencia de si el usuario ha clicado o no el botón «Me gusta» o de si tiene o no cuenta en

[380] TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA (2019): Asunto C-40/17, Fashion ID GmbH & Co. KG vs Verbraucherzentrale, de 29 de julio. ECLI:EU:C:2019:629.

Facebook. En esencia, la controversia en el presente asunto se refiere a la recogida y transmisión de datos personales con fines de optimización publicitaria.

La cuestión principal, y sobre la que parten las demás, gira en torno a si el administrador de un sitio web -Fashion ID- que inserta un código que permite la recogida de datos personales -como botones de redes sociales- es responsable del tratamiento. El Tribunal declara que Fashion ID puede ser corresponsable junto con Facebook por las actividades que se refieren únicamente a la "recogida y la comunicación por transmisión de datos personales" de los visitantes de su web a Facebook, incluso aunque el administrador de Fashion ID no tuviera acceso a los datos. La responsabilidad sobre el tratamiento posterior de los datos que lleve a cabo Facebook únicamente le corresponde a este.

Posteriormente, se plantean cuestiones relativas a la base de legitimación del tratamiento de datos personales. En primer lugar, en la medida en que mediante el botón insertado se pueda haber accedido o transmitido información almacenada en el dispositivo del usuario, como aquella proveniente de cookies, resultaría de aplicación la Directiva e-Privacy . En virtud de esta, en las circunstancias del caso, un agente únicamente podría acceder a la información almacenada en el equipo terminal de los usuarios si contase con consentimiento para ello, el cual no fue solicitado. En consecuencia, el Tribunal nacional deberá determinar si realmente se instalaron cookies o rastreadores similares mediante las que el proveedor del módulo social accediese a los datos almacenados en dispositivo y actuar en consecuencia.

Para analizar la base de legitimación del tratamiento de los demás datos de carácter personal, deberá acudirse a la Directiva de protección de datos. Existen varias consideraciones relevantes. En primer lugar, el Tribunal analiza si existió base de legitimación del tratamiento, en concreto, interés legítimo, en vista de que no se solicitó consentimiento de los usuarios. El caso se decide sobre la base de la Directiva 95/46, pero bajo el RGPD esto

no sería posible puesto que el responsable está obligado a indicar antes de iniciar el tratamiento qué base de legitimación lo sustenta.

En segundo lugar, el Tribunal resuelve qué intereses legítimos deberían tomarse en consideración en la ponderación que exige el art.7.f) de la Directiva 95/46, los del administrador -Fashion ID- o los del proveedor -Facebook-. La cuestión resulta interesante por cuanto puede abrirse a considerar, entre otros factores, si Fashion ID puede aludir únicamente a su interés propio en la inserción de contenidos de terceros o al interés legítimo de un tercero como la red social. El TJUE declara que han de tenerse en cuenta los intereses legítimos de ambos corresponsables, pues ambos deben contar con una base de legitimación propia que justifique sus operaciones de tratamiento.

El marketing y una mayor eficacia publicitaria pueden constituir, de por sí, intereses legítimos. Sin embargo, el órgano judicial nacional que remitió el caso al TJUE no comunica qué intereses legítimos fueron aludidos en el procedimiento, ni pide ayuda para valorarlos, de modo que el TJUE no tiene información suficiente para analizar si en el caso concreto existe dicho interés legítimo. Así, será el tribunal nacional quien deberá analizar el contexto para determinar si los intereses legítimos de ambos responsables cumplen los requisitos para ser una válida base de legitimación.

9.3. Asunto Buivids (2019)[381]

El caso concierne los hechos por los que el Sr. Buivids grabó y publicó en el portal YouTube un vídeo de su propia declaración en una comisaría de la Policía Nacional en el marco de un procedimiento incoado contra él. En la grabación también aparecían varios policías en su actividad en lo que, a su juicio, constituía una actuación ilegal de estos. El caso plantea la posibilidad de si dicha filmación y publicación en internet podría estar amparada por el derecho de libertad de expresión con fines periodísticos

[381] TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA (2019): Asunto C-345/17, Sergejs Buivids vs Datu valsts inspekcija, de 14 de febrero. ECLI:EU:C:2019:122.

conforme al art. 9 Directiva 95/46, para demostrar comportamientos policiales supuestamente ilegales.

Además del interesante desarrollo sobre el equilibrio entre el derecho de libertad de expresión con el derecho a la protección de datos personales, la Abogado General[382] analiza la alegación presentada por el Gobierno checo en el sentido de que el Sr. Buivids está amparado por el art. 7.f) de la Directiva en estas actividades de tratamiento. En este caso, la Abogado General aprecia que esta provisión debe interpretarse en relación con el art. 6.1.b de la Directiva, que proclama que los datos personales sean recogidos con fines determinados, explícitos y legítimos. Puesto que el Sr. Buivids no había informado a los interesados sobre la finalidad concreta de la realización de la grabación del vídeo, no contaba con el consentimiento de los afectados y, asimismo, el art. 7.f) tampoco es de aplicación al caso.

En consecuencia, la resolución del Tribunal no entra siquiera a valorar el interés legítimo del Sr. Biuvids.

9.4. Asunto Nowak (2017)[383]

El caso concierne la solicitud del Sr. Nowak, contable en prácticas, de acceder a la información personal, incluidos los exámenes, que se hallaban en poder de la organización donde había realizado varios exámenes, a lo que la institución se negó sobre la base de que un examen escrito no era un dato personal.

El TJUE reconoció que un examinando tiene un interés legítimo en poder oponerse al tratamiento de las respuestas presentadas por él en dicho examen y de las observaciones del examinador con respecto a dichas respuestas al margen del procedimiento de examen y, en particular, a que se envíen a terceros o se publiquen sin su autorización. Del mismo modo,

[382] Conclusiones del Abogado General Sra. Eleanor Sharpston presentadas el 27 de septiembre de 2018, C-345/17, Sergejs Buivids vs Datu valsts inspekcija. ECLI:EU:C:2018:780, párrafos 68-71.

[383] TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA (2017): Asunto C-434/16, Peter Nowak vs Data Protection Commissioner, de 20 de diciembre. ECLI:EU:C:2017:994.

el organismo que realiza el examen, en su calidad de responsable del tratamiento, está obligado a garantizar que las respuestas y comentarios se almacenan de forma que se garantice que no se permite el acceso ilícito de terceros a los mismos.

Asimismo, el candidato al examen también puede tener un interés legítimo en que se supriman sus datos personales, es decir, que se destruya el examen, cuando haya perdido valor probatorio del resultado del examen. Por último, por lo general tendrá un interés legítimo en averiguar qué información sobre ellos procesa el responsable del tratamiento. Es evidente que los derechos de acceso y rectificación previstos en el artículo 12, letras a) y b), de la Directiva también pueden hacerse valer en relación con las respuestas escritas presentadas por un candidato en un examen profesional y con las observaciones formuladas por un examinador con respecto a dichas respuestas.

9.5. Asunto Rīgas (2017)[384]

Este asunto concernía los daños que un pasajero de taxi que abrió la puerta de forma repentina causó sobre un trolebús de la compañía de transportes de Rīgas Satiksme, hecho por el cual Rīgas quiso iniciar un procedimiento contra al pasajero por daños y perjuicios. Para ello, Rīgas solicitó a las autoridades policiales los datos del pasajero necesarios para iniciar acciones, a lo que estas se negaron.

El Tribunal analizó el concepto de interés legítimo de un tercero a quien se comuniquen los datos como base de licitud del tratamiento. El órgano jurisdiccional remitente preguntaba si el art. 7.f) de la Directiva implicaba una obligación de ceder datos personales a un tercero, y si el hecho de que el interesado fuese menor de edad debía influir en la interpretación de la disposición.

[384] TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA (2017): Asunto C-13/16, Rīgas, de 4 de mayo. ECLI:EU:C:2017:336.

El TJUE indicó que el art. 7.f) de la Directiva confería la *facultad* de realizar un tratamiento de datos personales, pero en ningún caso *obliga* a comunicar datos personales a un tercero.

En relación con el caso concreto, el TJUE declaró que la obtención de información personal de una persona que dañó un bien por parte del propietario de dicho bien para iniciar acciones legales es un interés legítimo y necesario. Asimismo, expuso que la edad del interesado puede ser uno de los factores que deben tenerse en cuenta en la ponderación de intereses. No obstante, siguiendo las conclusiones del Abogado General, el TJUE consideró que, en el caso que se juzgaba, la minoría de edad del interesado no era un factor que modificase el resultado de la ponderación de intereses y por tanto no justificada que las autoridades se hubiesen negado a proporcionar al tercero los datos personales necesarios para ejercer acciones legales contra el propio interesado o contra quienes ejercieran la patria potestad. Con todo, el TJUE no resolvió sobre la ponderación de intereses, labor que quedó encomendada al tribunal nacional.

9.6. Asunto Manni (2017)[385]

Este caso concernía la inscripción de datos personales por parte de una autoridad pública en el registro de sociedades en un Estado miembro, accesible públicamente. El Sr. Manni solicitó la eliminación de sus datos con el fin de que sus clientes no accediesen a la información según la cual este había sido administrador de una sociedad que quebró años atrás alegando que su interés comercial podría ser perjudicado.

El Tribunal determinó que el tratamiento de datos que lleva a cabo la autoridad pública responsable de mantener el registro de sociedades en un Estado miembro, y que contiene datos personales, puede estar basada en tres bases de legitimación: primera, la existencia de una obligación legal;

[385] TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA (2017): Asunto C-398/15, Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce vs Salvatore Manni, 9 de marzo. ECLI:EU:C:2017:197.

segunda, el ejercicio de autoridad pública o ejecución de una misión de interés público; y tercera, la realización de un interés legítimo del responsable o los terceros a quienes se comunican los datos.

El caso gira en torno a la cuestión de si el responsable debe, pasado un tiempo, conservar los datos o bien eliminarlos, anonimizarlos o limitar su publicidad. En este caso, el carácter público del registro estaba establecido por ley con la finalidad de favorecer los intereses legítimos de terceros de acceso a la información de sociedades con las que iniciar algún tipo de actividad. El TJUE afirma que "en la ponderación que debe llevarse a cabo en el marco de esta disposición prevalece, en principio, la necesidad de proteger los intereses de terceros en relación con las sociedades (…) y de garantizar la seguridad jurídica".[386] Así, el Tribunal consideró que los intereses de terceros de conocer el estado patrimonial de las sociedades, así como la protección de la seguridad jurídica, la lealtad comercial y el funcionamiento del mercado interior prevalecían sobre los derechos del Sr. Manni, que no tenía un derecho de supresión.

A pesar de ello, el Tribunal recuerda que cuando el tratamiento se base en el art. 7.e) -interés público- o art. 7.f) -interés legítimo- de la Directiva el interesado puede ejercitar un derecho de oposición. Este es el medio para poder ponderar la situación particular y observar si existen razones legítimas propias que justifiquen, de manera excepcional, que el acceso a los datos personales debe ser limitado. El TJUE recuerda que corresponde a los tribunales nacionales tomar en consideración todo el contexto y las circunstancias particulares del sujeto, así como la posible expiración de un plazo suficientemente largo que justifique la disminución del interés de los terceros de consultar la información. Aun así, el TJUE señaló que en el caso concreto del Sr. Manni, la afectación de su interés comercial no constituía un interés preponderante, sino que la injerencia sobre sus derechos e intereses se justificaba por un interés general.

[386] Párrafos 60-63.

9.7. Asunto Breyer (2014)[387]

El caso trata el concepto de interés legítimo de las administraciones públicas.

El asunto se inicia por la reclamación del Sr. Breyer y gira en torno al hecho de si la dirección IP dinámica, unida a otros datos que permiten la identificación del usuario, es un dato personal. Los sitios web de las instituciones públicas alemanas accedían y almacenaban la dirección IP de los visitantes para evitar ataques o iniciar acciones legales. El TJUE consideró que la dirección IP dinámica constituye un dato personal en determinadas circunstancias.[388]

Además de ello, el caso trataba la cuestión de la existencia de legislación nacional que no permitía que se tuviera en cuenta el interés legítimo del responsable del tratamiento para conservar los datos personales de los visitantes de las páginas web.

El TJUE manifestó que una norma nacional no puede reducir el alcance del art. 7.f) de la Directiva al establecer el tratamiento de ciertos datos personales solo podrá realizarse con el consentimiento del interesado o cuando sea necesario para facturar un servicio en línea. El TJUE recuerda jurisprudencia anterior según la cual los Estados miembros no pueden añadir requisitos ni exigencias adicionales de legitimación que modifiquen el alcance dado a dicho artículo por el legislador comunitario a las seis bases de legitimación del tratamiento. Si bien es cierto que los Estados miembros gozan de un cierto margen de apreciación, en el caso en lid la norma nacional no se limita a precisar el concepto de interés legítimo, sino que lo limita. En este sentido, el TJUE reconoce que existe un interés

[387] TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA (2016): Asunto C-582/14 Patrick Breyer v Germany, de 19 de octubre. ECLI:EU:C:2016:779.

[388] En concreto, una dirección IP dinámica será dato personal para aquél tercero que disponga de los datos adicionales para identificar a la persona, en este caso, el proveedor del servicio de acceso a Internet (por ejemplo, Google). Por su parte, para el proveedor de servicios de medios de internet (por ejemplo, el responsable de una página web), resultará ser dato personal cuando disponga de medios legales para acceder a la información adicional en poder del proveedor de acceso a internet que permita identificar al sujeto.

legítimo en pretender garantizar la continuidad del funcionamiento de los servicios web y su seguridad.

Asimismo, señala el tribunal que un Estado miembro no puede decidir de forma categórica el resultado de la ponderación de los derechos e intereses en conflicto ni, por tanto, excluir de manera generalizada la posibilidad de ponderar los intereses y tener en cuenta las circunstancias en cada caso concreto.

Por otro lado, el Tribunal considera que en este caso las autoridades públicas, a pesar de su naturaleza, actúan en calidad de particulares y fuera del ámbito de sus actividades. Por este motivo, es posible alegar un interés legítimo como base para el tratamiento de datos personales.

9.8. Asunto Rynes (2014)[389]

El Tribunal consideró que el tratamiento de datos a través de cámaras de videovigilancia instalado en la puerta de la vivienda familiar y que capta parte del espacio público para la protección de los bienes, la salud y la vida del responsable y los de su familia no se amparan en la excepción de uso doméstico pero pueden constituir un interés legítimo sin necesidad de informar al interesado ni garantizarle otros derechos, conforme a lo previsto en la propia Directiva sobre limitación de derechos de los interesados, aunque deja que el balance de intereses lo realice el tribunal nacional. En sus conclusiones, el Abogado General[390] señalaba que, en la ponderación de intereses, debe tomarse en cuenta que el interés del responsable es la protección de un derecho fundamental propio, como lo es el derecho de propiedad y de la vida familiar. Asimismo, señalaba expresamente que el objetivo de la Directiva es “establecer un equilibro justo entre los derechos [del responsable] y los derechos de otras personas físicas”.

[389] TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA (2014): asunto C-212/13, Ryneš, de 11 de diciembre. ECLI:EU:C:2014:2428.

[390] Conclusiones del Abogado General Sr. Niilo Jääskinen presentadas el 10 de julio de 2014, Asunto C-212/13 Ryneš, ECLI:EU:C:2014:2072.

9.9. Asunto Google Spain (2014)[391]

El caso se refería al derecho a la supresión (o al derecho al olvido).[392] En otras palabras, estaba en juego el equilibrio entre, por una parte, el derecho de una persona a que se retiren sus datos del índice de los motores de búsqueda e impedir el acceso a los mismos y, por otra, el interés legítimo de los proveedores de motores de búsqueda y de los usuarios de internet.

En caso de que la base de legitimación del tratamiento sea el art. 7.f) de la Directiva, el interesado puede ejercer un derecho de oposición por motivos propios de su situación particular en virtud del art. 14, párrafo 1.a, para lo cual debe realizarse una ponderación de intereses y derechos. Adicionalmente, el interesado también goza del derecho del art. 12, relativo a la rectificación, supresión o bloqueo de los datos.

El Tribunal reconoce la existencia de un interés económico del responsable del tratamiento, así como un interés legítimo de los internautas en tener acceso a la información, que han de ponderarse en busca de un equilibro con el interés y los derechos fundamentales del Sr. Costeja. El Tribunal declara que los derechos de privacidad y protección de datos del interesado prevalecen con carácter general sobre el interés de los internautas a acceder a la información. El TJUE ofreció orientaciones sobre los factores que deben tenerse en cuenta durante el ejercicio de ponderación equilibrada, tales como la naturaleza de la información, la sensibilidad de la información para la esfera privada de la persona o el interés público de disponer de la información. En este sentido, el resultado de la ponderación,

[391] TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA, (2014): Asunto C-131/12, Google Spain SL, Google Inc v Agencia Española de Protección de Datos (AEPD), Mario Costeja González, de 13 de mayo.

[392] Para un análisis extenso sobre el derecho al olvido, ver ÁLVAREZ CARO, María (2017): La privacidad en la sociedad de la información: el derecho al olvido en la UE como reto derivado del avance digital, tesis doctoral; ÁLVAREZ CARO, María (2015): *Derecho al olvido en internet: el nuevo paradigma de la privacidad*, Madrid, Reus; ÁLVAREZ CARO, María (2014): "Reflexiones sobre la sentencia del TJUE en el asunto "Mario Costeja" (C-131/12) sobre derecho al olvido", en *Revista española de derecho europeo*, No. 51, p. 165-187; RECIO GAYO, Miguel (2020): "Derecho al olvido: notas sobre su evolución y futuro en la Unión Europea", en *El Cronista del Estado Social y Democrático de Derecho*, No. 88-89 (Ejemplar dedicado a: Protección de datos: antes, durante y después del coronavirus).

que debe realizarse en virtud de los arts. 7.f) y 14.1.a de la Directiva, puede variar en función del responsable que realice la valoración (en el caso en lid, en función de si la ponderación la realiza un editor de una página web o el gestor de un motor de búsqueda de internet).

El Tribunal consideró que los derechos fundamentales del interesado a la protección de datos y el respeto a la vida privada engloban el llamado "derecho al olvido" y prevalecerían en principio sobre el interés económico del responsable del tratamiento y el interés de terceros en que se les conceda acceso a la información. Si bien el Tribunal alude a que no parece que en el caso concreto el interés público de acceder a la información sea superior al derecho del interesado, deja en manos de la jurisdicción nacional determinar este factor a la luz de las circunstancias concretas del caso. El Tribunal indica que el gestor de un motor de búsqueda debe, en su caso, eliminar de la lista de resultados los vínculos a páginas web de terceros que aparezcan al realizar una búsqueda a partir del nombre de la persona, incluso aunque no se obligue al editor de dichas páginas web a eliminar la información (en otras palabras, que los datos se olviden tras un lapso de tiempo).

Asimismo, recuerda el Tribunal que incluso cuando el tratamiento de los datos fue inicialmente lícito en virtud del art. 7, este puede devenir incompatible con la Directiva, en concreto con el art. 6, por resultar no pertinente, excesivo en relación con los fines o los datos estén siendo conservados por un tiempo superior al necesario, lo cual es, por otra parte, independiente de que mantener la información cause un perjuicio al interesado.

Como la propia sentencia indica, "la respuesta a esta cuestión depende del modo en que debe interpretarse la Directiva 95/46 en el marco de estas tecnologías, que han surgido después de su publicación".[393] Esto es, hace mención expresa a una evolución en la interpretación de las normas a la

[393] Párrafo 19.

luz del desarrollo tecnológico para conseguir una mejor consecución de los objetivos perseguidos con la normativa de protección de datos.

En esencia, el Tribunal reconoce que el tratamiento de los datos por parte del responsable del motor de búsqueda puede constituir un interés legítimo, y no pone en duda la licitud del tratamiento bajo el art. 7.f) de la Directiva. No obstante, puesto que el tratamiento de datos debe respetar los principios del art. 6 durante toda la duración del tratamiento, este puede devenir contrario a dichos principios en un momento posterior, para lo cual el interesado dispone de un derecho al olvido de sus datos. Puesto que las disposiciones a través de las cuales el interesado puede ejercitar su derecho a que sus datos sean olvidados o restringir el acceso a ellos requieren una ponderación, el Tribunal indica que, en dicha etapa posterior, de manera apriorística, se puede determinar que el derecho del interesado sea mayor que el derecho económico del responsable o el derecho del público a acceder a la información. En todo caso, habrá que atenerse a las circunstancias del caso concreto que puedan determinar que el derecho del interesado pueda restringirse, tales como la posible relevancia pública del interesado.

Tras la sentencia del TJUE, el Grupo de Trabajo del Artículo 29 adoptó directrices para la aplicación del fallo, que incluyen una lista de criterios a aplicar por las autoridades de control en la ponderación de derechos.[394]

9.10. Asuntos ASEF y FECEMD (2011)[395]

El Tribunal decidió que el uso del interés legítimo como base de legitimación no debe estar limitado por el Derecho nacional. Por lo tanto, la condición establecida en la legislación nacional española de protección de datos de que los datos personales estén disponibles en fuentes públicas

[394] GRUPO DE TRABAJO DEL ARTÍCULO 29 (2014): *Guidelines on the implementation of the Court of Justice of the European Union judgment on "Google Spain and Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" C-131/12* (WP 225), de 26 de noviembre.

[395] TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA (2011): Asuntos acumulados C-468/10 y 469/10 ASNEF y FECEMD, de 24 de noviembre. ECLI:EU:C:2011:777.

para que puedan aplicarse los intereses legítimos no era lícita, pues modificaba la disposición de la Directiva. Este asunto será analizado en mayor detalle en el siguiente epígrafe, durante la exposición de diversos precedentes en España.

9.11. Comentarios

La primera y más llamativa conclusión que puede extraerse de la jurisprudencia analizada es el escaso número de casos de que el TJUE ha conocido en relación con la aplicación del interés legítimo como base del tratamiento. Asimismo, es necesario resaltar que gran parte de esta jurisprudencia se refiere a la aplicación del art. 7.f) de la Directiva, y no al art. 6.1.f) RGPD. No obstante, a pesar de la falta de abundancia de la jurisprudencia, debido al hecho de que el RGPD mantuvo los principios fundamentales del interés legítimo como base legal para el tratamiento, el conocimiento y la experiencia que ofrece esta jurisprudencia constituyen un punto de partida útil para la interpretación del arte. 6.1.f) del RGPD.

Por otro lado, estos precedentes sientan las bases y aclaran algunos de los conceptos más significativos en relación con el art. 7.f) de la Directiva y su correspondiente art. 6.1.f) RGPD. En concreto, se refieren algunos factores de ponderación que deben formar parte del balance de intereses y se valoran aspectos ambiguos de la redacción normativa. Tal es el caso del concepto de interés legítimo de las administraciones públicas, la consideración de niño como factor relevante en la ponderación de intereses, o el interés legítimo de tercero. También de la necesaria ponderación entre diferentes derechos, como el derecho de propiedad y de la vida familiar, así como el ejercicio de los derechos inherentes del interesado para la protección de sus datos personales, concretamente el derecho de oposición al tratamiento.

A pesar de lo anterior, también destaca el hecho de que el Tribunal no entra a decidir sobre el resultado del balance de intereses, tarea que es sistemáticamente remitida a los tribunales nacionales, perdiéndose oportunidades para posicionarse en el que quizás el aspecto más delicado

de esta base jurídica. En todo caso, esta remisión a los tribunales nacionales no debe verse como una elusión de funciones por parte del Tribunal, ni como una decisión de no pronunciarse sobre determinadas cuestiones. En efecto, esta práctica responde a la configuración del sistema jurisdiccional en la Unión Europea, que únicamente responde a aquellas cuestiones que les son remitidas por los jueces nacionales y sobre la información que les es proporcionada. En otras palabras, cuando un juez nacional tiene dudas sobre la interpretación de un determinado precepto normativo, remiten una cuestión al tribunal comunitario, cuya función radica en clarificar o interpretar la norma en aras de que su aplicación sea homogénea en todos los Estados.

10. El interés legítimo en la normativa española de protección de datos personales

Como ya fue analizado en el capítulo anterior, bien es cierto que, con carácter general, el consentimiento ha sido considerado la piedra angular de la protección de datos desde sus inicios, y esta tendencia se ha podido apreciar en la práctica jurídica de los Estados miembros, facilitada en gran medida por la validez del consentimiento táctico.

En esta práctica generalizada, el caso español goza de particularidades que hicieron que, aún con mayor intensidad, el consentimiento fuera la base de legitimación del tratamiento utilizada por defecto, en contra del uso del resto de bases jurídicas, a pesar de que, en muchas ocasiones, podría no ser la más apropiada. La transposición de la Directiva 95/46 al ordenamiento jurídico español, realizada a través de la LOPD de 1999, incluyó ciertas particularidades que la alejaban de lo dispuesto en la norma comunitaria, y este hecho fue especialmente notorio en lo que se refería a las bases de legitimación del tratamiento, esto es, el art. 6 LOPD.

Por su parte, la adaptación del RGPD al ordenamiento jurídico nacional, realizado a través de la conocida como LOPDgdd también ha contado con especificidades que han determinado el contenido final de la norma.[396]

Es este capítulo analizaremos la evolución del interés legítimo en las normas de protección de datos españolas hasta la actualidad. Sin duda, en el caso español se observa un patrón claro que ayuda a explicar qué concepto tiene el legislador y la autoridad de control sobre esta base jurídica y cómo ello puede afectar, especialmente en tratamientos que conlleven el análisis masivo de datos a través de nuevas tecnologías.

10.1. La Ley 15/1999 Orgánica de Protección de Datos de carácter personal

10.1.1. Los precedentes

La Constitución española de 1978 fue pionera en el reconocimiento de la protección de datos personales como derecho fundamental. Su art. 18.4 establece que "la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos".[397] Este momento estuvo marcado por la reciente salida de España de un período dictatorial sin libertades, lo que definitivamente influyó en nuestros constituyentes, que elaboraron un amplio catálogo de derechos fundamentales. Si bien a finales de los años 70 el desarrollo

[396] Otros juristas españoles también han abordado el interés legítimo como base de licitud, tanto en relación con las normas comunitarias como en nuestro ordenamiento jurídico. Destacan los comentarios de FERNÁNDEZ-SAMANIEGO, Javier; FERNÁNDEZ-LONGORIA, Paula (2019): "El interés legítimo como principio para legitimar el tratamiento de datos", en Artemi Rallo Lombarte (coord.), *Tratado de protección de datos*, Madrid, Tirant lo Blanch; SEMPERE, Francisco Javier (2019): "Interés legítimo en el tratamiento de datos: análisis, ponderación y supuestos prácticos", en *Privacidad Lógica*; BENITO, Ruth (2017): "Examen del interés legítimo como base del tratamiento de datos", en *Con la venia, Señorías*; GARCÍA HERRERO, Jorge (2018): "Interés Legítimo y LOPD: Tutorial de uso", en Jorge García Herrero Blog.

[397] HERNÁNDEZ LÓPEZ, José Miguel (2013): "El derecho a la protección de datos personales en la doctrina del Tribunal Constitucional", en *Aranzadi, Cizur Menor*, p. 29-33.

informático era aún incipiente, sobre todo si lo comparamos con la realidad actual, existía una "conciencia social" acerca de sus riesgos.[398]

El desarrollo de esta disposición a nivel legislativo, no se produjo hasta bastante más adelante, con la promulgación en 1992 de la Ley Orgánica 5/1992, de 29 de octubre, reguladora del tratamiento automatizado de datos personales (LORTAD). La motivación última de la creación de la LORTD no fue el desarrollo del precepto constitucional, sino la integración de España en el entorno del Grupo Schengen.[399]

Más adelante, el Tribunal Constitucional declaró en su STC 94/1998 que se trata este de un derecho por el que se garantiza a la persona el "control" sobre sus datos, cualesquiera datos personales, y sobre su uso y destino, para evitar el tráfico ilícito de los mismos o lesivo para la dignidad y los derechos de los afectados. De esta forma, el derecho a la protección de datos se configuró como una facultad del ciudadano para oponerse a que determinados datos personales sean usados para fines distintos a aquel que justificó su obtención.[400]

La construcción constitucional del derecho a la protección de datos personales muestra una evolución desde los derechos de intimidad, privacidad y autodeterminación informativa surgida de la necesidad de resolver diferentes recursos de amparo y de la delimitación de la capacidad de control de la persona sobre sus datos.[401]

---

[398] MURILLO DE LA CUEVA, Pablo Lucas (2003): "La Constitución y el derecho a la autodeterminación informativa", en *Cuadernos de Derecho Público*, No. 19 (Ejemplar dedicado a: Protección de datos), p. 27-44.

[399] MURILLO DE LA CUEVA, Pablo Lucas (2003): "La Constitución y el derecho a la autodeterminación informativa", en *Cuadernos de Derecho Público*, No. 19 (Ejemplar dedicado a: Protección de datos), p. 27-44. Para un mayor detalle sobre la doctrina constitucional ver MURILLO DE LA CUEVA, Pablo Lucas (2003): "La primera jurisprudencia sobre el derecho a la autodeterminación informativa", en *Datospersonales.org: La revista de la Agencia de Protección de Datos de la Comunidad de Madrid*, Nº. 1, 2003.

[400] Preámbulo a la LOPDgdd.

[401] PIÑAR MAÑAS, José Luís (2005): "El derecho fundamental a la protección de datos personales. Algunos retos de presente y futuro", en *Asamblea: revista parlamentaria de la Asamblea de Madrid*, No. 13, págs. 21-46.

10.1.2. Sentando el contexto de la LOPD

Un año más tarde de esta sentencia se culminó el proceso legislativo que dio lugar a la Ley Orgánica 15/1999, de 5 de diciembre, de protección de datos personales (LOPD), a fin de trasponer a nuestro derecho a la Directiva 95/46/ y de recoger en una norma más actualizada la experiencia generada durante la vigencia de la anterior LORTAD. En este proceso pudieron conjugarse el punto de vista de los legisladores europeos, que ponían el desarrollo económico como una de las prioridades de la regulación comunitaria, con la visión del legislador español, principalmente atento al imperio de la Constitución.[402]

De manera coetánea, el Tribunal Constitucional aportó una intensa labor de interpretación y desarrollo, desde la consagración del denominado derecho a la autodeterminación informativa hasta la declaración de la doble naturaleza de este derecho: por un lado, se trata de un derecho autónomo y, por otro lado, resulta ser un derecho instrumental para la protección de otros derechos fundamentales, fundamentalmente el honor y la intimidad.[403] En concreto, la STC 292/2000, de 30 de noviembre, declaró el derecho a la protección de datos como un derecho autónomo e independiente del derecho a la intimidad.[404] Aunque el objeto principal de la sentencia fue declarar la inconstitucionalidad de parte de la LOPD, el Tribunal comienza con una completa definición del derecho a la protección de datos personales,[405] cuyo contenido faculta a la persona a decidir qué datos proporcionar a un tercero (ya sea el Estado o un particular), qué datos

[402] MURILLO DE LA CUEVA, Pablo Lucas (1999): "La construcción del derecho a la autodeterminación informativa", en Revista de estudios políticos, No. 104, p. 35-60.

[403] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (1999): *Memoria anual, 1999*, p. 184.

[404] El Tribunal Constitucional mostraba "su intención creadora" y la "necesidad de dotar de autonomía a la protección de datos, respecto del derecho a la intimidad" de tal forma que materializó un nuevo derecho fundamental "con tanta precisión y amplitud (…) que ha fijado completamente la categoría". MARTÍNEZ MARTÍNEZ, Ricard (2004): *Una aproximación crítica a la autodeterminación informativa*, Madrid, Civitas.

[405] MURILLO DE LA CUEVA, Pablo Lucas (2003): "La Constitución y el derecho a la autodeterminación informativa", en Cuadernos de Derecho Público, No. 19 (Ejemplar dedicado a: Protección de datos), p. 27-44.

pueden ser recabados por terceros. Asimismo, este derecho faculta a la persona a conocer quién posee esos datos personales y para qué, pudiendo oponerse a dicha posesión o uso.

Resulta relevante la separación del derecho a la protección de datos del derecho a la intimidad. En efecto, le primero brinda protección al tratamiento de datos de nuestras actividades que no siempre son íntimos y que no necesariamente ocultamos, sino que "desarrollamos a la luz pública y de las que dejamos, incluso, constancia en guías, registros, anuncios, o, simplemente, las facilitamos inocentemente".[406] La protección de aquella información personal que vertemos en las actuales redes sociales es quizás la máxima expresión de estas primeras concepciones.

Esto es, el desarrollo del derecho a la protección de datos se ha encontrado ligado a la declaración expresa de que este otorga a la persona un poder de decisión sobre sus datos y un poder de oposición, en esencia, una capacidad de control. Esta concepción tiene una clara manifestación en el listado de bases de legitimación del tratamiento. En concreto, la práctica diaria de protección de datos en España ha estado fuertemente marcada dos factores: en primer lugar, la prevalencia del uso del consentimiento como base jurídica frente a otras bases, y en según lugar, más concretamente por una postura contraria al uso del interés legítimo tal y como fue concebido. ¿Cómo se manifestaron estos elementos?

10.1.3. *Jerarquía de bases de legitimación*

Quizás la expresión más clara de la mayor prevalencia del consentimiento sobre otras bases del tratamiento en España fue la redacción dada al art. 6.1 LOPD 15/1999, que establecía que

> "1. El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la ley disponga otra cosa".

[406] MURILLO DE LA CUEVA, Pablo Lucas (2003): "La Constitución y el derecho a la autodeterminación informativa", en Cuadernos de Derecho Público, No. 19 (Ejemplar dedicado a: Protección de datos), p. 27-44.

La primera apreciación que cabe hacer es señalar la clara preferencia que mostró el legislador nacional por la figura del consentimiento, que se menciona no solo en primer lugar sino como una suerte de norma general sobre la que caben excepciones, que no son sino las bases de legitimación señaladas en el apartado segundo. De este modo, el legislador creó una jerarquía de bases de legitimación cuya cúspide ocupaba el consentimiento. Todo ello a pesar de que la Directiva 95/46, que servía de marco a la norma nacional, establecía un modelo de bases de legitimación alternativas y no jerárquico (al menos en teoría). De hecho, en relación con este apartado, un estudio[407] sobre la transposición de la Directiva a la norma española criticaba la decisión española indicando que no habría sido necesario forzar los supuestos de excepción del consentimiento, sino que habría bastado con admitir, al lado de este y en igualdad, las demás bases de licitud que enumeraba la Directiva. De hecho, el informe llega a comparar la LOPD de 1999 con "las piezas de un rompecabezas que hubieran sido colocadas de manera que la figura compuesta fuera distinta de la prevista, aunque hecha con las mismas piezas".

De este modo, la tendencia que también se observaba en otros Estados miembros en torno a la primacía del consentimiento, que ha sido considerado una pieza esencial de la protección de datos, tuvo un carácter más marcado en España, hasta el punto de que un responsable solicitaba el consentimiento con el único fin de crear una sensación de licitud del tratamiento.[408] Recordemos, este era solo el primer motivo por el que el consentimiento se convirtió en España, con mayor fuerza que en el resto de los Estados miembros, en la base de legitimación por defecto.

[407] HEREDERO HIGUERAS, Manuel (2000): "Estudio crítico de la transposición de la Directiva 95/46/CE en el Ordenamiento Jurídico español por la L.O. 15/1999, de 13 de diciembre", en Conferencia pronunciada en el curso de verano de la Universidad Nacional de Educación a Distancia, 18 de julio.

[408] PUENTE ESCOBAR, Agustín (2019): "Algunas cuestiones relevantes en la tramitación de la LOPDGDD", en Javier López Calvo (coord.), *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD*. Madrid, Wolters Kluwer.

10.1.4. *Requisitos adicionales para el interés legítimo*

En el apartado segundo del mencionado art. 6 LOPD se enumeraban, a modo de excepción, el resto de bases de legitimación con las siguientes palabras:

> "2. No será preciso el consentimiento cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones públicas en el ámbito de sus competencias; cuando se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento; cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del artículo 7, apartado 6, de la presente Ley, o cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado" (énfasis añadido).

Por su parte, el desarrollo de la LOPD dado por el RLOPD[409] de 2007 reiteraba en su art. 10 una posición preferencial en el uso del consentimiento, que no sería necesario cuando:

> "Lo autorice una norma con rango de ley o una norma de derecho comunitario y, en particular, cuando concurra uno de los supuestos siguientes: El tratamiento o la cesión tengan por objeto la satisfacción de un interés legítimo del responsable del tratamiento o del cesionario amparado por dichas normas, siempre que no prevalezca el interés o los derechos y libertades fundamentales de los interesados (…)"; o que "los datos objeto de tratamiento o de cesión figuren en fuentes accesibles al público y el responsable del

[409] Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

fichero, o el tercero a quien se comuniquen los datos, tenga un interés legítimo para su tratamiento o conocimiento, siempre que no se vulneren los derechos y libertades fundamentales del interesado".

En resumen, en lo que se refiere al interés legítimo, la LOPD supeditaba su validez al cumplimiento de los siguientes requisitos:

i. Que los datos figurasen en fuentes accesibles al público.
ii. Que el tratamiento fuera necesario para la consecución de los fines.
iii. Que existiese un interés legítimo del responsable del fichero o un tercero a quien se comuniquen los datos.
iv. Que dicho interés legítimo no vulnerase los derechos y libertades fundamentales del interesado.

Es decir, la norma nacional añadía un requisito adicional a los impuestos por el art. 7.f) de la Directiva: que los datos constasen en fuentes accesibles al público. Estas fuentes son, por su parte, un *numerus clausus*, a tenor del art. 3.j) LOPD compuesto exclusivamente por el censo promocional, los repertorios telefónicos, las listas de personas pertenecientes a grupos de profesionales, los diarios y boletines oficiales y los medios de comunicación.[410]

[410] De hecho, el tratamiento de datos personales públicos ha sido controvertido en relación con la nueva LOPDgdd, y muestra de ello son dos ejemplos principales.

En primer lugar, respecto a la definición de lo que debe considerarse "fuentes accesibles al público" utilizada por el art. 58 bis, cuyo apartado segundo indica que "Los partidos políticos, coaliciones y agrupaciones electorales podrán utilizar datos personales obtenidos en páginas web y otras fuentes de acceso público para la realización de actividades políticas durante el periodo electoral". De este modo, la redacción dada al precepto parece incluir las páginas web (y por tanto, internet en términos amplios) como fuente accesible al público, equiparando de manera errónea el sentido literal gramatical de la expresión -pues cierto es que una página web es accesible a la generalidad de la población- con la definición legal del concepto -que, como se indicaba, consiste en una lista tasada de fuentes entre las que no consta internet-.

En segundo lugar, el anteproyecto de Ley Orgánica contenía una habilitación legal para el tratamiento de "datos hechos manifiestamente públicos por el afectado", que se consideraba lícito, con carácter general. Este artículo fue puesto en entredicho por el Consejo de Estado, que consideró no estaba basado en ninguno de las bases de licitud del art. 6.1 RGPD. Asimismo, la jurisprudencia del TJUE ha sido clara al indicar que los Estados miembros no pueden incorporar en su ordenamiento nacional principios de legitimación no incluidos en las normas comunitarias.

La aversión del legislador nacional contra el interés legítimo pudo verse desde etapas tempranas del desarrollo de la LOPD. De hecho, una versión preliminar de la LOPD de 1999, ni siquiera incorporaba el art. 7.f) de la Directiva sobre interés legítimo como base del tratamiento. Tras una llamada de atención por parte de la Comisión Europea y determinadas negociaciones, finalmente el interés legítimo fue incorporado en la norma nacional[411] aunque de manera más limitada que en la Directiva. Pareciera así que el legislador nacional asumió que la existencia de la base del interés legítimo era equivalente a crear una puerta abierta para cualquier tipo de tratamiento que una organización o cualquier responsable deseara llevar a cabo. En otras palabras, un cheque en blanco. Al lector puede sonarle esta expresión, pues en efecto, en el capítulo anterior argumentábamos cómo, contra pronóstico, fue el consentimiento el que se convirtió en un cheque en blanco para los tratamientos que desease llevar a cabo el responsable utilizando la inercia del interesado para aceptar las condiciones que se le muestran.

Se trata este de uno de los innumerables ejemplos que escenifican el mosaico normativo que derivó de la transposición de la Directiva 95/46 a los ordenamientos jurídicos de cada Estado miembro y que condujo a la creación de diferencias significativas en materia de protección de datos personales entre Estados. Esta tendencia parece apreciarse también en otras disposiciones de la norma. Así por ejemplo, el art. 11 LOPD establecía la necesidad de contar con el consentimiento del interesado como base para la comunicación de datos personales a terceros, salvo que estos se encontrasen en fuentes accesibles al público.

Ciertamente, no debemos olvidar que la protección de datos personales es un derecho que solapa en determinadas ocasiones con el derecho a la intimidad, pero no se restringe a ello. La noción de dato personal abarca tanto aquellos datos de la persona que mantiene privados o en su esfera de intimidad como aquellos otros hechos públicos. PIÑAR MAÑAS, José Luis (2010), "Comentario al artículo 3", en Antonio TRONCOSO REIGADA (Dir.), *Comentario a la ley Orgánica de Protección de datos de carácter personal*, Civitas, Cizur Menor, pp. 184-213.

411 CERVERA NAVAS, Leonardo (2018): "Data processing beneficial to individuals: the use of legitimate interest", en *Computers, Privacy and Data Protection Conference*, Bruselas.

De esta lectura se desprende que, además de posicionarse en favor del uso del consentimiento, el legislador se posicionó también frente al uso del interés legítimo. Es decir, podría decirse que en España la jerarquía de bases jurídicas constaba de tres escalones. El primero, el consentimiento, dispuesto como regla general. El segundo, las demás bases de legitimación mencionadas en el art. 6, apartado segundo (que tampoco suponen una transposición directa de la Directiva) excepto el interés legítimo, que se configuran como una salvedad a la regla genérica. En último lugar, el interés legítimo se configuró como una base jurídica de tercera clase, pues además de ser también una salvedad a la norma general, quedó modificado en el sentido de que se le hizo depender de un que no se contemplaba en la Directiva europea.

En este contexto, las dudas sobre la validez de este requisito adicional de la LOPD con respecto a aquello que requería la Directiva de 1995 traspasaron nuestra frontera para llegar a ser objeto de estudio por el TJUE. Analicemos brevemente el caso.

10.1.5. *Resolución del TJUE. Asuntos acumulados ASNEF y FECEMD (2011)*

Como se adelantaba en el epígrafe anterior, esta cuestión fue analizada por el TJUE en los asuntos acumulados ASNEF y FECEMD.[412] El Tribunal Supremo conocía de sendos recursos presentados por la Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) y la Federación de Comercio Electrónico y Marketing Directo (FECEMD) contra el contenido del art. 10 RLOPD. El Tribunal reflexionaba que esta restricción constituiría un obstáculo a la libre circulación de los datos personales. Así, ello equivaldría a decir que la libre circulación de datos personales que se encuentren en ficheros que no se consideran accesibles al público vulneraría en todo caso los derechos y libertades del interesado.

[412] TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA (2011): Asuntos acumulados C-468/10 y 469/10 ASNEF y FECEMD, de 24 de noviembre. ECLI:EU:C:2011:777.

Ante la duda de que esta fuera la voluntad del legislador comunitario, el Tribunal Supremo planteó cuestión prejudicial ante el TJUE.[413]

El TJUE indicó que los Estados miembros no pueden añadir exigencias adicionales que modificasen el alcance del art. 7 de la Directiva y que, en el caso español, el Estado sobrepasó su margen apreciación limitando así el alcance de la Directiva.[414] Bien es cierto que el hecho de que los datos no figuren en una fuente accesible al público puede constituir un factor a tener en cuenta en la ponderación de intereses, en la medida en que agravaría la lesión a los derechos del interesado.[415] Con todo, este factor debe ser apreciado "en su justo valor, contra prestándolo al interés legítimo perseguido".[416]

De este modo, el TJUE considera que el margen de apreciación que tienen reconocido los Estados abarca la determinación de ciertos factores que puedan orientar la balanza a uno u otro lado en la realización del juicio de ponderación. Sin embargo, establecer el resultado definitivo de dicha ponderación sin permitir apreciar las circunstancias del caso concreto sobrepasa el dicho margen de apreciación, pues excluye "de forma categórica y generalizada" la posibilidad de ponderar ambos lados de la balanza.

Adicionalmente, el TJUE reconoce expresamente el efecto directo del art. 7.f) de la Directiva.

De hecho, también en 2011, en el marco del inicio del proceso de revisión que culminó años más tarde con la promulgación del RGPD, el Supervisor

---

[413] GUASCH PORTAS, Vicente; SOLER FUENSANTA, José Ramón (2015): "El interés legítimo en la protección de datos", en *Revista de Derecho UNED*, No. 16.

[414] Este mismo argumento fue reiterado, de nuevo, en jurisprudencia posterior, concretamente en el asunto Breyer C-582/14.

[415] RUBÍ NAVARRETE, Jesús (2012): "Tratamiento de datos personales. Satisfacción del interés legítimo. Ley de protección de datos. Sentencia Tribunal Supremo, de 8 de febrero de 2012. Sentencia TJUE, de 24 de noviembre de 2011", en *Comunicaciones en Propiedad Industrial y Derecho de la Competencia*, No.66.

[416] TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA (2016): Asunto C-582/14 Patrick Breyer v Germany, de 19 de octubre. ECLI:EU:C:2016:779.

Europeo de Protección de Datos indicaba que "la definición de las condiciones para el tratamiento de datos constituye un elemento esencial de toda legislación en materia de protección de datos. No se debe permitir a los Estados miembros que introduzcan modificaciones a los motivos o motivos adicionales para el tratamiento o que excluyan alguno de ellos".[417] A renglón seguido, el Supervisor expresaba su deseo de que el RGPD redujese el margen de apreciación en relación con las bases de legitimación del tratamiento.

10.1.6. *¿Supuso un cambio real?*

De manera posterior a la resolución del TJUE, al Agencia Española de Protección de Datos emitía una nota de prensa[418] afirmando que la interpretación que la propia AEPD venía realizando del precepto nacional tomaba el hecho de figurar en fuentes accesibles al público como un mero factor más en la ponderación de intereses. Ello, no obstante, sí era posible encontrar en la jurisprudencia española procedimientos en los que el precepto nacional fue aplicado atendiendo a la literalidad del mismo y por tanto no conforme a la interpretación que la AEPD defendía. De este modo, la resolución del TJUE sí tuvo un efecto modificador de la práctica jurídica nacional.[419]

Por su parte, el Tribunal Supremo, en su sentencia de 8 de febrero de 2012 (rec. 25/2008), aplicando los pronunciamientos contenidos en la sentencia del TJUE, afirma que "lo que expresa el Tribunal es que con la exigencia de que los datos figuren en fuentes accesibles al público se excluye de forma categórica y generalizada todo tratamiento de datos que no figuren en tales fuentes, y declara tal proceder contrario al artículo 7 f) de la

[417] SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS (2011): *Dictamen sobre la Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones — Un enfoque global de la protección de los datos personales en la Unión Europea (2011/C 181/01)*, de 22 de junio.

[418] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (2012): *Nota Informativa, El Tribunal de Justicia de la Unión Europea resuelve la cuestión prejudicial planteada por el Tribunal Supremo relativa a la interpretación del artículo 7 f) de la Directiva 95/46/CE*.

[419] GONZÁLEZ CALLEJA, David (2011): "TJUE: pueden tratarse datos sin consentimiento y sin que figuren en fuentes accesibles al público", en *Lexnova blogs*.

Directiva", por lo que la circunstancia de que los datos figuren en fuentes accesibles al público, referenciada en el artículo 10.2 b) del Reglamento, no actúa como elemento de ponderación. Ninguna dificultad de redacción habría para darle ese carácter. Actúa, y a ello se refiere la sentencia en su fundamento 47, como requisito habilitante que, por adicionarse a la previsión del artículo 7 f) de la Directiva, debe declararse nulo...".

Y en consecuencia anuló el art. 10.2.b) del Real Decreto 1720/2007 de 21 de diciembre.

10.1.7. *Consentimiento tácito vs interés legítimo. ¿dos caras de la misma moneda?*

El caso español es una magnífica oportunidad que sirve de punto de partida para aclarar esta cuestión.

En España, el consentimiento prestado de manera tácita gozaba de validez antes de la entrada en aplicación del RGPD y, de hecho, era un medio ampliamente utilizado. Este tipo de consentimiento es aquel que no requiere expresión activa del interesado, sino que se desprende de la inactividad, el silencio o la falta de oposición del interesado. La LOPD requería que el interesado hubiera sido adecuadamente informado y se garantizara su derecho a revocar el consentimiento cuando existiese causa justificada.[420] Así, parecen surgir similitudes entre el consentimiento tácito y el interés legítimo, en la medida en que ambos permiten el tratamiento sin necesidad de una manifestación expresa del interesado, siempre que este haya sido adecuadamente informado y se le haya otorgado la garantía de impedir dicho tratamiento, ya sea mediante la revocación del consentimiento o ejerciendo su oposición.

A pesar de todo ello, el RGPD prohíbe expresamente el consentimiento tácito, que además ha recibido diversas opiniones en contra.[421] Por su

[420] Art. 6 LOPD.

[421] Por ejemplo, el GT29 se había expresado en contra del consentimiento tácito sobre la base de que la definición de consentimiento bajo la Directiva 95/46 se refería a que este debía ser una manifestación inequívoca de voluntad, lo cual tiene difícil encaje en el mero silencio o pasividad del interesado, pues se tratan manifestaciones fácilmente equívocas.

parte, el interés legítimo continúa siendo una de las bases de licitud bajo el RGPD sin haber sufrido apenas cambios desde su redacción en la Directiva 95/46 y su validez ha sido defendida e incluso el GT 29 ha argumentado que tiene la misma validez que cualquiera de las otras bases. A mayor índole, cuando la transposición a la norma española se apartaba de lo dispuesto en la Directiva, el TJUE declaró la aplicación directa del precepto comunitario. En consecuencia, podría surgir la duda de ¿por qué si ambas figuras comparten características esenciales una ha sido deslegitimada y otra defendida? ¿Es el interés legítimo una suerte de consentimiento tácito? Cierto es que existen similitudes, y sin embargo, aún más cierto es que aquellos aspectos en los que se diferencian son claves.

En primer lugar, la regulación del interés legítimo ha exigido desde su inicio que, para basar un tratamiento sobre este, el responsable deba cumplir con diversos requisitos adicionales a aquel de informar, el único que pesa sobre el consentimiento tácito. En efecto, como se ha visto a lo largo de este capítulo, el interés legítimo requiere al responsable recapacitar sobre qué interés desea satisfacer, argumentar que el tratamiento cumple el requisito de necesidad y, con especial énfasis, realizar un balance de intereses. Por su parte, el consentimiento tácito permitiría iniciar directamente el tratamiento sin desplegar ninguna de estas garantías. Por otro lado, el consentimiento crea la presunción *iruris tantum* de que el interesado ha manifestado, por el medio que sea, su aquiescencia, otorgando al responsable un medio de prueba de la licitud del tratamiento que, en realidad, pocas veces puede sustentarse sobre evidencias sólidas.

En esencia, el interés legítimo aporta sin lugar a dudas un grado de garantía muy superior a aquél del consentimiento tácito.

GRUPO DE TRABAJO DEL ARTÍCULO 29 (2011): *Dictamen 15/2011 sobre la definición del consentimiento* (WP 187), de 13 de julio.

10.1.8. Asunto CITA (2012)[422]

La sentencia del TJUE tuvo de hecho efectos sobre otros asuntos pendientes en España, y en concreto jugó un papel relevante en el conocido como asunto CITA. La AEPD había impuesto sanción a un particular y a la empresa Cooperación Internacional en Tecnologías Avanzadas (CITA) por mostrar en una página web un video sin consentimiento de las personas que en ellas aparecían, bajo el argumento de que las imágenes se referían a funcionarios públicos realizando actividades conocidas y anunciadas en medios de comunicación, y los vídeos fueron obtenidos a través de páginas de internet de fácil acceso. Concretamente, CITA publicó en una página web, destinada a proporcionar noticias relacionadas con el ámbito judicial y en especial con la actividad de peritación, una información referida a la actividad desarrollada por varios profesores de la Universidad Politécnica de Madrid que actuaban como peritos de parte en procesos judiciales, pese a estar en régimen de dedicación exclusiva.

Tras un proceso en primera instancia, CITA interpuso recurso ante la Audiencia Nacional alegando, entre otros motivos, que, dado que la sanción en lid se basa en el tratamiento de datos personales sin consentimiento de los interesados y que no figuraban en fuentes accesibles al público, existía similitud con la cuestión prejudicial planteada ante del TJUE en los casos ASNEF y FEDEM, por lo que este Tribunal debía plantear también cuestión prejudicial.

La Audiencia estimó que la interpretación de la norma debía seguir lo indicado por el TJUE en la cuestión prejudicial indicada y el planteamiento de una nueva cuestión prejudicial era innecesario. Así, el Tribunal consideró que, entre los intereses legítimos alegables, se encuentran “de forma significativa” los derechos del art. 20 de la Constitución española,

[422] AUDIENCIA NACIONAL, Sentencia de 11 de abril de 2012. ECLI: ES:AN:2012:1702.

especialmente los derechos a la libertad de expresión y a comunicar o recibir libremente información.

En la ponderación de intereses, el Tribunal consideró factores como el tipo de derecho que se ejercía, el tipo de información que se facilitaba y su relevancia, la finalidad perseguida, el medio utilizado, el número de destinatarios posibles y la existencia de intereses generales en la obtención de ese tipo de información.[423]

Finalmente, el Tribunal consideró que el tratamiento de datos estaba amparado por el derecho a la libertad de expresión e información y no

[423] FJ 8º. "No debe olvidarse, al tiempo de realizar esta ponderación, que tanto la libertad de expresión, como también ocurre con la de información, adquieren especial relevancia cuando "se ejerciten en conexión con asuntos que son de interés general, por las materias a que se refieren y por las personas que en ellos intervienen y contribuyan, en consecuencia, a la formación de la opinión pública, alcanzando entonces su máximo nivel de eficacia justificadora frente al derecho al honor, el cual se debilita, proporcionalmente, como límite externo de las libertades de expresión e información, en cuanto sus titulares son personas públicas, ejercen funciones públicas o resultan implicadas en asuntos de relevancia pública, obligadas por ello a soportar un cierto riesgo de que sus derecho subjetivos de la personalidad resulten afectados por opiniones o informaciones de interés general, pues así lo requieren el pluralismo político, la tolerancia y el espíritu de apertura, sin los cuales no existe sociedad democrática" (STC 107/1988, de 8 de junio , FJ 2). (…).

FJ 9º. "La resolución [de la AEPD] parece inclinarse por una concepción expansiva de la protección de datos a la que anuda una sanción sin ponderar los intereses en conflicto, pues cuando aborda la colisión del derecho a la protección de datos de los denunciantes con el derecho a la libertad de expresión del hoy recurrente se limita a afirmar, esta vez de forma muy concisa y contundente, que las páginas web del imputado no puede ser consideradas un medio de comunicación social por lo que no cabe invocar la prevalencia del derecho de libertad de información.(…)

Esta concepción, como ya hemos tenido ocasión de señalar, ha sido superada por la jurisprudencia, pues ni resulta un requisito excluyente del tratamiento el que el dato no se haya obtenido de una fuente accesible al público, ni en la ponderación de los derechos fundamentales en conflicto es posible sostener que los derechos de libertad de expresión e información están reservados para los medios de comunicación social (prensa radio y televisión) y la pagina web del imputado no lo sea. (…)

Todo ello, sin perjuicio de que la protección que dispensan estos derechos en su confrontación con otros deba entenderse reforzada cuando su ejercicio se produce por los profesionales de la información o por los medios de comunicación convencionales, pero sin olvidar que la comunicación, hoy en día, no se circunscribe a los medios de comunicación tradicionales sino a otros medios muy diversos, propiciados por la actual tecnología, en los que internet ocupa un papel muy relevante para obtener y difundir información veraz y para expresar libremente las propias opiniones e ideas."

constituía una vulneración del derecho a la protección de datos, anulando así la sanción previamente impuesta por la AEPD.[424]

10.1.9. Conclusiones

En conclusión, el recorrido de la norma española muestra de forma muy clara nuestra tradición cultural en materia de protección de datos. La capacidad de control inherente al reconocimiento del derecho a la protección de datos ha sido interpretada en el sentido de que dicho control debe ejercerse a través de la manifestación del consentimiento, pues este era considerado el medio más seguro para prevenir usos no deseados de los datos personales.

Para asegurarse de que los responsables no encontrasen vacíos legales o áreas de interpretación oscuras sobre las que sustentar tratamientos abusivos, el legislador español creó una pirámide de bases de legitimación de tres pisos en la que primaba el consentimiento, seguido de otras bases que emanaban de la Directiva de protección de datos y habilitaciones legales, dejando en último lugar y a modo residual la base jurídica del interés legítimo.

Sería justo reconocer que en determinados momentos o entornos esta estructura jurídica conseguía su objetivo, al menos sobre el papel: ser especialmente protectora y garantista, así como reducir el margen de apreciación de los responsables, principalmente del sector privado. No obstante, la aplicación práctica de la norma, así como el paso del tiempo cambiaron, en mi humilde opinión, esta situación. ¿Por qué?

[424] FJ 10º. "El ejercicio de la libertad de expresión y de información que amparaba al recurrente implica el tratamiento de los datos personales de los sujetos objeto de la crítica y de la información, pues la utilización de sus datos personales, de forma proporcional y justificada por el fin que se persigue y la libertad que se ejerce, se constituye un instrumento imprescindible sin el cual la crítica o la información carecería de sentido y se vaciaría de contenido. Por otra parte, tanto sus nombres, cargos e imágenes eran de conocimiento público al haber sido obtenidas de las páginas web oficiales de la propia Universidad y los videos aparecen referidos a una actuación judicial pública que se encontraba colgada en youtube con la que estableció un vínculo, por lo que tampoco puede sostenerse que los datos proporcionados estuviesen fuera del alcance público desvelándose datos personales que desvinculados de la información no se conociesen anteriormente".

Respecto de la aplicación práctica, ocurrió algo paradigmático. El primer escalón de la pirámide se agrandó más de lo conveniente mediante la aceptación del consentimiento tácito, que, como ha sido argumentado, reduce el nivel de protección del consentimiento y es, por naturaleza, menos garantista que el consentimiento expreso y que el interés legítimo, del que se quería huir. Por su parte, el último escalón -interés legítimo- quiso ser reducido a la mínima expresión mediante la incorporación de mayores requisitos que los que preveía la norma europea, hasta el punto de dejar irreconocible la base jurídica, causando que los tribunales comunitarios invalidaran el precepto. Es decir, el intento ciego de proteger al interesado y su capacidad de control en realidad terminó por viciarse.

El paso del tiempo también es un factor relevante que debe manifestarse en las bases de legitimación más adecuadas de cada momento. Desde la creación de la LORTAD, la LOPD hasta la llegada del RGPD, el estado de la técnica cambió por completo, causando una transición de una sociedad analógica a una digital. En poco tiempo, las personas se han visto enfrentadas a continuas solicitudes de consentimiento para más tratamientos, de consecuencias de mayor magnitud, a través de métodos que no han podido ser comprendidos por un interesado medio razonable por su rapidez de desarrollo y cambio. Aquellos tratamientos cuyos factores y contexto resultan estables, sencillos, previsibles y comprensibles, el consentimiento es ciertamente un instrumento que aporta grandes garantías al interesado y que le permite ejercer un control efectivo y autónomamente manifestado. Sin embargo, cuando la naturaleza de las actividades del tratamiento es cambiante, compleja, imprevisible e incomprensible, el interesado pierde la capacidad de control porque simplemente no es capaz de manejar el contexto en el que debe desenvolverse. En esta situación, el empeño por responsabilizar al interesado de sus decisiones termina por limitar su protección. Así, el avance tecnológico es también uno de los factores más relevantes que han viciado el consentimiento.

10.2. El cóctel: interés legítimo, big data y la AEPD a la luz del RGPD

La autoridad de control española se ha pronunciado en diversas ocasiones en relación con el interés legítimo, pero especialmente relevante resultó la respuesta a una consulta concreta que reunía múltiples factores de interés. La consulta se refiere, entre otras cosas, al uso del interés legítimo para tratamientos masivos de datos bajo lo previsto en el RGPD, es decir, que tiene carácter de futurible.

10.2.1. Consulta de la Asociación Española de Banca

El Informe 0195/2017[425] de la AEPD en respuesta a diversas consultas planteadas por la Asociación Española de Banca es quizás el documento reciente más extenso y relevante que muestra la posición de la autoridad de control española en relación al uso del interés legítimo como base del tratamiento bajo el RGPD. El informe resuelve diversas cuestiones en torno a la base de legitimación aplicable a determinados tratamientos, y concretamente en relación a la posibilidad de la aplicación del art. 6.1.f).[426]

El interés que despertó la ha llevado a ser popularmente considerada como "La Consulta" del interés legítimo. Debido a su relevancia, conviene detenerse en algunos de los aspectos principales cubiertos en el informe.

10.2.2. Comunicaciones comerciales sin perfilado[427]

En primer lugar, la Asociación Española de Banca somete a consulta qué base de legitimación debe regir el envío de comunicaciones comerciales que no requieren perfilado, es decir, realizado a partir de información básica como los datos identificativos de los clientes. En este caso, se hace necesario diferenciar el canal utilizado para el envío de dichas

[425] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, GABINETE JURÍDICO (2017): *Informe 0195/2017*.

[426] Asimismo, el informe también resuelve determinadas cuestiones en relación con el ejercicio del derecho de portabilidad y posibles tensiones entre la normativa de protección de datos y de prevención de blanqueo de capitales y financiación del terrorismo.

[427] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, GABINETE JURÍDICO (2017): *Informe 0195/2017*, p. 6.

comunicaciones. Si el canal fueran medios electrónicos, el tratamiento de datos debe atenerse a lo dispuesto en el art. 21 LSSI, que únicamente permite el envío de publicidad con consentimiento del interesado o en situaciones específicas (concretamente, la existencia de una relación contractual previa con el cliente, que los productos o servicios ofertados sean similares a aquellos previamente contratados y posibilidad de ejercicio de derecho de oposición). El uso de otros canales, como el postal, sí podrá basarse en el interés legítimo del responsable conforme al RGPD, aunque la Agencia interpreta, por analogía que debe cumplirse el requisito de que los bienes o servicios sean similares a los previamente contratados, así como la necesidad de tomar en cuenta las expectativas razonables del destinatario en el juicio de ponderación. Asimismo, el interesado debe continuar siendo cliente actual de la organización.

Por ejemplo, una entidad bancaria no podrá enviar a sus clientes de servicios de crédito información comercial sobre otros productos, como pudiera ser un dispositivo inteligente para medir la velocidad del automóvil que forme parte de la rama aseguradora de dicha entidad.

En esencia, la Agencia añade al envío de comunicaciones por medio postal aquellos requisitos que la norma contiene para las comunicaciones enviadas por medios electrónicos. Esta interpretación podría resultar problemática, especialmente si se extiende a otras situaciones, pues podría implicar que el envío de comunicaciones comerciales por medios postales y sin perfilado -esto es, quizás uno de los tratamientos de datos más inocuos que se pueda llegar a imaginar- quede restringido. Por analogía, cualquier tratamiento de datos que pueda tener un impacto mayor sobre el interesado -esto es, virtualmente prácticamente cualquier tratamiento-, quedaría fuera del ámbito de aplicación del art. 6.1.f) RGPD.

A mayor abundamiento, esta misma conclusión ha sido posteriormente reiterada por la autoridad española en más de una ocasión.[428]

10.2.3. Perfilado básico[429]

En segundo lugar, la Asociación Española de Banca consulta sobre la base de legitimación aplicable cuando el tratamiento tenga por objeto analizar la solvencia de un cliente y realizar actividades de perfilado para posteriormente ofrecerle productos de financiación. Es decir, en este caso, las actividades comerciales se basan en un tratamiento de datos más exhaustivo con la finalidad de conocer la solvencia de cada persona y de personalizar la oferta de productos, por ejemplo, de crédito. En este caso será necesario diferenciar si el tratamiento se inicia a consecuencia de la solicitud de dichos productos por parte del cliente o no. En el primer caso, la base de legitimación será la necesidad para la ejecución del contrato o precontrato.

Si es la entidad quien, de forma proactiva, pretende iniciar el tratamiento para ofrecer productos no solicitados, la AEPD interpreta que, además de las limitaciones del caso anterior, el interés legítimo no podrá ser la base de legitimación en aquellos casos en los que los datos personales del cliente sean enriquecidos con información de fuentes externas a las de la propia entidad. En concreto, el informe señala que "debería excluirse de la aplicación del artículo 6.1.f) del Reglamento general de protección de datos el supuesto en que la entidad acudiera para la realización del perfilado a fuentes distintas de las que se derivasen de la relación del cliente con la entidad".[430]

---

[428] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, GABINETE JURÍDICO (2018): *Informe 0173/2018* y AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, GABINETE JURÍDICO (2017): *Informe 232/2017*.

[429] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, GABINETE JURÍDICO (2017): *Informe 0195/2017*, p. 9.

[430] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, GABINETE JURÍDICO (2017): *Informe 0195/2017*, p. 11.

Así, en su caso, y atendiendo al resto de circunstancias, únicamente se superará el juicio de ponderación si el perfilado y personalización de ofertas se realiza sobre la base de información proveniente de la misma entidad, y si se informa de manera adecuada al cliente. En otras palabras, la AEPD establece por vía interpretativa que el uso de fuentes de datos externas para enriquecer datos para realización de actividades de perfilado implica automáticamente la no superación del juicio de ponderación. Es decir, se vislumbra de nuevo una cierta tendencia a determinar de manera genérica el resultado del balance de intereses a partir de elementos que únicamente deberían ser factores a analizar en el caso concreto.

Alguien podría argumentar que la consulta realizada ya delimita el caso concreto y que, en consecuencia, la interpretación de la Agencia sobre el resultado del juicio de ponderación no es genérica sino adaptada a las circunstancias de un sector específico para actividades de tratamiento específicas y, por tanto, conforme al margen de apreciación que concede el RGPD. Sin embargo, la determinación de que la concurrencia de cualesquiera de dichos factores tan amplios -la utilización de fuentes de datos externas, la similitud de los bienes y servicios y la condición de cliente- resulta automáticamente en un juicio de ponderación desfavorable no puede considerarse sino una prohibición genérica que viene a prohibir tajantemente por vía interpretativa lo que la literalidad de la norma sí parece permitir.

De nuevo, esta misma conclusión fue reiterada con posterioridad por la Agencia.[431]

[431] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, GABINETE JURÍDICO (2018): *Informe 0173/2018*. Para elaborar su opinión, la AEPD se remite a la Opinión del GT29 sobre el interés legítimo, y en concreto a un párrafo (p.26) que indica:

"Sin embargo, esto no quiere decir que los responsables del tratamiento puedan remitirse al artículo 7, letra f), como fundamento jurídico para supervisar de manera indebida las actividades en línea y fuera de línea de sus clientes, combinar enormes cantidades de datos sobre ellos, provenientes de diferentes fuentes, que fueran inicialmente recopilados en otros contextos y con fines diferentes, y crear —y, por ejemplo, con la intermediación de corredores de datos, también comerciar con ellos— perfiles complejos de las personalidades y preferencias de los clientes sin su conocimiento, sin un mecanismo viable de oposición, por no mencionar la ausencia de un consentimiento informado. Es

10.2.4. Perfilado intensivo[432]

La Asociación de Banca plantea un tercer escenario relacionado con el uso de datos personales para la posterior realización de ofertas comerciales a sus clientes. En este supuesto, la consulta versa sobre la base de legitimación apta para el análisis de la totalidad de la información sobre movimientos y transacciones del cliente, así como la información obtenida como consecuencia del uso de los productos y servicios ya contratados por parte del cliente, todo ello para la realización de actividades de perfilado, esta vez más intensas y por tanto intrusivas, para una posterior personalización de ofertas sobre productos y servicios.

En dicho caso, la Agencia estima que la necesidad para la ejecución contractual no puede ser la base de dicho tratamiento.[433] El interés legítimo del responsable podría ser la base de legitimación sujeto a las mismas cautelas que las señaladas para el caso anterior que "deberán adoptarse incluso con una mayor precisión". Relevante es también señalar que el uso

---

probable que dicha actividad de elaboración de perfiles represente una intrusión importante en la privacidad del cliente y, cuando esto suceda, los intereses y derechos del interesado prevalecerán sobre el interés del responsable del tratamiento".

Como se observa, el GT 29 se refiere en su opinión a una actividad mucho más invasiva que la referida en el Informe de la AEPD, por cuanto comenta una situación en la que falta el deber de información al cliente, un mecanismo de oposición, así como un "consentimiento informado", que a todas luces parece referirse a la base de licitud para la recogida primera de los datos, pero no a la base que deba legitimar el tratamiento de perfilado.

Con todo, el GT29 mantiene la puerta abierta a considerar cada caso concreto cuando se expresa en términos abiertos "es probable que dicha actividad (…) representen una intrusión importante (…) y cuando esto suceda, los derechos del interesado prevalecerán". Por el contrario, la AEPD parece crear un criterio interpretativo cerrado y apriorístico con el que no terminamos de poder estar de acuerdo.

[432] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, GABINETE JURÍDICO (2017): *Informe 0195/2017*, p. 14.

[433] En realidad, en lo que debe interpretarse como un error, el informe hace referencia al art. 6.1.c) -necesidad del tratamiento para el cumplimiento de una obligación legal- donde en realidad parece referirse al art. 6.1.b) -necesidad del tratamiento para la ejecución de un contrato-. En concreto, el informe indica que "no cabría entender amparado en el artículo 6.1.c) citado el uso de estos datos y de los perfiles resultantes para la oferta de productos o servicios de terceras entidades y, evidentemente con mayor motivo, su posible cesión a entidades que presten servicios que no puedan considerarse "similares", incluso cuando se tratase de empresas del mismo grupo". AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, GABINETE JURÍDICO (2017): *Informe 0195/2017*, p. 15.

de datos históricos del cliente para la realización de las actividades de perfilado debe limitarse a lo necesario para conocer la situación actual de la persona, para lo cual la Agencia indica, a modo indiciario, un plazo no superior a un año.

Si bien es cierto que el uso de datos anteriores puede no ser beneficioso en ciertas circunstancias, ya que falsearía el perfil actual de la persona, determinado tipo de datos de mayor antigüedad que un año sí pueden ser relevantes para la determinación del perfil de la persona, más aún en relación con la capacidad de crédito y la posibilidad de impago de una persona, que únicamente puede determinarse de manera precisa analizando su comportamiento a lo largo de la duración del crédito o de la vida de los productos contratados. Ejemplo de ello puede ser un patrón repetitivo a lo largo del tiempo de falta de ingresos coincidente con los plazos máximos permitidos por la legislación para la contratación fija de un trabajador, lo que indicaría la falta de confianza de recobro del cliente.

10.2.5. *Anonimización y seudonimización para posterior analítica*[434]

Resulta interesante la cuestión de la consulta referente a la base de legitimación para llevar a cabo procesos de anonimización y agregación de datos con el objetivo de desarrollar nuevos productos y servicios. Esta práctica en realidad conlleva dos actividades de tratamiento diferentes. En primer lugar, la propia anonimización y agregación de los datos personales, y en segundo lugar, el análisis de estos para la obtención de valor y el desarrollo de nuevos productos.

De hecho, estas actividades se incluyen en las antes descritas 1-Recolección (que también incluye preparación de datos y posible anonimización o seudonimización) y Fase 2-Análisis (que incluye actividades de análisis secundario de los datos, búsqueda de información oculta como patrones y elaboración de nuevos desarrollos). En esencia,

[434] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, GABINETE JURÍDICO (2017): *Informe 0195/2017*, p. 15.

este tratamiento será la base para la posterior Fase 3, que incluye la realización del perfil de una persona específica (esto es, las actividades de perfilado a las que se referían las cuestiones previas de la consulta).

La Agencia enfatiza la necesidad de comprender la diferencia jurídica entre anonimización y seudonimización. Si bien ambos procesos conllevan un tratamiento de datos personales en primera instancia, si el resultado de la operación es un conjunto de datos verdaderamente anónimo, la normativa de protección de datos podría no ser aplicable en la segunda fase en función del riesgo de reidentificación asociado a actividades de enriquecimiento de datos y descubrimiento de nueva información. En cambio, si los datos son seudónimos, la norma seguirá siendo aplicable en la segunda fase. Así, para el caso en que lleve a cabo una anonimización completa, la Agencia interpreta que los derechos de los interesados tendrán una incidencia mínima, por lo que el interés del responsable podría vencer el juicio de ponderación. Esto es, el tratamiento de datos personales llevado a cabo para el propio proceso de anonimización podría basarse en el interés legítimo del responsable. El tratamiento posterior, en la medida en que no permita crear datos personales o reidentificar, quedaría fuera del ámbito de aplicación de la normativa de protección de datos.

Para el caso de que el tratamiento verse sobre datos seudónimos, la Agencia evita posicionarse de manera tajante, indicando que dependerá de las garantías que se adopten. De hecho, la consulta no indica si esta conclusión se refiere a ambos tratamientos -proceso de seudonimización y análisis posterior- o únicamente al segundo -análisis-. Sería razonable argumentar que la parte del tratamiento consistente en la seudonimización de datos podría basarse, casi con total seguridad, en el interés legítimo del responsable en la medida en que el objetivo es aumentar el nivel de seguridad y de protección del interesado.

Es destacable asimismo que, en línea con lo ya argumentado en páginas previas, en la evaluación de este tratamiento la AEPD incida de manera

específica en el impacto sobre los interesados como factor del balance de intereses.

10.2.6. Prevención del fraude[435]

Asimismo, la consulta realizada se refería al tratamiento de datos con la finalidad de prevención del fraude, bien intragrupo o entre compañías de ajenas al grupo empresarial. De hecho, recordemos que la prevención del fraude se encuentra entre los supuestos expresamente mencionados en el RGPD como posible interés legítimo, y así lo reitera la Agencia indicando por tanto que, en tanto existan indicios de fraude, tendrá legitimación con base en el art. 6.1.f) RGPD el tratamiento consistente en la comunicación de datos entre las compañías emisora y receptora de la cuantía económica. En cuanto a la creación de sistemas sectoriales multigrupo de intercambio de información con finalidades de prevención del fraude, la Agencia señala que el interés legítimo también podría constituir la base del tratamiento dependiendo de las circunstancias del caso concreto.

Esta respuesta, dada en sentido amplio, y en consonancia con todo lo anterior parece indicar que sería posible para una entidad llevar a cabo el siguiente planteamiento. Una entidad puede realizar un proceso de anonimización de datos sobre su interés legítimo, para posteriormente llevar a cabo actividades de análisis de datos masivo con el objetivo de detectar qué tipo de conductas son indicativas de fraude. Por último, los datos de una persona concreta pueden ser tratados, también sobre el interés legítimo de la entidad, para detectar en tiempo real dichas conductas y considerar cuándo actuar y recabar mayor información en caso de alarma. En el caso de que este proceso se produzca con datos seudónimos, la entidad deberá desplegar medidas y garantías suficientes para vencer el juicio de ponderación, aunque la Agencia no descarta de forma automática la licitud del tratamiento.

[435] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, GABINETE JURÍDICO (2017): *Informe 0195/2017*, p. 12.

10.2.7. Actualización de datos

Por último, la consulta responde a la cuestión en torno a la legitimación para actualizar datos previamente facilitados por el interesado. Tras reconocer el valor del principio de exactitud de los datos establecido en el art. 5.1.d RGPD, la Agencia apunta ciertos factores que deberán tomarse en cuenta en el juicio de ponderación para la posible aplicación de la base del interés legítimo, entre los que se encuentran el tipo de datos a actualizar (por ejemplo, datos necesarios para la óptima relación contractual con el interesado o datos accesorios útiles pero no necesarios para mejorar el perfil del interesado); y el tipo de fuentes de datos que se utilizarán para actualizar los datos (su naturaleza, si la información proviene directamente del interesado o un tercero, la existencia de una habilitación legal, etc.).

10.2.8. Extrayendo algunas reflexiones de la postura de la AEPD

El análisis de este informe permite observar que la AEPD acoge con facilidad el argumento del uso del interés legítimo, por ejemplo, con las finalidades de prevención del fraude o la realización de procesos de anonimización o, con garantías, de seudonimización. Por el contrario, el informe se posiciona en contra de la posibilidad de considerar que el ejercicio de ponderación pueda resultar favorable al uso del interés legítimo para determinadas finalidades comerciales, especialmente en las que se realice un perfilado de los clientes de una entidad bancaria a partir de datos enriquecidos con información proveniente de fuentes accesorias y diferentes de los datos derivados de la relación directa del cliente con la entidad.

Es decir, además de lo ya visto, a la luz de los precedentes sobre la aplicación del interés legítimo, parece que *de facto* su uso se relega a situaciones concretas como prevención del fraude. A pesar de que el RGPD mencione expresamente la mercadotecnia como ejemplo de posible interés legítimo, la interpretación dada por nuestra autoridad de control es muy restrictiva, hasta el punto de llegar a imponer requisitos adicionales, cuya

falta de cumplimiento, parece darse a entender, será interpretada en el sentido de significar automáticamente un resultado negativo del juicio de ponderación, incluso en aquellos casos más inocuos como el envío de comunicaciones comerciales por medios postales sin previo perfilado del interesado.

En esencia, parece entreverse un propósito más profundo en el posicionamiento de la AEPD. Los casos en los que se muestra más combativa contra el interés legítimo son precisamente aquellos en los que el responsable desea llevar a cabo un tratamiento de datos con finalidades comerciales y de lucro económico. Habiendo analizado la concepción histórico-cultural en torno a las bases jurídicas del tratamiento y conociendo el escenario actual de economía digital basada en datos, podemos concluir que el motivo que impulsa a la AEPD es buscar un medio de protección de los ciudadanos, susceptibles de sufrir las consecuencias negativas del tratamiento de sus datos personales frente a la actuación invasiva de entidades movidas por un ánimo de lucro insaciable. Para ello, la autoridad es contundente: el medio preferente es el consentimiento del interesado acompañado de una fuerte limitación del margen de apreciación del responsable que actúa sobre su interés legítimo.

Sin embargo, ya ha sido aquí ampliamente argumentado que, en dicho ecosistema, dejar al interesado al designio de sus supuestas decisiones informadas y autónomas es una utopía. El medio elegido por la AEPD para garantizar la protección de los ciudadanos podría haber quedado desbordado por el cambio tecnológico. Parece que aún existe cierta reticencia a abrirse a considerar el pleno potencial del interés legítimo como base del tratamiento que pueda aportar protección a los ciudadanos digitales y resolver algunas de las limitaciones detectadas.

En todo caso, también debe tenerse en cuenta el contexto de la resolución. En primer lugar, fechada en 2017, esto es, muy temprana. Recordemos que en 2017 el RGPD aún no era totalmente aplicable. En consecuencia, sería plausible argumentar que no se hubiera producido un cambio cultural o de

concepción con respecto a las posibilidades de utilización del interés legítimo que pueden surgir del RGPD en su aplicación en entornos de análisis complejos de datos masivos. Sin embargo, bien es cierto que parte de sus conclusiones han sido repetidas con posterioridad en lo que parece ser una cristalización de criterio interpretativo. En segundo lugar, es importante no olvidar la herencia de la corriente de pensamiento española, que como ha sido analizado, está muy fuertemente ligada a la consideración del consentimiento como la regla general para el tratamiento de datos personales y la base de legitimación más garantista con los intereses y derechos de los ciudadanos. Sin embargo, las posturas e interpretaciones adoptadas por la AEPD gozan de especial trascendencia, pues la autoridad de control española es muy tenida en cuenta tanto en Europa como en Iberoamérica.[436]

En este sentido, en nuestra opinión, sería de gran utilidad mantener la mente abierta hacia el interés legítimo como base de licitud que, aplicada de manera estricta, pueda solventar los problemas ya expuestos con el consentimiento. Para ello, el paso del tiempo, la previsible actualización de las Directrices del CEPD sobre el interés legítimo y la necesaria coordinación entre autoridades de control de todos los Estados miembro pueda llevar a un paulatino cambio de percepción sobre el art. 6.1.f) RGPD.

10.3. La Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales

Recapitulemos algunas de las ideas principales expuestas hasta este momento. Hasta ahora hemos analizado la aproximación al interés legítimo como base jurídica para el tratamiento de datos personales en las normas españolas previas a la actual, y por tanto ya derogadas. También hemos analizado la respuesta a la consulta de la banca, que siendo previa a la norma española actual, se analiza ya bajo los parámetros del RGPD y tiene

[436] PIÑAR MAÑAS, José Luís (2005): "El derecho fundamental a la protección de datos personales. Algunos retos de presente y futuro", en Asamblea: revista parlamentaria de la Asamblea de Madrid, No. 13, págs. 21-46.

especial interés al referirse a la base de legitimación en relación con diversos tratamientos de datos masivos.

En este epígrafe analizaremos cómo ha quedado regulado el interés legítimo como base del tratamiento en la norma actual de protección de datos española, que viene a adaptar a nuestro ordenamiento jurídico lo dispuesto en el RGPD, la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales[437] (LOPDgdd). El proceso legislativo y el contenido final de la norma en este extremo tienen ciertas particularidades de interés.

Se trata de un hecho innegable que en los últimos años hemos atestiguado un incremento de las críticas al consentimiento, en los términos analizados en el capítulo anterior. La principal consecuencia de ello fue el reforzamiento de los requisitos para su validez que trajo el RGPD.

Esto ha desencadenado, de manera subsecuente, la consecuencia de que muchos tratamientos antes basados en el consentimiento ahora no encuentren amparo en esta base, de modo que los responsables del tratamiento se han visto en la posición de abrirse a la posibilidad de utilizar otras bases de legitimación más apropiadas. En el sector privado, las principales alternativas al consentimiento son la necesidad para la ejecución de un contrato o precontrato y el interés legítimo del responsable. En concreto, y por lo que aquí interesa, cabe destacar, por tanto, la creciente atención en el interés legítimo.

10.3.1. *Anteproyecto de Ley Orgánica*

En una muestra de apertura hacia la figura del interés legítimo, el anteproyecto de LOPDgdd[438] incluía, en su art. 9 la posibilidad de que una

[437] Sobre la incorporación de un catálogo de derechos digitales en la LOPDgdd ver RALLO LOMBARTE, Artemi (2020): "Una nueva generación de derechos digitales", en *Revista de estudios políticos*, No. 187

[438] Para mayor detalle sobre el proceso de tramitación parlamentaria de esta Ley Orgánica ver TRONCOSO REIGADA, Antonio (2019): "La Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales", en *Derecom*, No. 26.

ley futura pudiera habilitar tratamientos de datos personales basados en interés legítimo. Es decir, el anteproyecto se abría a la posibilidad de que una norma futura con rango de ley dictara, con carácter general, la presunción de prevalencia de un determinado interés del responsable o un tercero, y que, en dichos casos, la ley pudiera establecer la obligación del responsable de adoptar garantías adicionales. Asimismo, reconocía la posibilidad de que el interés legítimo pudiera ser la base de licitud del tratamiento aun en aquellos otros casos no habilitados por una norma legal.

En relación con esta previsión, la AEPD manifestó, en su informe sobre el anteproyecto de LOPDgdd, que con este precepto se pretendía dar solución a diversos casos asiduos en los que no existe una obligación legal de tratamiento de los datos, ni se pueden entender realizados en misión de interés público. En dichos casos, clarifica la AEPD, los responsables estarían exentos de realizar la ponderación de intereses. En realidad, el precepto parecía permitir que el responsable estuviera también eximido de llevar a cabo las demás fases de la evaluación de interés legítimo -identificación del interés, argumentación de la legitimidad, análisis de los intereses, derechos y libertades fundamentales de los interesados-, pues ello ya estaría implícito en la habilitación legal. El objetivo de ello sería aportar seguridad jurídica.

10.3.2. *Toque de atención del Consejo de Estado*

No obstante, el Consejo de Estado se opuso a este extremo[439] y abogó por eliminar esta referencia contenida en el art. 9, con base en diversos motivos. El primero, por considerar que el anteproyecto sobrepasaba el margen de actuación que el RGPD concede a los Estados miembros, que no incluye la posibilidad de que un Estado miembro pueda desarrollar o concretar el contenido del art. 6.1.f) RGPD (que sí se permite expresamente

[439] Consejo de Estado, Dictamen sobre el Anteproyecto de Ley Orgánica de Protección de Datos de Carácter Personal, número de expediente 57/2017, de 26 de octubre de 2017. Disponible en: https://www.boe.es/buscar/doc.php?id=CE-D-2017-757.

para otras bases jurídicas), ni de imponer por vía normativa exigencias adicionales que modifiquen el alcance de esta base de licitud.

El segundo motivo, por considerar que el hecho de permitir que el legislador lleve a cabo la ponderación de intereses y establezca su resultado con carácter definitivo, sin permitir tener en cuenta las circunstancias del caso concreto, viciaría el rigor del art. 6.1.f) RGPD. A este hecho se añadiría, además, la facultad que confería el anteproyecto para incluir nuevas obligaciones y garantías. De hecho, el Consejo de Estado recuerda que el TJUE se ha pronunciado en más de una ocasión en este sentido, precisamente una de ellas en relación con la norma española anterior, la LOPD (los ya más que mencionados asuntos acumulados ASNEF y FECEMD). Asimismo, el Consejo de Estado alegaba que el margen de apreciación de los Estados miembros bajo un Reglamento es más estrecho que bajo una Directiva y la postura española provocaría fragmentación del marco normativo europeo, siendo que la armonización y la libre circulación de datos son la finalidad última del RGPD.

Por todo ello, el informe concluye que "aunque sea en aras a una siempre deseable mayor seguridad jurídica, por tanto, ha de concluirse el legislador español no puede sustituir con supuestos legalmente tasados la flexibilidad que el legislador comunitario ha querido en apariencia atribuir a la aplicación del artículo 6.1.f) del Reglamento general".

Recuperando las palabras de Rallo, el legislador nacional, en su función de adaptación del RGPD al ordenamiento nacional debe limitarse a adoptar las previsiones a las que obligue el RGPD con vocación de uniformidad en todo el territorio comunitario.[440] Pues bien, en nuestra opinión, la postura del Consejo de Estado fue acertada por cuanto la regulación del interés legítimo en el borrador normativo trascendía la mera adaptación del RGPD.

Sin embargo, el Consejo de Estado se hizo consciente de la necesidad de dar solución a los casos que pretendía facilitar la propuesta del

[440] RALLO LOMBARTE, Artemi (2029): "El nuevo derecho a la protección de datos", en Revista española de derecho constitucional, No. 116.

anteproyecto, sugiriendo una solución alternativa, que fue la finalmente adoptada en la Ley Orgánica. Se trata de introducir, a través de normas con rango de ley, la posibilidad de que en determinados casos puntuales se pueda establecer una presunción *iuris tantum* favorable a la prevalencia del interés legítimo del responsable del tratamiento cuando se cumplan determinados requisitos o condiciones.

En este caldo de cultivo ha de interpretarse la nueva Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDgdd), que ha adaptado el RGPD al ordenamiento jurídico nacional.

10.3.3. *Presunciones de prevalencia del interés legítimo*

La nueva LOPDgdd hace alusión al término de interés legítimo en contadas ocasiones. En concreto, el Título IV contiene disposiciones aplicables a tratamientos concretos, algunos de cuales gozan de una presunción *iuris tantum* de prevalencia de interés legítimo. Se trata de los siguientes casos.

En primer lugar, el tratamiento de datos de contacto profesionales (art. 19), en la medida en que los datos sean tratados únicamente con la finalidad de iniciar una relación profesional y no personal. Este supuesto es sencillo y no desencadena mayores riesgos.

En segundo lugar, se presumirá la prevalencia de interés legítimo para tratar datos en relación con sistemas de información crediticia (art. 20) en caso de incumplimiento de obligaciones dinerarias o de crédito. La inclusión de datos personales en ficheros de morosidad ha sido ampliamente abordada por la AEPD en los últimos años y el objetivo de este precepto es facilitar el tratamiento, siempre sujeto a una serie de requisitos cumulativos, tales como que los datos hayan sido aportados por el acreedor, que la deuda sea cierta, vencida, exigible y no disputada, o que únicamente ciertas personas puedan tener acceso a los datos. En concreto, se trata de aquellos que mantengan una relación contractual o hayan iniciado acciones pre-contractuales con el deudor en relación con un contrato de financiación, pago aplazado o similares. Es decir, parece que en este caso el art. 20

LOPDgdd presume no solo un interés legítimo del acreedor de comunicar los datos de un deudor para su inclusión en un fichero, sino también el interés legítimo de un tercero para acceder a ellos.

En tercer lugar, la norma española establece una presunción de interés legítimo y por tanto de licitud del tratamiento en tratamientos relacionados con determinadas operaciones mercantiles (art. 21). Este precepto podría legitimar el acceso a datos personales en el contexto de una adquisición o fusión con la finalidad, por ejemplo, de analizar la situación legal de una organización, calcular su valor, etc. En todo caso, si la operación mercantil no se concluye, el responsable cesionario debe suprimir los datos sin excepción. De este modo, por ejemplo, el acceso a una base de datos con motivo de una posible fusión de empresas no podría justificar en ningún caso que dichos datos se utilizasen para enriquecer la base de datos del cesionario, ni siquiera para anonimizar los datos y posteriormente utilizarlos para operaciones de analítica, perfilado, envío de comunicaciones comerciales, venta de bases de datos, ni ninguna otra finalidad. En este caso surge una duda relevante: ¿qué sucede con el acceso a datos resultantes de un proceso de inferencia, cuya consideración de datos personales no es clara? ¿Existe una obligación clara del cesionario de eliminar dichos datos y no utilizarlos para ninguna otra finalidad?

En todo caso, tal y como dispone el preámbulo de la norma, esta lista de presunciones de interés legítimo es meramente ejemplificativa y no exhaustiva. Asimismo, la presunción de licitud no elimina la obligación de los responsables de cumplir con el resto de obligaciones impuestas por el RGPD y la propia LOPDgdd. Por último, la no concurrencia de los requisitos que establecen los artículos no obsta para que el tratamiento de dichos datos personales pueda basarse en el interés legítimo, pero en tales casos no existirá una presunción favorable y por tanto el responsable deberá llevar a cabo el ejercicio de ponderación.

10.3.4. Interés legítimo de terceros para responsables del sector público

En otro orden de cosas, la disposición adicional décima se refiere a otro caso de uso de interés legítimo (si bien en este caso no se trata de una presunción de prevalencia, como los casos anteriores). La DA 10ª se refiere a determinadas categorías de responsables, aquellos enumerados en el art. 77.1 LOPDgdd, que son en esencia responsables del sector público tales como órganos jurisdiccionales, órganos administrativos, Universidades públicas o grupos parlamentarios. Estos responsables podrán comunicar datos personales que les sean solicitados por sujetos de derecho privado cuando cuenten con el consentimiento del interesado o aprecien que concurre en los solicitantes un interés legítimo que prevalezca. Esto es, determinadas categorías de responsables del sector público pueden utilizar como base de licitud el interés legítimo de un tercero privado para conceder acceso a información, en lo que parece una ponderación entre la protección de datos personales y la transparencia o el acceso a documentos. Es cierto que este conflicto de derechos es uno de los más comunes en lo que respecta el tratamiento de datos personales por parte de entes públicos, y que por tanto necesita solución. Se trata así de una de las circunstancias en las que un ente público puede actuar sobre el interés legítimo, que tiene prohibido por lo demás hacerlo cuando actúe en el ejercicio de sus funciones.[441] Destaca sin embargo la amplitud de la determinación de esta disposición, especialmente frente a las estrictas interpretaciones que se imponen cuando es un ente de derecho privado quien desea actuar sobre el interés legítimo.

10.4. Conclusiones

La normativa española y su aplicación se ha caracterizado históricamente por una postura combativa respecto a la figura del interés legítimo para el tratamiento de datos personales. Esta postura se ha caracterizado, no solo

[441] Art. 6.1.f), párrafo segundo RGPD.

por una interpretación estricta sobre los supuestos en los que esta puede ser la base de licitud del tratamiento más adecuada conforme a la normativa de protección de datos personales, sino por la creación de restricciones y prohibiciones que trascienden lo establecido en las normas comunitarias, de las que derivan las normas nacionales. Parece, además, que la postura de la Agencia hacia la posibilidad de basar tratamientos big data en interés legítimo es también restrictiva, tal y como se desprende de sus conclusiones aportadas en respuesta a La Consulta remitida por diversos representantes del sector bancario. Así, parece que lo que debiera ser una base jurídica que necesita ser aplicada con cautela pero que tiene potencial para ofrecer soluciones a algunos de los principales límites subyacentes en otras bases de licitud, en concreto para entornos tecnológicamente complejos, puede convertirse en una base de legitimación excepcional aplicada únicamente en casos tan concretos que se asemejan a una lista taxativa.

Los casos tasados por la actual LOPDgdd como presunciones de interés legítimo son relativamente básicos en el sentido de tratarse de casos de acceso a determinada información, (datos de contacto profesional, ficheros de morosos o datos empresariales previo a una compra). Por otro lado, la AEPD parece mostrarse favorable a tratamientos de perfilado únicamente cuando se trate de procesos básicos, que parecen no incluir procesos analíticos con tecnologías de datos masivos.

En el contexto español, y debido a lo todo lo ya analizado, el desarrollo tecnológico puede suponer un choque contra la idea férrea de la supremacía del consentimiento que encumbró la LOPD, en ocasiones diferente a la práctica de otros Estados miembros, más asiduos en el uso de otras bases de licitud como el interés legítimo.

Este hecho puede intuirse trasladado al del ciudadano medio, pues la apreciación de la opinión pública deja entrever que existe un nivel escaso de comprensión y aceptación de que existen situaciones plenamente

legítimas y lícitas en las que los datos puedan ser tratados sin el consentimiento del ciudadano.

La evolución digital justifica abrirse a considerar que una base de licitud flexible y, por qué no, ambigua, pueda ser utilizada en tratamientos que impliquen el uso de tecnologías más avanzadas. En la medida en que ello pueda suponer un mayor beneficio y también un mayor riesgo, no debemos obviar que las garantías y la precaución deben también extremarse. Esta circunstancia también puede dar lugar a un riesgo de fragmentación normativa por vía interpretativa y de inseguridad jurídica en relación con otros Estados miembros que puedan estar más abiertos a aplicar el interés legítimo como base jurídica para el tratamiento de datos en relación con la utilización de tecnologías big data o la realización de actividades como, por ejemplo, elaboración de perfiles. Asimismo, el hecho de que el instrumento jurídico del RGPD sea la figura de un Reglamento, en contraposición a una Directiva, obliga a los Estados miembros a alcanzar una mayor armonización. Por ello, es razonable argumentar que España debe hacer un esfuerzo por no anclarse en una postura férrea. Todo ello no obsta, sin embargo, para que un Estado miembro no pueda ejercer un cierto margen de actuación o intervención mediante su Derecho nacional -eso sí, significativamente más restringido que en el caso de transposición de una Directiva-.

En cualquier caso, es posiblemente pronto para poder anticipar las consecuencias de este escenario. Por un lado, es previsible que, de producirse un cambio de postura en la autoridad de control española o incluso entre los profesionales de la protección de datos, este necesite tiempo. Ciertamente, un cambio de cultura y quehacer jurídico de este calibre no se acomete con rapidez. Por otro lado, también es pronto aún para conocer en detalle la postura de las autoridades de control de otros Estados miembros en materias que se refieren a la aplicación práctica de tecnologías recientes con respecto a un cuerpo normativo nuevo, como es el RGPD, a pesar de que lo relativo concretamente al interés legítimo se haya mantenido prácticamente inalterado. Como último resorte, la

jurisprudencia del TJUE puede resultar en pautas a través de las cuales las opiniones de diferentes Estados miembros se armonicen, aunque esta vía toma años y por tanto no es capaz de generar respuestas inmediatas a los retos actuales

11. Interés legítimo y otras garantías del RGPD. Buenos compañeros de viaje

El interés legítimo parece una base de legitimación perfectamente alineada con el espíritu del RGPD y con muchas de sus disposiciones más relevantes, principalmente en relación con el tratamiento de datos personales a través de tecnologías cada vez más avanzadas. Por este motivo, si hace unos años podría ser impensable justificar en un interés legítimo tratamientos que hiciesen un uso cada vez más intenso de tecnologías de datos masivos, esta posibilidad se abre como nueva en la actualidad.

Los principales elementos del RGPD que se encuentran alineados con la figura del art. 6.1.f) RGPD en este contexto son las siguientes.

11.1. Flexibilidad

Como ya se expuso en la parte introductoria de este capítulo, el interés legítimo es una de las bases de legitimación del tratamiento de datos personales más flexibles. Esto es con frecuencia utilizado como argumento contra la eficacia de esta base. En concreto, se alega que dicha flexibilidad puede ser utilizada para vestir de lícito un tratamiento que en realidad no lo es.[442] No obstante, la flexibilidad no hace sino aportar una mayor capacidad

[442] Véase la respetable, aunque no compartida opinión: "No podemos negar que el recurso al interés legítimo por parte del responsable es una opción poco aconsejable y a la que recurrimos en este análisis como posible vía de convalidación de consentimientos perfectamente legítimos y documentados conforme la LOPD pero que, por su tipología, no alcanzan los estándares que el Reglamento establecen". LLANEZA, Paloma (2019): "La adaptación de los consentimientos tácitos y presuntos: el uso del interés legítimo", en Javier López Calvo (coord.), *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD*. Madrid, Wolters Kluwer, p. 1136-1137.

-y deber- al responsable de actuar conforme sea requerido en función de las circunstancias del caso concreto.

Esta misma flexibilidad ha sido también incorporada en otras disposiciones del RGPD, y, de hecho, alabada. Ejemplos de ello son la obligación de realizar una evaluación de impacto, que deben realizarse "cuando sea probable que un tipo de tratamiento entrañe un alto riesgo",[443] el establecimiento de las medidas de seguridad, que deben ser "apropiadas" al riesgo,[444] o la aprobación de normas corporativas vinculantes, cuya determinación es eminentemente abierta.

Así, la flexibilidad, que subyace en el espíritu del RGPD, no ha de ser vista como maleabilidad, en el sentido de poder ser manejada al capricho de cualquier fin. Al contrario, ha de ser vista como adaptabilidad, en el sentido de permitir dejar atrás obligaciones encorsetadas incapaces de solucionar problemas o hacer frente a riesgos novedosos.[445] Ya señaló Rodotà el problema de tener cada vez más y peores normas, y abogaba por un Derecho más flexible que no pretendiera regular todo, el no-Derecho.[446]

Asimismo, la flexibilidad ha de ser vista como una oportunidad del responsable de demostrar madurez en el tratamiento de datos personales, especialmente cuando hace uso de nuevas tecnologías.

En conclusión, nos encontramos ante una realidad acelerada, diversa e impredecible que requiere de soluciones flexibles para no paralizar el

[443] Art. 35 RGPD.

[444] Art. 32 RGPD.

[445] Y señalaba Pablo García Mexía, recogiendo las reflexiones de Villoria Mendieta que "En cuanto al Derecho, no es necesario enmarañarlo (¿más de lo que ya está?) con normas excesivamente numerosas (por abrumadoramente casuísticas) e ineficaces (en tanto que ignorantes de la realidad social a que han de aplicarse)". "Podrán obtenerse resultados notoriamente más satisfactorios mediante la simple interpretación «éticamente sensible» de los preceptos jurídicos existentes, muy singularmente de los constitucionales". GARCÍA MEXÍA, Pablo Luís (2001): "La ética pública: Perspectivas actuales", en Revista de Estudios Políticos, No. 114, p. 131-168; MENDIETA, Manuel Villoria (2000): *Ética pública y corrupción: Curso de ética administrativa*, Tecnos-Universitat Pompeu Fabra, Madrid, 2000, p. 175-188.

[446] RODOTÀ, Stefano (2010): *La vida y las reglas. Entre el Derecho y el no Derecho*, Madrid, Trotta.

funcionamiento del sistema. Tan flexibles, por otro lado, como los nuevos tratamientos que se vislumbran.

11.2. Responsabilidad proactiva

El RGPD ha introducido en el art. 5.2, por primera vez, el principio de responsabilidad proactiva, o al menos, de forma expresa.[447] Este principio conlleva la obligación del responsable de cumplir con todos los principios del tratamiento expresados en el primer apartado del artículo, así como de demostrar dicho cumplimiento. La tendencia a impulsar este principio de responsabilidad "aumentada" será una de las claves para el futuro de la protección de la persona.[448]

El principio de responsabilidad proactiva fue ya motivo de análisis por parte del GT 29 años antes de la reforma llevada a cabo por el RGPD, y ya en ese momento se perfilaron los dos elementos básicos que lo conforman.[449]En primer lugar, la necesidad de que el responsable tome medidas adecuadas para el cumplimiento de las obligaciones de protección de datos, que no deben ser concretadas *a priori* y, de hecho, es positivo que así sea. Entre las medidas adecuadas que el GT 29 recomendaba a modo de ejemplo, ya en 2010, se encontraba la de implementar procedimientos internos previos a nuevos tratamientos de datos personales. Esta medida tiene un encaje directo con la reutilización de la información que caracteriza el avance de las tecnologías big data. En

[447] Sin embargo, no se trata de un principio propiamente novedoso. La Directiva 95/46 ya contenía, en el art. 6.2 las bases de este principio, al establecer la obligación del responsable de cumplir con los principios de calidad de los datos consagrados en su apartado primero, así como mecanismos de depuración de responsabilidad del responsable, tales como la capacidad de la autoridad de control independiente para imponer sanciones por incumplimiento de la Directiva. Asimismo, existen precedentes del principio de responsabilidad proactiva en el ámbito de la protección de datos y la defensa de la privacidad, tales como las Directrices de la OECD sobre protección de la privacidad y flujos transfronterizos de datos personales de 1980, que contiene en su apartado 14 el "*accountability principle*".

[448] RECIO GAYO, Miguel (2017): "Big data: hacia la protección de datos personales basada en una transparencia y responsabilidad aumentadas", en *Revista de Derecho, Comunicaciones y Nuevas Tecnologías, Universidad de Los Andes (Colombia)*, No. 17.

[449] GRUPO DE TRABAJO DEL ARTÍCULO 29 (2010): *Dictamen 3/2010 sobre el principio de responsabilidad* (WP 173), de 13 de julio.

segundo lugar, el principio de responsabilidad proactiva conlleva la necesidad del responsable de demostrar el cumplimiento de sus obligaciones y de la efectiva implementación de aquellas medias que fueron consideradas adecuadas y pertinentes.

En este sentido ya se expresaban también Mayer-Schönberger y Cukier al indicar que "tenemos que proteger la privacidad desplazando la responsabilidad de los individuos hacia los usuarios de datos: es decir que rindan cuentas por su uso".[450]

Se trata de un concepto abierto y laxo, que por ello, está abierto a interpretaciones e incluso problemas de traducción. En cualquier caso, parece que la metodología necesaria para desplegar el art. 6.1.f) RGPD tiene buen encaje con el sistema de protección que despliega el principio de responsabilidad proactiva, y de hecho, pone el énfasis en la asunción de responsabilidades por parte de la organización, aliviando la carga que el interesado asume cuando presta su consentimiento.

La introducción de este principio de responsabilidad proactiva -de manera conjunta con los principios de lealtad y de transparencia-[451] puede interpretarse, en relación con la aplicación del art. 6.1.f) RGPD en el sentido de que eleva el umbral de responsabilidad del responsable del tratamiento para demostrar la existencia de dicho interés legítimo y su validez como base del tratamiento a lo largo del tiempo. [452]

[450] MAYER-SCHÖENBERGER, Viktor; NEIL CUKIER, Kenneth (2013): *Big Data. La revolución de los datos masivos*, 1ª ed., Turner Publicaciones, p. 236.

[451] El principio de transparencia debe entenderse, por su parte, en consonancia con los arts. 13.1.c) y d y art. 14.1.c) y 2.b) RGPD.

[452] En relación con el umbral de responsabilidad bajo el RGPD, Piñar Mañas ha señalado que "En mi opinión el nuevo modelo no es en absoluto más sencillo que el anterior. De entrada, las reglas del juego son más uniformes a nivel de la Unión Europea, pero al mismo tiempo se deja mayor margen de apreciación y valoración a los responsables y encargados. La falsa idea de que es suficiente el cumplimiento formal de las obligaciones que fijan la ley y el reglamento ha de quedar definitivamente superada. (…) A partir de ahora será necesario adoptar decisiones propias en función de los tratamientos de datos que se lleven cabo y de la naturaleza de éstos". PIÑAR MAÑAS, José Luís (2016): "El objeto del Reglamento", en José Luís Piñar Mañas (dir.), Reglamento General de Protección de Datos: Hacia un nuevo modelo europeo de privacidad, Madrid, Reus.

Otra manifestación de una necesaria combinación de estos principios es la obligación del responsable de informar de cuál es la base de legitimación del tratamiento y que documentar los tres pasos de la evaluación del interés legítimo (cuáles son dichos intereses, por qué son necesarios y el juicio de ponderación con los intereses, derechos y libertades de los interesados). A pesar de la falta de obligación explícita de publicar esta información, el mero deber de probar la realización de estos pasos crea una prueba documental que podrá ser revisada en cualquier momento posterior por la autoridad de control o los tribunales, de modo que el responsable queda vinculado a sus propias conclusiones.

En resumen, lo que consagra este principio no es sino el axioma de que aquel responsable que desee hacer un uso -siempre legítimo- de datos personales y obtener cualquier suerte de beneficio, máxime si es mayoritariamente propio y no común, debe asimismo asumir las posibles consecuencias del tratamiento.

11.3. Enfoque basado en riesgos

El interés legítimo respeta a la perfección el enfoque basado en riesgos que exalta el RGPD, en la medida en que uno de los factores principales para determinar su validez sea, como aquí ha sido propuesto, el impacto del tratamiento sobre los interesados.

En relación con ello, realizar un mapa de datos, una de las actividades principales para poder llevar a cabo un efectivo análisis de riesgos, puede servir también de gran ayuda para el responsable en su labor de comprender todos los aspectos del tratamiento y su posible influencia sobre sus intereses y aquellos de los interesados.

11.4. Vuelta a las raíces. Principio general del derecho

Lo anterior puede leerse bajo la luz del principio general del Derecho "*ubi commodum, ibi et periculum*", que viene a significar que aquél que obtiene el beneficio de una actividad debe asumir también el riesgo de la misma.

Este principio ha sido invocado por Jorge García Herrero precisamente en materia de protección de datos personales y seguridad del tratamiento.[453]

No obstante, sus raíces se retrotraen al sistema de atribución de responsabilidad cuasiobjetiva sentada en nuestro Código Civil[454] y desarrollado por la jurisprudencia[455] en la ampliamente utilizada doctrina del riesgo. Esta doctrina, resumida en la apelación "aquél que provoca un riesgo que le reporta un beneficio, debe asumir la responsabilidad de los daños causados" tuvo un amplio impulso en el desarrollo de la responsabilidad civil en materia de circulación de automóviles en la medida en que el avance de la técnica y la transformación de los medios de locomoción incrementaron el riesgo de la conducción y, por tanto, la necesidad de atribuir responsabilidad.[456]

Es decir, nuestro Derecho ya cuenta, desde hace décadas, de mecanismos por los que, cuando el desarrollo de la tecnología incrementa el riesgo de una actividad, el máximo beneficiado debe responder de dichos riesgos. En el caso de la aplicación de la teoría del riesgo a la responsabilidad automovilística, una de las consecuencias básicas fue la consiguiente obligación de indemnizar a quien viera materializado un daño en relación con el riesgo y al consiguiente desarrollo del derecho asegurador.

En materia de protección de datos personales, el responsable lo es por el mero hecho de infringir la normativa, sin necesidad de que el daño sobre el interesado llegue a materializarse. Por ese mismo motivo, el interesado tampoco adquiere automáticamente un derecho a ser indemnizado.

Por su parte, esta doctrina pierde utilidad en aquellos casos en los que la actividad sea totalmente inocua, en cuyo caso, la teoría de la asignación de

[453] GARCÍA HERRERO, Jorge (2016): "Responsabilidad por Ciberataques: ¿Quién Pagará el Pato?", en Jorge García Herrero Blog.

[454] Art. 1902 del Código Civil español.

[455] Tribunal Supremo, sentencia de 10 de julio de 1943.

[456] Para un análisis en mayor detalle de este principio en doctrina jurisprudencial española, véase DOMINGO MONFORTE, José; et al (2013): "Evolución y socialización del riesgo. Compás legislativo", en *Revista INESE*, No. 7.

responsabilidad cuasiobjetiva deriva en la asignación de responsabilidad cuando existe dolo o imprudencia. En relación con tratamientos complejos de datos personales a través de tecnologías big data, puede afirmarse, casi con absoluta certeza, que siempre existirá un riesgo. A pesar de ello, la mera imprudencia -y por supuesto la voluntad dolosa- también pueden encontrar castigo en las normas de protección de datos. Un ejemplo de ello es la selección de encargados del tratamiento sin haber comprobado previamente su capacidad para dar cumplimiento al RGPD.

11.5. Evaluaciones de impacto

Por otro lado, el interés legítimo como base del tratamiento está en consonancia con la obligación el responsable de llevar a cabo una evaluación de impacto en determinadas circunstancias, concretamente, cuando sea probable que el tratamiento entrañe un riesgo alto para los interesados, especialmente cuando se utilicen nuevas tecnologías (art. 35 RGPD). En particular, la realización de una evaluación de impacto debe ser previa al inicio del tratamiento y es obligatoria cuando se llevan a cabo ciertos tratamientos que implican una evaluación exhaustiva y automatizada de los interesados, tratamientos a gran escala de categorías especiales de datos, etc.[457]

Quizás el precedente más claro del art. 35 RGPD se encuentre en las evaluaciones de impacto medioambiental, con la diferencia de que, en materia de protección de datos el centro del análisis es el impacto sobre los individuos (libertad de expresión, privacidad, no-discriminación, etc.).[458] En caso de que el resultado de la evaluación de impacto muestre un riesgo para los derechos de los individuos, deben establecerse medidas de salvaguarda orientadas, no solo a reducir el riesgo, sino a minimizarlo.

[457] Véase la metodología propuesta por la AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (2019): *Guía práctica para las evaluaciones de impacto en la protección de los datos sujetas al RGPD*.

[458] ZANFIR, Gabriela (2019): "10 reasons why the RGPD is the opposite of a 'notice and consent' type of law", en *Medium Blog*.

Tal y como adelantamos previamente, la evaluación del interés legítimo puede ser vista como una evaluación de impacto simplificada. De hecho, será de gran ayuda para identificar situaciones en las que sea necesaria la realización de una evaluación de impacto completa, y servirá de punto de partida en la identificación de los riesgos y medidas mitigadoras.

En el contexto de uso de tecnologías de datos masivos, la complejidad del proceso puede conllevar que el contenido de la evaluación del interés legítimo se asimile más a aquel de una evaluación de impacto. De igual modo, la evaluación de impacto de protección de datos y la evaluación de interés legítimo deben ser realizadas con la intención real de detectar y mitigar riesgos, y no ser un mero documento de cumplimiento normativo vacío de significado real.

En este sentido, ambas evaluaciones comparten una misma limitación: la falta de publicidad de sus resultados y de los factores que se han tomado en consideración.

11.6. Determinación de garantías adecuadas

El RGPD hace referencia en múltiples ocasiones repartidas a lo largo de todo el texto, al concepto de garantías adecuadas. Únicamente en contadas ocasiones se refiere a medidas adecuadas “y específicas”.

Precisamente debido a la relación entre la base del interés legítimo con el enfoque basado en riesgos, existe también una relación indudable con las medidas de protección adecuadas y específicas a las que se refiere el RGPD.

Así por ejemplo, la autoridad francesa de protección de datos CNIL, observó que las transferencias de datos desde Whatsapp a Facebook, realizadas, entre otras finalidades para mejorar sus funciones de inteligencia de negocio no tenían base de legitimación en tanto no se apreciaba un consentimiento válido ni era posible alegar un interés legítimo conforme al art. 6.1.f) RGPD. La razón de ello no era el hecho de que la mejora de los servicios de inteligencia de negocio no pudiera calificarse

como un interés legítimo del responsable, sino que en dicho tratamiento no se establecieron garantías adecuadas para proteger los intereses y libertades de los usuarios, ni se había previsto un medio de rechazar la transferencia manteniendo el uso de la aplicación -es decir, el único modo de paralizar la transferencia de datos era desinstalando la aplicación-.[459]

11.7. Determinación de fines no incompatibles

Otra crítica frecuente contra el interés legítimo es el hecho de que sea el responsable quien deba determinar la idoneidad de su uso como base de legitimación, de modo que cree una suerte de situación en la que es "juez y parte". Sin embargo, el Reglamento ya permite al responsable decidir y argumentar su decisión respecto de determinados extremos similares y no obstante poco controvertidos. Ejemplo de ello es el análisis sobre la (in)compatibilidad de las finalidades secundarias de los datos. Este análisis no es cualitativamente muy diferente del análisis que requiere la determinación de la existencia de un necesario y legítimo interés del propio responsable, así como de la realización del balance de intereses.

En el análisis sobre la no incompatibilidad de las finalidades primarias y secundarias, el responsable, tras haber cumplido todos los requisitos para la licitud del tratamiento original, debe tomar en consideración, entre otros, los siguientes aspectos: cualquier relación entre estos fines y los fines del tratamiento ulterior previsto, el contexto en el que se recogieron los datos, en particular las expectativas razonables del interesado basadas en su relación con el responsable en cuanto a su uso posterior, la naturaleza de los datos personales, las consecuencias para los interesados del tratamiento ulterior previsto y la existencia de garantías adecuadas tanto

[459] COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS (2017): *Data transfer from WHATSAPP to FACEBOOK: CNIL publicly serves formal notice for lack of legal basis*, de 18 de diciembre. Si bien el caso es anterior a la entrada en aplicación del RGPD, la calificación jurídica de los hechos continúa siendo relevante.

en la operación de tratamiento original como en la operación de tratamiento ulterior prevista.[460]

¿Nos suenan estos factores? Este análisis recuerda enormemente al que debe realizar el responsable en caso de que pretenda utilizar el art. 6.1.f) del RGPD como base de legitimación del tratamiento. Sin embargo, en dicho supuesto, el responsable no tiene una labor documental para manifestar por escrito el análisis que culmine con la conclusión sobre si otorgar una finalidad secundaria a los datos, de modo que, a pesar de ser más controvertida, la figura del interés legítimo ofrece incluso mayores garantías.[461]

11.8. Registro de actividades de tratamiento

La obligación introducida por el RGPD de mantener un registro de actividades de tratamiento (art. 30)[462] está también relacionada y alineada con la documentación que debe mantenerse para la válida determinación del interés legítimo como base de legitimación. En efecto, el registro de actividades es un documento base con el que el responsable realiza un ejercicio de consciencia sobre el modo en que la organización trata los datos personales. Así, este registro puede servir de ayuda al responsable para determinar sus intereses legítimos en relación con cada actividad de tratamiento, así como las posibles consecuencias negativas o positivas para los interesados y los terceros.

[460] Considerando 50.

[461] En opinión de María Loza, esto supone una quiebra al principio del consentimiento y una rebaja de los estándares de la Directiva 95/46, y añade que incluso el GT29 aboga por su supresión. Ver LOZA CORERA, María (2017): "De los microdatos a los datos masivos. Cuestiones legales", en *Universitat de València*, p. 422.

[462] Se exceptúan de esta obligación aquellas organizaciones pequeñas que no tratan datos personales de manera asidua, sino únicamente ocasional. Por este motivo, sería improbable que un responsable de datos que acometa actividades de análisis de datos con big data en el sentido aquí tratado pudiera acogerse a esta excepción.

11.9. Cumplimiento de todos los principios del reglamento

Además de todo lo anteriormente expuesto, el responsable del tratamiento tiene la obligación de respetar los principios relativos al tratamiento de datos, sea cual sea la base jurídica.

Si bien esta afirmación parece obvia, se hace importante señalarla, pues en ocasiones la visión negativa del interés legítimo va unida a la percepción de que cuando esta fuese la base de licitud del tratamiento, el responsable encontraría modos sencillos de incumplir principios del tratamiento como el de limitación de la finalidad, minimización de datos o limitación del plazo de conservación. En realidad, esta problemática puede darse igualmente en el caso de que el consentimiento o la ejecución contractual sean las bases del tratamiento.

Así, por ejemplo, pensemos en un responsable que argumente un interés legítimo para el tratamiento de datos obtenidos a través de un dispositivo con la finalidad de análisis de datos para descubrimiento de patrones o de entrenamiento de un modelo algorítmico. El responsable tiene la obligación de no tratar más datos de los necesarios para este fin, y de anonimizarlos o eliminarlos cuando ya no sean necesarios para la finalidad del tratamiento, que debe ser siempre específica. Por su parte, el interés legítimo alegado por un responsable de mantener los datos personales almacenados sin limitación temporal alguna, con la única finalidad de quedar disponibles para que en cualquier momento futuro estos puedan ser analizados en búsqueda de patrones y creación de perfiles no sería válido, pues dicho interés legítimo no se refiere a una finalidad específica ni prevé un plazo de conservación de los datos.

11.10. Conclusiones

En esencia, en las líneas anteriores hemos argumentado que el art. 6.1.f) RGPD es una base de legitimación alineada con el espíritu del nuevo Reglamento que la hace viable específicamente en tratamientos que utilicen nuevas tecnologías.

En ocasiones se argumenta que el RGPD ha consolidado un modelo de información y consentimiento, pues indudablemente algunos de los cambios más significativos del Reglamento han sido reforzar las exigencias del consentimiento, así como incrementar los derechos de información y el deber de transparencia del responsable. Sin embargo, este argumento únicamente se sostiene si se obvian los demás aportes y cambios relevantes del RGPD.

Muchas de las nuevas obligaciones o principios introducidos por el RGPD comparten las características de ser flexibles, cuyo objetivo es únicamente orientar al responsable, que debe adaptarse al caso concreto y especificar cómo se materializarán sus obligaciones para asegurar un adecuado nivel de cumplimiento normativo y protección efectiva. Ejemplos claros de ello son el principio de responsabilidad proactiva o la elección de medidas de seguridad y garantías adecuadas al riesgo.

Por este motivo, aquellos argumentos que se basan en la mera premisa de que el interés legítimo no permite alcanzar el mismo estándar de garantías que otras bases debido a su redacción amplia y su naturaleza flexible no están teniendo en cuenta que, en realidad, estas son precisamente las características que el RGPD ha deseado ensalzar en el nuevo sistema de protección de datos.

En consecuencia, descartar de modo automático los posibles efectos positivos de basar los tratamientos de datos del ecosistema digital en el interés legítimo parece una postura rígida que en realidad desaprovecha las oportunidades del interés legítimo, la elasticidad del RGPD para adaptarse a multitud de situaciones futuras y la protección amplia que todo ello aporta a los interesados.

12. Conclusiones

En este capítulo hemos analizado los elementos esenciales del art. 6.1.f) RGPD como base de licitud del tratamiento, así como su correspondencia en la normativa española. En concreto, hemos hecho referencia a la

aplicación del interés legítimo en relación con tratamientos de datos personales que utilizan tecnologías del tratamiento masivo de datos.

Ha quedado argumentado por qué, en nuestra opinión, el interés legítimo es capaz de aportar garantías que otras bases de licitud como el consentimiento no otorgan, a pesar de gozar de mayor popularidad, principalmente en nuestro país. Por ejemplo, el requisito de demostrar la necesidad del tratamiento y, principalmente, la obligación del responsable de llevar a cabo una ponderación de intereses. Asimismo, aplicada con las debidas garantías, esta base es capaz de mantener la capacidad de control de los interesados sobre sus datos, pues estos mantienen un derecho de oposición cuyo rechazo debe ser fuertemente fundado por el responsable.

Asimismo, precisamente aquellos elementos que caracterizan al interés legítimo como la necesidad de analizarse caso por caso, de ser dependiente del contexto del tratamiento y de dejar al responsable la carga de definir el impacto del tratamiento, las medidas de mitigación y de hacerse cargo de las consecuencias, son aquellos elementos que también se han ensalzado en el RGPD con respecto a la Directiva anterior. Ello, no obstante, no podemos obviar que el interés legítimo como base del tratamiento no está exento de limitaciones que pueden dificultar su aplicación, tales como la insorteable subjetividad del responsable en determinados momentos de la evaluación de interés legítimo.

Por su parte, en el concreto contexto español, se aprecia un especial rechazo del legislador hacia la figura del interés legítimo, creando restricciones que no tienen correspondencia en las normas comunitarias, hasta el punto de que el impulso prohibitivo del legislador ha debido ser frenado en diversas ocasiones.

Con todo lo expuesto hasta este momento, ¿en qué aspectos podemos concretar el potencial positivo y las limitaciones del interés legítimo como base de licitud del tratamiento en contextos de utilización de nuevas tecnologías, y en concreto, aquellas que hemos definido como tecnologías big data?

12.1. Reequilibrio

En primer lugar, el interés legítimo como base de legitimación del tratamiento puede servir de gran ayuda para lograr restablecer el equilibro que debe regir la relación entre aquellos que deseen tratar datos personales y aquellos cuyos datos son tratados. La aplicación del art. 6.1.f) en entornos caracterizados por la recolección y análisis de cantidades masivas de datos supone una oportunidad para resolver situaciones abusivas que crean un contexto desleal, injusto y opaco en el entorno digital a las que de otro modo los interesados se ven sometidos bajo una falsa apariencia de aceptación, manifestada a través del consentimiento o de un acuerdo (pre)contractual.

12.2. El responsable como figura central

En el contexto digital, la protección de los usuarios debe derivarse de soluciones que eliminen las cargas de la persona y las imputen sobre los responsables que desean tratar los datos. En esta línea se han expresado diversas voces dentro y fuera de la Unión Europea, tanto en relación con el derecho de protección de datos personales[463] como en relación con otras ramas jurídicas como la protección de los consumidores.[464]

[463] Por ejemplo, María Loza afirma que "para aquellos casos en que el consentimiento ya no pueda ofrecernos todas las respuestas, deberemos introducir nuevas medidas destinadas a garantizar la protección de este derecho fundamental. Estas nuevas medidas pueden poner el centro de atención en el responsable. (…) Estas "nuevas medidas" destinadas a garantizar el derecho fundamental de protección de datos que vendrían a suplir la no adecuación del consentimiento para todos los supuestos que se plantean en el mundo actual, deberán recaer exclusivamente sobre el responsable de dicho tratamiento, ya que la participación del individuo es imposible, con la única excepción de que existiera un derecho de exclusión para este tipo de tratamientos masivos". LOZA CORERA, María (2017): "De los microdatos a los datos masivos. Cuestiones legales", en *Universitat de València*, p. 413.

[464] En este sentido pueden entenderse manifestaciones como las realizadas por Jan Schakowsky, Presidenta del subcomité de protección del consumidor y comercio del Congreso de Estados Unidos: "[…] necesitamos encontrar soluciones que eliminen la carga del consumidor e imponga responsabilidades sobre aquellos que quieren nuestro datos", cita recogida de MCCABE, David (2019): "The sun may be setting on the old privacy rulebook", en *Axios*. La perspectiva de la protección del consumidor en lugar de la perspectiva del derecho a la protección de los datos personales no minimiza, en todo caso, la utilidad de la propuesta de redistribuir el equilibrio de cargas, derechos y obligaciones entre responsable del tratamiento e interesados.

Más concretamente, el ICO se ha posicionado sobre el interés legítimo afirmando que esta base jurídica implica por parte del responsable la aceptación de un nivel adicional de responsabilidad de protección de los derechos e intereses de los interesados,[465] e incluso recomienda no utilizar esta base de legitimación si el responsable desea mantener la carga de la responsabilidad sobre el interesado en lugar de sobre sí mismo.[466] El órgano de control ha indicado expresamente también que el interés legítimo permite al responsable demostrar que los intereses de aquellos que no tienen capacidad para autorizar han sido adecuadamente considerados y protegidos.[467] El contexto en el que la autoridad británica remarcaba esta consideración era la posible falta de capacidad de un niño para manifestar su voluntad contractualmente, y por tanto, la posibilidad de que el art. 6.1.f) -interés legítimo- fuera una base más adecuada que el art. 6.1.b -ejecución de un contrato-. Sin embargo, las conclusiones pueden hacerse extensibles en la medida en que podamos considerar que un adulto de plena capacidad pueda encontrar problemas para comprender lo que autoriza, ya sea por medio de la prestación del consentimiento o por la firma de un contrato.

En este sentido, resulta esencial el hecho de que el uso del interés legítimo exige que sea el responsable del tratamiento quien deba demostrar que tuvo en cuenta los intereses y derechos de los interesados, y que actuó en consonancia.

12.3. Justificación dura

Debido a los nuevos requisitos de consentimiento introducidos por el RGPD, algunos responsables ven en el interés legítimo una vía más atractiva en la que basar el tratamiento de datos personales y obtener réditos de la economía digital basada en datos.

---

[465] INFORMATION COMMISSIONER'S OFFICE (2018): *Guide to the General Data Protection Regulation (RGPD)*, p. 81.

[466] INFORMATION COMMISSIONER'S OFFICE: *Guidance on legitimate interest*.

[467] INFORMATION COMMISSIONER'S OFFICE (2018): *Guide to the General Data Protection Regulation (RGPD)*, p. 81, p. 68.

Sin embargo, a este punto del análisis es innegable concluir que la utilización del art. 6.1.f) como base de legitimación conlleva intrínsecamente una labor más tediosa, ardua, larga y necesitada de recursos que cualquier otra base. Ello es así porque el responsable adquiere la obligación adicional de justificar cuál es su finalidad y cómo se relaciona con el tratamiento de manera específica, cuáles son sus intereses y por qué estos priman sobre aquellos del interesado. Asimismo, esta valoración está abierta a opiniones contrarias que, en último lugar, pueden implicar una sanción por falta de base de legitimación para el tratamiento. Por este preciso motivo, sin embargo, el responsable tiene incentivos para no acudir a este precepto salvo que pueda demostrar de manera sólida que cumple cada uno de los requisitos. Como consecuencia, el tipo de tratamientos y el contexto en el que se utilice el interés legítimo en relación con el análisis de datos a gran escala a través de operaciones complejas deberá tener mayores garantías para el interesado, actuando así en su favor.

12.4. Elección vs aprobación

La regulación del interés legítimo es, como hemos analizado, genérica. Es labor del responsable concretar en qué se traduce, en el caso concreto, su interés, la finalidad del tratamiento, los intereses de las personas cuyos datos son tratados y los medios de mitigación de riesgos e impacto.

Esta concreción, no obstante, continúa siendo algo genérico desde el punto de vista de una persona individual, pues la ponderación realizada por el responsable se refiere al interesado medio razonable. Sin embargo, la norma también toma en consideración la posibilidad de que las circunstancias individuales de un interesado se aparten del contexto general en el que la aplicación del interés legítimo tuvo lugar a través del derecho de oposición, por el que el individuo puede cuestionar y objetar el tratamiento manifestando su situación particular. De este modo, el interesado mantiene una capacidad de control y de elección sobre sus datos personales sin necesidad de compelirle a decidir si aprobar o no

aprobar determinado tratamiento, tal y como sucede cuando la base del tratamiento es el consentimiento.

12.5. Fatiga del consentimiento

Por otro lado, la utilización del art. 6.1.f) como base de legitimación puede ayudar a paliar la fatiga de los interesados causada por la constante exposición a solicitudes de consentimiento a la que hacíamos referencia en el capítulo anterior, al tiempo que mantiene las medidas de protección y los requisitos de información a que tienen derecho los interesados.[468]

12.6. Resultado algorítmico menos sesgado

Hasta ahora, hemos argumentado por qué en determinadas circunstancias, el interés legítimo permite alcanzar un nivel de protección de la persona mayor que con otras bases de licitud. Es decir, el análisis se ha centrado en los posibles beneficios del art. 6.1.f) como instrumento jurídico. Sin embargo, es razonable atribuirle también efectos positivos para el funcionamiento propio de las tecnologías de análisis de datos.

Cuando un usuario de un servicio digital es expuesto a una solicitud de consentimiento, se crea un riesgo de que determinados subgrupos de población se auto-excluyan, causando que los datos finalmente analizados por el sistema contengan sesgos. Ello causa a su vez que los resultados analíticos sean también sesgados. En la medida en que el tratamiento de datos cumpla con todas las garantías exigidas, el uso de modelos no basados en mecanismos *opt-in* tienen la capacidad de poder obtener datos que representen de forma más precisa cada subgrupo de población y no existan perfiles infrarrepresentados.

12.7. Limitaciones

A pesar de estos factores favorables, también ha quedado argumentado que el art. 6.1.f) es susceptible de quedar sometido a algunas limitaciones.

[468] INFORMATION COMMISSIONER'S OFFICE: *Guidance on legitimate interest*.

Así por ejemplo, no existe una obligación expresa de publicar el ejercicio de ponderación de intereses, dificultando así la comprensión del contexto del tratamiento por parte del interesado y el ejercicio sencillo de su derecho de oposición. Asimismo, la realización de la ponderación de intereses mantiene un riesgo de parcialidad por parte del responsable, que es quien generalmente más se beneficia del tratamiento y quien decide en primera instancia sobre la validez de la base jurídica del tratamiento. Además, el ejercicio del derecho de oposición es susceptible de ser complejo de ejercitar para el interesado o desatendido por el responsable si este falsease el resultado del balance de intereses que requiere este derecho. Es posible imaginarse que, debido a la cada vez mayor complejidad de los tratamientos de datos personales en los ecosistemas tecnológicos actuales y la falta de conocimiento de los interesados sobre sus derechos, los responsables encuentren modos para no garantizar de modo leal este derecho a los interesados. Bien es cierto que cuando el interesado no esté de acuerdo con los motivos alegados por el responsable para denegar el ejercicio de su derecho, este podrá solicitar protección a la autoridad de control o, en última instancia, a los tribunales. Sin embargo, este proceso entraña un camino largo que únicamente aquellos interesados más motivados iniciarán, dejando potencialmente otros muchos desprovistos de la efectiva protección que la norma pretende otorgarles.

Por todo lo visto, puede concluirse que el recurso al art. 6.1.f) RGPD como base jurídica para legitimar el tratamiento de datos personales en relación con el uso de tecnologías de tratamiento masivo de datos no debe ser relegado a un segundo plano. De hecho, algunas autoridades nacionales de control[469] o el Supervisor Europeo de Protección de Datos[470] han manifestado en algunas ocasiones la posibilidad de acudir al interés

[469] INFORMATION COMMISSIONER'S OFFICE (2017): *Big data, artificial intelligence, machine learning and data protection* (versión 2.2), p. 32 y ss.

[470] SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS (2015): *Opinion 7/2015, Meeting the challenges of big data, A call for transparency, user control, data protection by design and accountability*, de 19 de noviembre.

legítimo como título de licitud en entornos de utilización de tecnologías big data.

En esencia, el interés legítimo debe ser considerado con la mente abierta, pero no como una puerta abierta a cualquier tipo de tratamiento.

CAPÍTULO VI. OTROS DERECHOS (Y REVESES) DEL RGPD

> "Nuestra identidad es, cada vez más, el fruto de una operación en la que son otros quienes llevan la batuta con una constante elaboración y control. Y no se trata solo de una construcción basada en el modo con el que el otro nos ve o nos define (…).
>
> La representación colectiva puede determinar la manera con la que se nos va a considerar, aunque no sea ella la que aporte los materiales constitutivos de la identidad, como sucede cuando se utilizan directamente nuestros datos personales".[471]

1. Introducción

El Capítulo III del RGPD contiene el elenco de derechos de los interesados en materia de protección de datos personales que ayudan a poner en práctica los principios enumerados en el art. 5 RGPD. En concreto, por lo que aquí interesa, en las páginas siguientes haremos referencia a algunos de los derechos más relevantes en relación con el tratamiento de datos personales en el contexto de datos masivos. Durante nuestro análisis tomará también especial importancia las posibles consideraciones que la elección de la base jurídica del tratamiento tenga respecto al ejercicio de los derechos del interesado. En otras palabras, prestaremos especial atención a cómo el principio de licitud del tratamiento despliega consecuencias en las diferentes prerrogativas que la norma concede al interesado.

[471] RODOTÀ, Stefano (2014): *El derecho a tener derechos*, Madrid, Trotta.

Ello es así, en primer lugar, puesto que el responsable no debe garantizar los mismos derechos en cualquier circunstancia. En efecto, una de las más directas consecuencias de la elección de una u otra base de legitimación es el conjunto de derechos asociados a esta.

Así, por ejemplo, como se observa en la siguiente tabla, algunos derechos tales como el de información o acceso deben garantizarse siempre. Por el contrario, otros derechos tales como el de portabilidad u oposición se aplican en diferentes casos. En aras de mantener la coherencia argumental y debido a su conexión con la base jurídica del interés legítimo, en el capítulo anterior de este trabajo ya hemos hecho referencia al derecho de oposición, por lo que este quedará fuera del ámbito de este capítulo. Por último, respecto al derecho a no ser objeto de decisiones automatizadas, incluido también en este gráfico, podríamos argumentar que, en la práctica, no se trata de un derecho *per se*. Durante este capítulo indagaremos más en este aspecto.

Derechos de cada base legitimadora RGPD	Arts. 13-14 Información	Art. 15 Acceso	Art. 16 Rectificación	Art. 17 Supresión	Art. 18 Limitación	Art. 20 Portabilidad	Art. 21 Oposición	Art. 22 No decisiones automatizadas
Consentimiento							Retirada consentimiento	Retirada consentimiento
Contrato							x	
Obligación legal				x		x	x	x
Interés vital						x	x	x
Interés público				x		x		x
Interés legítimo						x		x

Gráfico 4: Derechos del RGPD asociados a cada base de licitud del tratamiento. Fuente: elaboración propia.

Asimismo, el correcto ejercicio de los derechos del interesado encuentra su base en el principio de transparencia. Así lo reconoce el art. 12 RGPD, que bajo el título de Transparencia de la información indica que “el responsable del tratamiento facilitará al interesado información relativa a sus actuaciones sobre la base de una solicitud con arreglo a los artículos 15 a 22”. Es decir, parece existir una obligación del responsable de adaptar su

actividad para poder garantizar el ejercicio de los derechos del interesado y "facilitarlo". Esta adaptación debe darse a nivel organizativo (por ejemplo, asignando un responsable directo dentro de la organización para resolver las solicitudes de derechos en tiempo y forma así como creando mapas del flujo de datos completos que permitan comprender dónde se almacenan y cómo se llevará a cabo la identificación de los sujetos) o técnico (por ejemplo, implementando modos para eliminar la información de diferentes bases de datos cuando se ejerza un derecho de supresión o habilitando opciones para que el propio interesado pueda acceder u obtener una copia de la información que la organización trata sobre él).

En ocasiones, los responsables del tratamiento alegan dificultades para gestionar ejercicios de derechos de los interesados sobre la base de una compleja gestión de diferentes bases de datos, la existencia de datos duplicados, controles complejos para eliminar información, etc. Cabría pensar que esta situación pudiera ser aún más compleja en aquellas organizaciones que hacen uso de tecnologías de tratamiento automatizado de datos masivos y tecnologías big data o de aprendizaje automático. No obstante, son precisamente estas organizaciones las que están en disposición de establecer mecanismos y sistemas que, a través de medios automatizados, permitan cumplir de manera efectiva y eficiente los derechos del interesado.[472]

2. Derecho de portabilidad

Merece la pena detenerse a comentar el derecho de portabilidad, introducido por primera vez en el elenco de derechos relacionados con el tratamiento de datos personales en el art. 20 RGPD.[473] Este tiene su origen

[472] En el contexto de la administración pública -contexto diferente, pero interesante por analogía-, Piñar Mañas exponía que con las nuevas tecnologías "tan posible es conseguir una Administración transparente como convertirla en esencialmente opaca". PIÑAR MAÑAS, José Luís (2011): "Administración electrónica y protección de datos personales", en *Revista Xuridica da Universidade de Santiago de Compostela*, Nº Extra 1, p. 145-175.

[473] El derecho de portabilidad aparecía ya en el primer borrador de RGPD propuesto por la Comisión Europea, fruto de un amplio debate surgido en los años previos en torno a la necesidad o no de regularlo.

en el derecho reconocido en el ámbito de las telecomunicaciones a la portabilidad del número de teléfono del cliente que decide contratar un proveedor diferente de aquél que venía prestándole el servicio hasta el momento. Sin embargo, en el ámbito jurídico de protección de datos personales, se trata de una provisión novedosa, del que en consecuencia aún no existe una experiencia práctica relevante ni pautas claras en relación con determinadas cuestiones que surgen al interpretar el precepto.

En concreto, el art. 20 RGPD establece que el interesado tendrá derecho a recibir los datos personales que le incumban, que haya facilitado a un responsable del tratamiento, en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable del tratamiento sin que lo impida el responsable al que se los hubiera facilitado, si se cumplen dos condiciones cumulativas: que el tratamiento de datos sea automatizado y que la base de legitimación de dicho tratamiento sea el consentimiento del interesado o la ejecución de un contrato. Asimismo, el interesado podrá solicitar que, cuando sea técnicamente posible, los datos sean portados directamente de un responsable a otro sin necesidad de que el interesado intervenga.

La primera lectura del art. 20 nos lleva a extraer que el derecho de portabilidad se puede entender como un doble derecho. Por un lado, el derecho a obtener una copia de los datos y, por otro lado, el derecho a que dichos datos sean transferidos al proveedor receptor de la elección del interesado en un formato de lectura mecánica.[474]

La principal justificación y la razón de ser de este derecho, tal y como se expuso durante la tramitación del RGPD, fue favorecer que los interesados pudieran migrar sus datos entre proveedores -en concreto, con los proveedores de servicios en la nube y redes sociales en mente-, lo que facilitaría aumentar el control del interesado sobre los datos al tiempo que favorecería la libre competencia. Un objetivo ciertamente loable y en

[474] ZANFIR, Gabriela (2012): "The Right to Data Portability in the Context of the EU Data Protection Reform", en *International Data Privacy Law*, Vol. 2, No. 3, p. 9.

consonancia con el libre flujo de datos dentro de la UE, que constituye uno de los objetivos principales del RGPD.[475]

Esto es, el derecho de portabilidad se sustenta en un doble ámbito de protección: por un lado, la libre competencia, y por otro lado la autodeterminación informativa que se deriva del derecho a la privacidad y la protección de datos personales. Para conseguir este objetivo doble, es necesario crear las condiciones jurídicas y técnicas adecuadas.

2.1. Consumidor cautivo

La capacidad de un usuario final de un servicio de migrar sus datos a otro proveedor permite liberar la competencia y otorgar al usuario capacidad de elección sobre el proveedor. Cuando el consumidor debe hacer frente a un coste alto para reemplazar el proveedor de sus servicios se crea lo que la ciencia económica define como consumidor cautivo, donde se genera una dinámica de dependencia del servicio actual. Esto crea barreras de entrada de nuevos competidores al mercado que pueden llegar a instaurar situaciones de oligopolio (o, en el peor de los casos, de monopolio). Como consecuencia de ello, pueden desarrollarse prácticas anticompetitivas y condiciones de mercado menos favorables para el consumidor final.

Un caso sencillo y tradicional de consumidor cautivo que permite comprender mejor este concepto se da, por ejemplo, cuando se celebra un festival de música en un recinto cerrado. Dentro del recinto existe un número muy limitado de vendedores de agua, de modo que el mercado funciona como un oligopolio sobre el que no hay alternativas, porque los asistentes al festival no pueden salir del recinto. Cuando esto se produce, el precio de una botella de agua puede duplicarse o triplicarse con respecto al precio normal en la calle, esto es, en una economía de libre competencia. De manera similar, un usuario de una app de música encontrará dificultad para comenzar a utilizar otra si no puede migrar sus listas de música a otra app. Así, la dificultad de trasladar sus datos le convierte en cautivo. En

[475] Art. 1.3 RGPD.

estas circunstancias, se debilita la competencia, pues un proveedor que desarrolle un mejor servicio tendrá elevadas dificultades para ganar mercado, al tiempo que las condiciones ofrecidas a los usuarios y consumidores empeoran.

De este modo, un medio de perpetuar el coste de migrar entre servicios o proveedores de servicios análogos es dificultar la portabilidad de los datos. *A sensu contrario*, un modo de favorecer la competencia y en última instancia las condiciones de los consumidores es garantizar que los datos puedan moverse con facilidad. En este sentido, el derecho a la portabilidad del art. 20 RGPD parte de la comprensión de que los datos son un activo de mercado de gran valor en la economía, cuya importancia trasciende (aunque no sustituye) a la concepción de la protección de datos personales como un derecho fundamental.

2.2. Autodeterminación informativa

Por otro lado, la posibilidad de un interesado de portar sus datos aumenta su capacidad de control, desarrollando por tanto la autodeterminación informativa,[476] que es la base sobre la que se ha asentado tradicionalmente el desarrollo del derecho de protección de datos personales.[477]

En la actualidad, el uso de servicios en línea, aplicaciones, programas informáticos, dispositivos conectados o redes sociales crean una realidad digital sobre cada uno de nosotros hasta el punto de llegar a identificarse con una identidad digital. No se trata de una cuestión baladí. La determinación de los gustos, los modos de actuar, hábitos y, en esencia, nuestra personalidad digital nos define de manera precisa. En la medida en que todo ello es posible gracias a la recolección, tratamiento y análisis de

[476] Tribunal Constitucional Federal de Alemania, Sentencia de 15 de diciembre de 1983.

[477] Para un análisis más exhaustivo sobre la relación entre el derecho de portabilidad y la autodeterminación informativa ver FIALOVÁ, Eva (2014): "Data portability and informational self-determination", en *Masaryk University Journal of Law and Technology*, Vol. 8, No. 1; MURILLO DE LA CUEVA, Pablo Lucas (2008): "El derecho a la autodeterminación informativa y la protección de datos personales" en *Azpilcueta: cuadernos de derecho*, No. 20.

los datos, y que a partir de ello se toma acción o decisiones, la creación y utilización de los datos adquieren un carácter esencial en el desarrollo de la persona. Asimismo, esta esfera digital de la persona trasciende y crea consecuencias tangibles en la realidad material analógica.

Por este motivo, la protección básica de la persona en su esfera digital se encuentra cada vez más estrechamente ligada con la capacidad de control sobre sus datos personales, con su autodeterminación. En la medida en que la intensidad y complejidad de los tratamientos de datos aumentan se hace necesario crear nuevos modos de protección al interesado. Como fruto de nuestra interacción digital en multitud de lugares, la información que forma parte de esta identidad en el entorno electrónico no está en un lugar único, sino que se encuentra dispersa en bancos de datos distribuidos, que incluso llegan a formar lo que Rodotà denominó cuerpo distribuido[478] o cuerpo electrónico[479] cuya trascendencia supera en ocasiones a la identidad física.

Es en este ámbito cuando el derecho de portabilidad de datos se convierte en necesario para la protección de la esfera de control de la persona.

Sin embargo, cuando uno comienza a pensar en los pormenores del derecho de portabilidad varias cuestiones emergen. ¿Qué datos puede el interesado portar? ¿Debe el interesado concretar sobre qué datos desea ejercer su derecho?[480] ¿Cómo se lleva a cabo el proceso desde el punto de vista técnico? ¿Qué conclusiones pueden extraerse, no del contenido del art. 20 RGPD sino de sus lagunas o ausencias de contenido?

Una vez expuesta la importancia del derecho a la portabilidad para la esfera más íntima de la persona, así como para la protección de unas condiciones

[478] RODOTÀ, Stefano (2005): Quale diritto per il nuovo mondo, en *Estudios de derecho civil. Obligaciones y contratos. Libro Homenaje a Fernando Hinestrosa*, No. 3, p. 201 y ss.

[479] RODOTÀ, Stefano (2010): *La vida y las reglas. Entre el Derecho y el no Derecho*, Madrid, Trotta.

[480] FERNÁNDEZ-SAMANIEGO, Javier y FERNÁNDEZ-LONGORIA, Paula (2016): "El derecho a la portabilidad de los datos", en José Luís Piñar Mañas (dir.), Reglamento General de Protección de Datos: Hacia un nuevo modelo europeo de privacidad, Madrid, Reus, p. 265 y ss.

de mercado leales, analizaremos algunas limitaciones que emergen de la aplicación art. 20 RGPD.

2.3. ¿Qué datos pueden ser portados?

En primer lugar, destaca el ámbito restringido al que se aplica el derecho de portabilidad, por cuanto únicamente se puede ejercer respecto de aquellos datos personales aportados por el individuo al responsable. Una posible explicación de esta circunstancia puede verse en el hecho de que en 2012, año en que se publica la primera propuesta de RGPD, el legislador había configurado el derecho de portabilidad pensando únicamente en dotar a los usuarios de redes sociales de la capacidad de migrar datos de una red social a otra. Sin embargo, la evolución, tanto de la redacción del precepto como del uso de los datos terminó por ampliar esta concepción originaria.

2.3.1. *Datos aportados y observados*

El derecho de portabilidad cubre, los datos aportados por la persona. Entre los datos aportados por el interesado se encuentran, por ejemplo, nombre, dirección de correo electrónico, fotografías, comentarios en una red social o edad y peso introducidos por la persona en una aplicación de monitorización de salud, etc., en tanto hayan sido proporcionados directamente por el interesado.

También podría interpretarse que este grupo incluye datos no directamente aportados por el usuario, pero directamente observables sobre este en virtud del uso del servicio o dispositivo.[481] Ejemplos de ello pueden ser la frecuencia de conexión a una red social, tiempo de respuesta a cuestiones planteadas por los posibles compradores en una aplicación de venta, número de artículos vendidos, kilómetros corridos o velocidad media y el ritmo cardíaco de un usuario de una aplicación de monitorización de actividad física, etc. Esto es relevante, pues la proporción de datos

[481] GRUPO DE TRABAJO DEL ARTÍCULO 29 (2017): *Guidelines on the right to data portability* (WP 242 rev.01), de 5 de abril. Adoptadas por el Comité Europeo de Protección de Datos, p. 9-10.

recogidos que provienen directamente del interesado es cada vez menor en relación con aquella de datos observados.

Asimismo, especialmente importante puede ser incluir en esta categoría los datos de localización del interesado que el responsable hubiera recopilado durante la utilización del servicio. De hecho, la Agencia Española de Protección de Datos ha manifestado que, bajo su criterio, estos datos son objeto de portabilidad, aunque estos no alcanzan a incluir una definición tan abstracta de datos como "visitas web".[482]

2.3.2. *Datos inferidos y perfiles*

Por el contrario, parece que el individuo no tendrá derecho a portar datos tales como aquellos inferidos sobre él por el responsable, información sobre patrones de comportamiento o su perfil detallado, es decir, datos creados u obtenidos por el responsable como fruto del análisis llevado a cabo en lo que hemos definido como Fase 2-Análisis, a partir del estudio de los datos primarios y la posterior reutilización de dichos datos para cruzarlos con o enriquecer a los datos del interesado durante la Fase 3-Aplicación.[483] Este hecho es relevante, pues la proporción de datos obtenidos a través de un análisis deductivo del interesado es cada día mayor en relación con los datos obtenidos directamente de este.[484] Asimismo, las finalidades principales de los datos se orientan, en muchas ocasiones, hacia la

[482] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (2020): Resolución Nº: R/00552/2019, de 5 de febrero, p. 8.

[483] Este mismo criterio ha sido seguido por la AEPD en su primera resolución relacionada con el derecho de portabilidad. En ella se indica que "no son objeto del derecho de portabilidad aquéllos datos que puedan ser considerados "inferidos" y "derivados", entendidos como los que resulten de la aplicación a la información generada en el desarrollo del servicio de conocimientos o técnicas propias del responsable; es decir, procedentes de la aplicación sobre los datos relacionados con el producto o servicio de técnicas que forman parte del *know how* del responsable (como pueden ser entre otros, técnicas matemáticas o resultantes de la aplicación de algoritmos)". AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (2020): Resolución Nº: R/00552/2019, de 5 de febrero, p. 7.

[484]HOFFMAN, David; MASUCCI, Riccardo (2018): "Intel's AI Privacy Policy White Paper. Protecting individuals' privacy and data in the artificial intelligence world", en *Intel Corporation*; INTERNATIONAL DATA CORPORATION (IDC) (2017): *Data Age 2025: The Evolution of Data to Life-Critical, Don't Focus on Big Data; Focus on the Data That's Big*.

elaboración de perfiles y la posterior toma de decisiones con respecto al interesado.

Así, la limitación del tipo de datos susceptibles de ser portados de manera que se excluya cualquier información inferida de un interesado puede constituir una barrera a la libre circulación de datos, así como una barrera de entrada a nuevos competidores en un mercado. Igualmente, constituye una limitación para el interesado y para sus intereses. Como ha señalado Rodotà, millones de personas tienen un "doble" electrónico, cuya existencia condiciona mucho más que el cuerpo físico.[485] Pensemos, por ejemplo, en el usuario de una entidad financiera que desea portar sus datos a otra entidad. El individuo puede tener un interés en que la nueva entidad, que puede no contar con información abundante o relevante sobre este, acceda a su perfil para comprobar su nivel de fiabilidad o probabilidad de morosidad. En un sentido similar se expresaba Picker, que expone como ejemplo la reputación de buen vendedor de un usuario en Ebay, generada con esfuerzo a lo largo del tiempo. Dicho usuario tendrá un interés claro en poder exportar esta información a un nuevo proveedor, pues ser un vendedor fiable en una plataforma, es indicativo de que también lo será en otra plataforma. En línea con lo ya dicho sobre la relación entre el derecho de portabilidad y de autodeterminación informativa, Picker argumenta que las características personales ligadas al perfil de una persona forman parte de su identidad digital, estando por tanto en la base del desarrollo de la libre personalidad.[486] De este modo, la limitación sobre la capacidad de control de los datos de la persona le afecta de manera esencial.

En este punto cabe reflexionar sobre ¿por qué se limita la portabilidad de los datos inferidos?

---

[485] RODOTÀ, Stefano (2005): Quale diritto per il nuovo mondo, en *Estudios de derecho civil. Obligaciones y contratos. Libro Homenaje a Fernando Hinestrosa*, No. 3, p. 201 y ss.

[486] En concreto, Picker argumenta que las características personales ligadas al perfil de una persona forman parte de su identidad digital, estando por tanto en la base del desarrollo de la libre personalidad. PICKER, Randal C. (2008): "Competition and privacy in web 2.0 and the cloud", en University of Chicago Law & Economics, Olin Working Paper No. 414.

2.3.3. *Propiedad intelectual*

Una de las principales justificaciones que podría alegar la entidad financiera originaria sería su interés en proteger el conocimiento de la organización o los derechos sobre los desarrollos algorítmicos complejos mediante los cuales pudo ser analizada la información básica para extraer información secundaria de valor añadido. Ciertos matices podrían apreciarse.

Pensemos, de nuevo, en la elaboración de un perfil de fiabilidad de los usuarios de un servicio de venta de productos en línea. El proveedor del servicio puede realizar un perfil y obtener conclusiones a partir de grandes cantidades de datos que retroalimentan un modelo de aprendizaje automático, que a su vez sirve de base para la mejora continua de su motor de recomendación de artículos. Algunos de los resultados del análisis de datos podrían ser en la línea de "el modelo de comportamiento del usuario en relación con comportamientos pasados de otros usuarios similares refleja una probabilidad del 88% de comprar, al menos, uno de los siguientes productos si es expuesto a tres o más impactos publicitarios en menos de siete días: cámara fotográfica digital junto con un set de objetivos, comida de perro, un taladro de pared o un reloj de mujer de gama alta".

Se trata de un proceso que conlleva inteligencia, recursos y métodos complejos, y por lo tanto existe un interés legítimo de la organización por mantener el secreto de dicho conocimiento y no desvelarlo a la competencia. En paralelo, imaginemos que un vendedor de la misma plataforma quiere comenzar a vender sus productos en otras plataformas, y tiene un interés en poder evidenciar su trayectoria como vendedor fiable.[487] ¿Debería el usuario poder tener derecho a portar el resultado de su perfil cuando ello no conlleve un peligro de revelación de información sensible del responsable? Un ejemplo de ello sería la afirmación, obtenida de su perfil "el vendedor x tiene un índice de fiabilidad de un 96%" o "el

[487] La definición de lo que se consideraría un vendedor fiable no es necesaria para el desarrollo del argumento propuesto; baste aquí con referirnos de manera intuitiva a ello.

vendedor x goza de una puntuación de 4 estrellas sobre 5 sobre parámetros tales como la puntuación de los usuarios o su tiempo medio de respuesta". En tanto el responsable no deba verse obligado a desvelar los parámetros exactos y los métodos que le han llevado a dicha conclusión, no debería existir inconveniente para la portabilidad de dicha información, a pesar de que los datos no hayan sido aportados directamente por el interesado.

De hecho, parece que el RGPD sí ha tenido en cuenta, en otros lugares del texto, el interés de los individuos en obtener cierta información relacionada con el proceso que subyace al tipo de análisis de datos y conclusiones que se presenta en el ejemplo. Nos referimos precisamente a las disposiciones relacionadas con la obtención de información en relación con la toma de decisiones automatizadas, que recordemos, incluye la elaboración de perfiles. Así, los arts. 13, 14 obligan al responsable a informar sobre la lógica aplicada, y el art. 15 permite al interesado ejercer un derecho de acceso que comprende, de nuevo, información sobre dicha lógica implícita en todo tratamiento automático de datos personales, en concreto, cuando se base en la elaboración de perfiles, teniendo en cuenta la necesidad de protección de los secretos comerciales y la propiedad intelectual del responsable.[488]

De este modo, si el Reglamento ya ha tenido en cuenta el derecho del usuario a acceder a y ser informado de la información relevante sobre la lógica aplicada en la elaboración de un perfil, no existe, en nuestra humilde opinión, motivo suficientemente fundado para impedirle al mismo usuario portar un resultado simplificado de dicha lógica. Entonces, ¿cuál es la base de dicha limitación?

2.3.4. *Interés legítimo del responsable*

La limitación del derecho de portabilidad a los datos aportados directamente por el interesado parece traer causa de la decisión del legislador de proteger el interés legítimo del responsable de mantener el

[488] Considerando 63 RGPD.

secreto comercial o su derecho de propiedad intelectual, en los términos vistos en los párrafos anteriores.[489] Esta conclusión puede desprenderse a pesar de que el término interés legítimo no se mencione en relación con el derecho de portabilidad ni que este derecho sea ejercitable cuando el tratamiento se ha basado en el art. 6.1.f) RGPD.

Ciertamente, es necesario mantener un equilibrio proporcional entre la protección de la economía, la sociedad digital y los intereses de los responsables, por un lado, y los derechos de los interesados o usuarios finales de servicios en línea, por otro lado. Sin embargo, la limitación absoluta del derecho de portabilidad cuando el tratamiento de datos personales se basa en el interés legítimo parece ser consecuencia de la concepción de que un ejercicio de ponderación en el que un lado de la balanza lo ocupe el derecho del responsable a mantener su conocimiento protegido como secreto comercial o propiedad intelectual vencerá, en cualquier caso, a los intereses puestos en el lado contrario de la balanza, tales como el derecho de un interesado a poder mostrar su identidad digital a otro proveedor.

Es decir, parece que el RGPD transgrede en este aspecto la necesaria ponderación de intereses en el caso concreto y crea una presunción iuris et de iure de interés legítimo en favor de los responsables para proteger el conocimiento, secretos comerciales o su propiedad intelectual. Esta protección sin previa ponderación de intereses se extiende también al resultado de los procesos por los que se extrae información inferida de los interesados.

---

[489] Así lo demuestra, por ejemplo, una de las enmiendas presentadas durante el proceso legislativo del RGPD que indica: "*Due regard must be given to the limits to data portability, especially in relation to the legitimate interests of businesses to protect trade secrets and intellectual property rights, within reason*." Opinion of the Committee on Industry, Research and Energy for the Committee on Civil Liberties, Justice and Home Affairs on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)), de 26 de febrero de 2013, enmienda 172.

2.4. Restricción de bases de legitimación

El art. 20.1 RGPD contiene otro límite al derecho de portabilidad, pues restringe su ejercicio a los tratamientos basados en el consentimiento del interesado o en la necesidad de la ejecución de un contrato. En otras palabras, el RGPD no permite portar datos cuando el responsable del tratamiento utiliza las demás bases de legitimación, como por ejemplo, el interés legítimo. ¿Por qué?

2.4.1. *Un camino por las versiones previas de este derecho*

La primera versión del derecho de portabilidad comprendido en el art. 18 de la propuesta de RGPD de la Comisión permitía al individuo obtener una copia de sus datos independientemente de la base de legitimación sobre la que se basaba el tratamiento. En cambio, la capacidad de transferir datos de un proveedor a otro sí se restringió a datos tratados sobre la base del consentimiento o un contrato. Esta disparidad podría crear conflictos, por ejemplo, en la aplicación conjunta de la retención de datos por parte de los responsables con base en la entonces Directiva 2006/24[490] sobre retención de datos -datos sobre los que se aplicaba la normativa de protección de datos pero que sin embargo no diferenciaba entre bases de legitimación- y el derecho de portar los mismos datos retenidos a otro proveedor.[491] Esta disparidad surge del hecho de que si los datos debían ser obligatoriamente retenidos y el interesado podía incluso obtener una copia de ellos, ¿por qué no permitir al interesado elegir qué proveedor debía retenerlos y así seleccionar, por ejemplo, aquél que aportara mayores garantías de seguridad?[492] Es decir, unificar los criterios para hacer aplicable ambas

[490] Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas.

[491] La Directiva 2006/24/CE fue anulada por el TJUE en su sentencia en los Asuntos acumulados C-293/12 y C-594/12, Digital Rights Ireland, de 8 de abril de 2014.

[492] ZANFIR, Gabriela (2012): "The Right to Data Portability in the Context of the EU Data Protection Reform", en *International Data Privacy Law*, Vol. 2, No. 3, p. 10.

vertientes del derecho de portabilidad (obtener una copia de los datos y poder trasladarla) era necesario.

Ciertamente, las versiones consecutivas de propuestas de RGPD modificaron el derecho de portabilidad en relación con este factor y lo unificaron, aunque en direcciones diferentes. La propuesta de RGPD del Parlamento[493] eliminaba la restricción basada en el uso del consentimiento o la ejecución de un contrato para ambas vertientes del derecho de portabilidad. Es decir, abría la posibilidad a que los interesados tuvieran un derecho de portabilidad en todo caso, con independencia de qué base legitimadora sustentara el tratamiento. Por su parte, la propuesta de RGPD presentada por el Consejo[494] incluía en ambas vertientes del derecho de portabilidad, la limitación a los datos que hubieran sido tratados bajo estas bases de legitimación.

La versión finalmente adoptada en el art. 20 RGPD sigue la propuesta del Consejo y por tanto mantiene la restricción en ambas vertientes del derecho, obtención de copia y migración de datos a los datos tratados con el consentimiento del interesado o sobre la base de una relación contractual con este. En este extremo incide, además, el considerando 68 al indicar que este derecho “debe aplicarse cuando el interesado haya facilitado los datos personales dando su consentimiento o cuando el tratamiento sea necesario para la ejecución de un contrato. No debe aplicarse cuando el tratamiento tiene una base jurídica distinta del consentimiento o el contrato”.

---

[493] PARLAMENTO EUROPEO (2014): *Resolución legislativa del Parlamento Europeo, de 12 de marzo de 2014, sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo 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)* (COM(2012)0011 — C7-0025/2012 — 2012/0011(COD)), de 12 de marzo.

[494] CONSEJO DE LA UNIÓN EUROPEA (2016): *Posición del Consejo en primera lectura con vistas a la adopción de un Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva95/46/CE (Reglamento general de protección de datos)*, 2012/0011 (COD) 5419/16 Rev. 1, de 8 de abril.

2.4.2. *¿Qué motivó esta decisión?*

Desde un punto de vista meramente jurídico no parece razonable concluir que el derecho de portabilidad de datos personales únicamente tenga sentido respecto de aquellos datos tratados bajo consentimiento o contrato. De hecho, el Supervisor Europeo de Protección de Datos ya había llamado la atención sobre este extremo y animó a abrir el debate a la posibilidad de extender el ejercicio de este derecho sobre datos tratados bajo otras bases de legitimación.[495]

Pareciera, por tanto, una decisión fruto de un compromiso político alcanzado como resultado del proceso de redacción del Reglamento. En consecuencia, parece que no existe un argumento sólido para justificar que, en todo caso y sean cuales sean las circunstancias del tratamiento, los interesados no tengan derecho a solicitar la migración de sus datos personales aportados u observados cuando el responsable utiliza el interés legítimo como base del tratamiento.

2.5. La relación entre estas dos limitaciones

Recapitulando lo dicho hasta ahora, el derecho de portabilidad únicamente puede ejercitarse cuando se cumplen tres condiciones cumulativas: (i) que los datos hayan sido aportados por el interesado; (ii) que el tratamiento tenga como base el consentimiento del interesado o un contrato con él, y (iii) que se produzca por medios automatizados. Sobre este último requisito volveremos más adelante, al hablar de la toma de decisiones automatizadas. Por ahora, hagamos el ejercicio de interpretar de manera conjunta los dos primeros requisitos.

Ciertamente es posible pensar en una gran cantidad de supuestos en los que, cuando es el interesado el que aporta los datos directamente al responsable, el tratamiento se basa en su consentimiento o en una relación contractual. Esto es, los datos recogidos durante la Fase 1, y

[495] SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS (2012): *Opinion on the data protection reform package*, de 7 de marzo, p. 25.

posteriormente tratados con la voluntad del interesado para su finalidad primaria aceptada mediante la manifestación de la voluntad del interesado podrán ser portados. Sin embargo, también es posible pensar en situaciones en las que, siendo el interesado quien aporta los datos al responsable, el tratamiento se fundamenta en otras bases del art. 6 RGPD. Así, por ejemplo, usos adicionales de los datos basados en el interés legítimo del responsable, tales como su análisis para descubrir nueva información durante la Fase 2. Bajo la redacción del RGPD los datos utilizados en dichos tratamientos no podrán ser portados por el interesado.

Recuperando de nuevo el ejemplo anterior sobre el perfil reputacional de una persona, cabe pensar que un usuario que ha trabajado por construir una huella o personalidad digital que le caracterice como persona confiable tenga un gran interés en que esta le sea reconocida en otro lugar de internet. Imaginemos que nuestro vendedor de alta calificación en Ebay desea comenzar a utilizar el Marketplace de Facebook o el servicio de Amazon para realizar ventas. La llegada “en blanco” a las nuevas plataformas le harían partir de una posición de desventaja, por cuanto no es capaz de transmitir a los compradores su imagen de vendedor de productos de calidad, que responde de manera rápida, implementa medidas para facilitar la devolución rápida, etc.

2.6. Interoperabilidad de bases de datos

Retomando las consideraciones sobre el ejercicio práctico del derecho de portabilidad, el considerando 68 RGPD menciona expresamente que los datos objeto de portabilidad deban ser facilitados al interesado “en un formato estructurado, de uso común, de lectura mecánica e interoperable”, esto es, de modo que permitan su reutilización. En otras palabras, parece que la redacción de este considerando pretende impulsar el desarrollo de sistemas interoperables que permitan el flujo de datos de un responsable a otro manteniendo su utilidad. De hecho, el propio considerando 68 alienta a los responsables a crear formatos interoperables que permitan el ejercicio de este derecho de portabilidad.

La interoperabilidad puede definirse como "la capacidad de comunicar, ejecutar programas, o transferir datos entre distintas unidades funcionales de un modo que requiera un escaso o nulo conocimiento por parte del usuario de las características diferenciadoras entre dichas unidades".[496]

Adicionalmente, el art. 20.1 RGPD indica que el interesado debe poder portar sus datos sin que el responsable lo impida. Se trata de una fórmula muy ambigua que quizás sea mejor comprendida acudiendo a la versión en inglés del artículo. La redacción en inglés utiliza la expresión "*without hindrance*", esto es, el responsable no debe poner "impedimentos" u "obstáculos" al ejercicio de este derecho. En un sentido similar cabe interpretar la manifestación del GT29 que defiende que los responsables que almacenen datos personales deben estar preparados para facilitar el ejercicio del derecho de portabilidad de un interesado.[497]

2.6.1. *Falta de obligatoriedad*

Además de lo anterior, el considerando 68 también indica que el responsable debe transmitir los datos directamente a otro responsable "cuando sea técnicamente posible" y que el derecho de portabilidad "no debe obligar al responsable a adoptar o mantener sistemas de tratamiento que sean técnicamente compatibles". En línea con esta afirmación, el art. 20.2 RGPD exceptúa la capacidad del interesado de ejercer su derecho a que los datos sean portados directamente por los proveedores cuando ello no fuere "técnicamente posible".

Esto es, la vertiente del derecho de portabilidad consistente en remitir los datos de un proveedor a otro encuentra una excepción cuando los sistemas técnicos de dichos proveedores no permitan la migración de los datos. En efecto, más allá de estas superfluas referencias a los beneficios de la interoperabilidad, nada parece realmente obligar a los responsables al

[496] Norma ISO/IEC 2382-01 sobre Vocabulario de Tecnologías de la Información, Términos Fundamentales.

[497] GRUPO DE TRABAJO DEL ARTÍCULO 29 (2017): *Guidelines on the right to data portability* (WP 242 rev.01), de 5 de abril. Adoptadas por el Comité Europeo de Protección de Datos, p. 7.

desarrollo de dichos estándares comunes e interoperables, al menos, en lo que a datos personales se refiere.

2.6.2. *¿En qué se traduce esta falta de obligaciones de interoperabilidad de los responsables del tratamiento?*

Debilidad del derecho

En primer lugar, y como consecuencia principal de lo aquí descrito, en una indudable debilidad del nuevo derecho de portabilidad de datos personales nacido con el RGPD. En concreto, la falta de interoperabilidad y de formatos de uso común desvirtúa el objeto último de este derecho[498] y puede ser utilizada por los responsables del tratamiento como modo de desincentivar su obligación de transmitir una copia de los datos y evitar la migración de datos de un usuario a otro servicio. Ello también puede causar que, a pesar de que el proveedor en cuyo sistema se almacenen los datos a portar garantice la recepción de una copia de los datos personales, estos no sean fácilmente reutilizables por el interesado, poniendo en entredicho una de las razones principales de ser del derecho de portabilidad.

Dependencia tecnológica

La segunda consecuencia de la falta de interoperabilidad de sistemas es la llamada dependencia tecnológica ("*technological lock-in*").[499] Este concepto describe la situación según la cual cuanto más adoptada se encuentra una tecnología en la sociedad menos probabilidad existe de que los usuarios migren a otra tecnología diferente. Esto se debe, por ejemplo, a los costes de aprendizaje de una nueva tecnología.

Las compañías son conscientes de este comportamiento y, de hecho, una estrategia de marketing para soluciones tecnológicas se basa precisamente en desarrollar funcionalidades y actualizaciones constantes

[498] FERNÁNDEZ-SAMANIEGO, Javier y FERNÁNDEZ-LONGORIA, Paula (2016): "El derecho a la portabilidad de los datos", en José Luís Piñar Mañas (dir.), Reglamento General de Protección de Datos: Hacia un nuevo modelo europeo de privacidad, Madrid, Reus, p. 265 y ss.

[499] PERKINS, Richard (2003): "Technological ´lock-in´", en *Internet Encyclopedia of Ecological Economics*, International Society for Ecological Economics, p-1-8.

que supongan un pequeño pero continuo esfuerzo de adaptación en los usuarios, de forma tal que a medio y largo plazo logre crear dependencia por el gran esfuerzo necesario para reaprender a manejar la solución o el producto de un competidor. En otras palabras, la adopción de tecnología única es un mecanismo para crear usuarios cautivos y mantener una ventaja competitiva de mercado.

Esta situación crea barreras de entrada de nuevos competidores al mercado, impulsando situaciones de comportamiento oligopolístico (o en el peor de los casos, monopolístico). Uno de los ejemplos históricos más reseñables es la adopción del teclado Qwerty. Esto es, parece que todo ello crea impedimentos u obstáculos ("*hindrance*"), aquellos mismos que el RGPD pretendía reprimir. Ciertamente, falta de una obligación fuerte, una empresa no tendrá incentivos para transmitir datos de sus clientes a un competidor, e incluso desarrollará estrategias para evitarlo.

De hecho, ya en 2012, precisamente en pleno debate sobre la necesidad de actualizar la normativa europea de protección de datos que dio como fruto el RGPD y el reconocimiento del derecho de portabilidad, García Mexía[500] reflexionaba sobre la lucha de poder existente entre las grandes empresas tecnológicas por el liderazgo del software. Para ello destacaba el ejemplo a Apple, líder como fabricante de dispositivos, precisamente con un modelo de negocio basado en la incompatibilidad con otros fabricantes, con un rango de precios elevado y que puede llegar a ser capaz de modificar la idea de la Internet tal y como la concebimos actualmente. A pesar de todo, este continúa siendo su modelo de negocio actual.

Por este motivo, desde el inicio el derecho de portabilidad y el fomento de la competencia en el mercado digital se han visto ligadas. También en 2012, Joaquín Almunia, entonces Comisario Europeo de Competencia

[500] GARCÍA MEXÍA, Pablo Luis (2012): *Historias de internet. Casos y cosas de la red de redes*, en Tirant Humanidades, Valencia.

expresó que el derecho de portabilidad "se dirige al corazón de la política de competencia".[501]

2.6.3. *Consecuencias*

En resumen, hemos detectado dos efectos principales de la falta de obligación de interoperabilidad entre servicios. La primera, debilidad de este derecho, afecta al ejercicio del derecho de portabilidad reconocido en el RGPD, y así desencadena una consecuencia individual. Por otro lado, el efecto de dependencia tecnológica es, por naturaleza, de alcance social, por cuanto surge, precisamente, de una amplia adopción de un producto o servicio específico.

Esto conlleva a su vez diversas consecuencias. En primer lugar, supone que los efectos de un incorrecto funcionamiento del derecho de portabilidad tienen una escala mucho mayor que aquellos que afectan al concreto individuo que desea trasladar sus datos de un proveedor a otro. En segundo lugar, ello muestra que las implicaciones de la redacción dada al derecho de portabilidad tienen un amplio alcance económico y competitivo y no se circunscribe a la mejor protección del tratamiento de los datos personales o a la capacidad de control de un individuo sobre estos. En tercer lugar, esto también explicaría, por tanto, los incentivos para que la redacción final de este derecho contuviese las grandes excepciones y limitaciones que han sido ya expuestas.

En esencia, cabría incluso preguntarse si la normativa de protección de datos, en atención a su objeto de protección, es el instrumento jurídico más apropiado en el que incorporar un derecho tan cercanamente ligado a bienes jurídicos de naturaleza económica y anticompetitiva. En cualquier caso, el impulso del desarrollo de estándares comunes entre agentes sectoriales es un punto de partida positivo.

---

[501] FERNÁNDEZ-SAMANIEGO, Javier y FERNÁNDEZ-LONGORIA, Paula (2016): "El derecho a la portabilidad de los datos", en José Luís Piñar Mañas (dir.), Reglamento General de Protección de Datos: Hacia un nuevo modelo europeo de privacidad, Madrid, Reus, p. 273.

2.6.4. *Esfuerzos en favor de la interoperabilidad*

Algunas iniciativas de mejora ya se encuentran en la agenda. A nivel nacional, la AEPD ya ha manifestado desde hace años la necesidad de fomentar la interoperabilidad de los sistemas de fabricantes y proveedores de servicios de seguridad informáticas, así como de las redes sociales.[502]

Entre las iniciativas más recientes destaca el proyecto de código abierto Data Transfer Proyect, que centra sus esfuerzos en la creación de un marco común para la transferencia o portabilidad de datos entre servicios de manera sencilla y sin necesidad de que el individuo deba descargar la información por sí mismo. El proyecto cuenta ya con grandes compañías como contribuidoras, que incluyen Google, Microsoft, Twitter o Facebook.[503]

En paralelo, diversas compañías alegan la inversión en mejoras en sus estándares de portabilidad. Facebook, por ejemplo, ha desarrollado la funcionalidad "Descarga tu información",[504] que permite al usuario obtener una copia de su información en formato JSON file. La herramienta, que comenzó como un servicio de archivo personal para al individuo, evolucionó tras el escándalo de Cambridge Analytica y la entrada en aplicación del RGPD para convertirse en una herramienta de portabilidad de datos.[505] Sin embargo, Facebook ha mostrado continuas reticencias con respecto a permitir la posibilidad de descargar o exportar el listado de contactos de un individuo, algo especialmente interesante a la hora de migrar entre redes sociales. La posibilidad existe, pero la opción activada por defecto es aquella que no permite exportar el listado de contactos, lo cual resulta

---

[502] INSTITUTO NACIONAL DE TECNOLOGÍAS DE LA INFORMACIÓN Y AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (2009): *Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales online*, p. 16 y 58.

[503] SHANK, Craig (2018): "Microsoft, Facebook, Google and Twitter Introduce the Data Transfer Project: An Open Source Initiative for Consumer Data Portability", en *EU Policy blog*, de 20 de julio.

[504] Accesible desde https://www.facebook.com/help/1701730696756992?helpref=hc_global_nav.

[505] BANKSTON, Kevin (2018): *How Should Facebook and Other Companies Protect Privacy While Letting People Share Their Information Between Apps and Services?*

especialmente llamativo al tratarse de una de las pocas opciones que Facebook activa sistemáticamente por defecto para no compartir información con tus contactos.[506] Ello puede explicarse por el hecho de que la compañía ha considerado el listado de contactos y la gran red de conectividad de personas una de sus mayores ventajas competitivas.

De este modo, las limitaciones al derecho de portabilidad pueden generar deficiencias de mercado por las que los proveedores de un servicio generen o mantengan costes de cambio que dificulten al usuario el movimiento de sus datos a otro proveedor, creando consumidores cautivos.[507]

A pesar de todo ello, es especialmente relevante recordar que en la actualidad una cantidad cada vez mayor de datos no tienen un formato estructurado, e incluso cuando lo tienen, los formatos son diversos. De este modo, establecer una obligación de interoperabilidad provocaría diversas dificultades.[508] En primer lugar, crearía una gran presión sobre el legislador para concretar esta obligación con parámetros técnicos, en ocasiones dependientes del sector, la naturaleza o el origen de los datos, de muy compleja o imposible generalización. En segundo lugar, es razonable pensar que una redacción de este tipo podría quedar fácilmente desactualizada por el desarrollo tecnológico. Por último, crearía una carga en ocasiones desproporcionada sobre los responsables de garantizar en todo caso la comunicación entre sistemas y bases de datos que, dado el ecosistema de datos realmente existente sería prácticamente irrealizable. Por todo ello, quizás la inclusión de la salvedad de la viabilidad técnica como límite a un derecho de portabilidad sí cobre sentido. En orden a evitar situaciones de abuso de esta salvedad, no obstante, es necesario orientar

[506] BANKSTON, Kevin (2018): *How Should Facebook and Other Companies Protect Privacy While Letting People Share Their Information Between Apps and Services?*

[507] SLUIJS, Jasper P.; LAROUCHE, Pierre; SAUTER, Wolf (2006): “Cloud computing in the EU policy sphere”, en *TILEC Discussion paper*, 2006.

[508]FATHAIGH Ronan Ó.; VAN HOBOKEN, Joris (2019): “European Regulation of Smartphone Ecosystems”, en Data Protection Law Review, Vol. 5, No. 4.

esfuerzos en crear incentivos y conciencia en los responsables para trabajar en una mayor interoperabilidad de sistemas.

En esencia, parece que aún queda un largo camino para desarrollar estándares de interoperabilidad de bases de datos y servicios que faciliten el derecho de portabilidad reconocido en el art. 20 RGPD. Al mismo tiempo, es razonable pensar que las organizaciones pudieran tener incentivos en no invertir esfuerzos para facilitar dicha portabilidad respecto de determinados datos. Por ello, el desarrollo de una obligación jurídica de inversión razonable en estándares de interoperabilidad sería el punto de partida para permitir un ejercicio real de este nuevo derecho.

2.7. Efectos sobre otros interesados

Resulta también interesante resaltar que, de acuerdo con el párrafo 4 del art. 20 RGPD, el derecho de portabilidad no debe afectar negativamente a los derechos de otras personas. Sin embargo, en ocasiones al exportar un fichero, el interesado no solo lo hace respecto de datos personales que se refieren únicamente a él, sino que también los derechos de otras personas pueden ser incluidos.

Siguiendo con el ejemplo del individuo que desea portar sus datos entre redes sociales, surge el dilema de qué tratamiento debe darse a aquellos datos de otros usuarios de la red social. Ciertas cuestiones han sido ya planteadas por la doctrina. Pensemos, por ejemplo, en las fotografías, comentarios y "me gusta" intercambiados entre usuarios. ¿Existe un derecho a portar datos de tus contactos a otra red social en la que estos no quieren participar? ¿Sería necesario en este caso contar con mecanismos técnicos para solicitar el consentimiento de otros interesados para portar datos que se refieren a ellos? [509]

[509] VAN EIJK, Nico (2018): "*How Should Facebook and Other Companies Protect Privacy While Letting People Share Their Information Between Apps and Services?*.

En este sentido, el GT29 ha interpretado[510] que el responsable que recibe los datos portados por un interesado no podrá realizar un tratamiento de dichos datos para finalidades propias, más allá de permitir al interesado almacenar sus datos y controlarlos. Un tratamiento de datos ilícito en este sentido sería, por ejemplo, utilizar los datos de terceros con la finalidad de ofrecerles productos y realizar acciones comerciales, o realizar un perfilado de estos. Y ello debido a que, entre otros motivos, respecto de dichos datos y tales finalidades, el responsable no contará con una base de legitimación.

En cualquier caso, en la actualidad numerosas cuestiones permanecen abiertas, propias de la falta de desarrollo de los nuevos derechos que surgen a la luz de la digitalización y los servicios basados en datos.

En otro orden de cosas, también cabría interpretar que esta consideración a la protección que merecen los derechos de otros interesados incluye los derechos de propiedad intelectual o secretos comerciales. Así entendida, esta limitación al derecho de portabilidad está estrechamente relacionada con aquella de no portar datos elaborados por el responsable, como por ejemplo el resultado de un perfilado o de actividades de inferencia. Ciertamente, la protección del esfuerzo y la inversión de un responsable en el desarrollo de conocimiento y aplicaciones debe protegerse. Sin embargo, cabría preguntarse, de nuevo, si ello debe implicar, siempre y en todo caso, que el resultado más simplificado de un perfil del interesado realmente revelaría los métodos intelectuales que subyacen.

De la lectura de ambas limitaciones en conjunto parece extraerse que el legislador ha concluido que la capacidad de portar datos sobre, por ejemplo, el perfil de una persona, incluso en su vertiente más simplificada, entrañaría, *iuris et de iure*, un perjuicio para el responsable que ostente los derechos sobre el funcionamiento del algoritmo o la solución técnica que haya dado lugar a dicho perfilado. Perjuicio que, bajo dicha lógica merece

[510] GRUPO DE TRABAJO DEL ARTÍCULO 29 (2017): *Guidelines on the right to data portability* (WP 242 rev.01), de 5 de abril, p. 12. Adoptadas por el Comité Europeo de Protección de Datos.

una mayor protección que aquel perjuicio causado al interesado como consecuencia de no poder hacer uso de determinados datos a pesar de la creciente importancia de estos, hasta el punto de que configuran parte de la huella o personalidad digital del individuo.

3. Derecho de acceso

El derecho de acceso tiene un papel de especial relevancia para permitir al interesado ejercer un control real sobre los datos personales que le conciernen, así como para facilitar el correcto ejercicio de otros derechos[511] reconocidos por el RGPD. Es decir, el derecho de acceso goza de especial relevancia intrínseca por su contenido propio, pero también actúa como bisagra o instrumento para un correcto ejercicio de otros derechos.

Las raíces del derecho de acceso pueden buscarse ya en el Convenio 108 (1981)[512] cuyo artículo 8 indicaba que el interesado deberá estará habilitado para obtener, sin demora excesiva y sin coste, confirmación acerca de si datos personales relativos a él están siendo almacenados en un fichero automatizado, así como la comunicación de dichos datos de forma inteligible.

Siguiendo esta estela, el derecho de acceso continuó formando parte esencial de la Directiva y del actual RGPD. El art. 15 RGPD reconoce el derecho de acceso y otorga al interesado las siguientes potestades:

- La capacidad del interesado de requerir al responsable confirmación sobre si se está realizando un tratamiento de datos personales referidos a este.
- Obtener determinada información relativa al tratamiento.

[511] TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA (2017): Asunto C-434/16, Peter Nowak vs Data Protection Commissioner, de 20 de diciembre. ECLI:EU:C:2017:994; TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA (2009): Asunto C-553/07, College van burgemeester en wethouders van Rotterdam v MEE Rijkeboer, de 7 de mayo. ECLI:EU:C:2009:293.

[512] CONSEJO DE EUROPA (1981): Convenio 108, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal.

- Obtener una copia de los datos objeto de tratamiento.

Entre la información que debe prestar el responsable durante el ejercicio de un derecho de acceso cabe destacar aquella que se refiere a las finalidades del tratamiento, las categorías de datos personales tratados, los destinatarios (o al menos la categoría de destinatarios a los que se comuniquen los datos), la fuente de los datos personales cuando estos no fueron obtenidos del interesado o las garantías que se hubieran establecido en caso de que exista una transferencia internacional de datos personales. Asimismo, el responsable debe informar al interesado de la posibilidad de que este ejerza otros derechos, tales como rectificación, supresión, limitación del tratamiento u oposición. Del mismo modo, el responsable debe informar también acerca de la existencia de decisiones automatizadas junto con información significativa de la lógica aplicada y sus consecuencias previstas.

El contenido de la información a la que tiene derecho el interesado se ha visto aumentado en el RGPD respecto de la Directiva, de modo que podría concluirse que este derecho mejora la posición del interesado para ejercer un control sobre los datos personales que se refieren a él.

3.1. El gran límite del derecho de acceso

A pesar de que el RGPD parece mejorar la efectividad del derecho de acceso, existe una gran limitación que puede poder en entredicho esta afirmación.

El considerando 63 RGPD, relativo al derecho de acceso, indica que, si el tratamiento de los datos personales se refiere “a una gran cantidad de información relativa al interesado, el responsable del tratamiento debe estar facultado para solicitar que, antes de facilitarse la información, el interesado especifique la información o actividades de tratamiento a que se refiere la solicitud”.

Así, cuando el volumen de información acerca del interesado sea elevado, este debe concretar sobre qué datos desea ejercer su derecho de acceso,

de lo que se puede desprender que el RGPD no contiene una obligación de aportar todos los datos e información sobre el interesado que el responsable trata cuando esta supone un volumen elevado. Esto puede restringir mucho el ejercicio real del derecho de acceso por parte del interesado debido a cinco motivos principales.

3.1.1. *El derecho de acceso como base para otros derechos*

En primer lugar, el derecho de acceso puede ser la base para obtener la información necesaria para el ejercicio de otros derechos subsiguientes, tales como un derecho de oposición, de supresión o de no ser objeto de decisiones automatizadas. Puede también ser necesario para ejercer facultades incluidas en estos derechos, tales como la contestación a la decisión automatizada con argumentos. Por este motivo, y de manera más significativa en la economía de datos actual, la restricción del derecho de acceso puede perpetuar e incluso favorecer asimetrías de información.

3.1.2. *La falta de acceso a todos los datos*

En segundo lugar, cuando la cantidad de datos personales que el responsable trata sea abundante, parece que el interesado no goza de un derecho absoluto a acceder a dichos datos de forma directa (ergo, con la facilidad que predica el considerando), sino que puede ser compelido a detallar qué información desea obtener.

Esto es relevante por cuanto, precisamente cuando un responsable trata un gran volumen de datos sobre un interesado, mayor será el interés de este en acceder a toda la información, ejercer su capacidad de control y verificar que el tratamiento es lícito.

Así, despojar al interesado de la capacidad de acceder a una información lo más completa posible, precisamente cuando las actividades de recolección y tratamiento de datos son más complejas que nunca, supone una gran limitación.

3.1.3. *Qué es gran cantidad de información*

En tercer lugar, el RGPD no incluye parámetros para delimitar cuándo puede un responsable considerar que está tratando una gran cantidad de información, ni si esta expresión debe equipararse a aquella de "tratamiento a gran escala" que se utiliza en diversas ocasiones a lo largo del RGPD. En su caso, el tratamiento a gran escala de datos personales puede desplegar mayores obligaciones del responsable, como aquella de llevar a cabo una evaluación de impacto o de designar a un delegado de protección de datos.

Parece que el uso de expresiones diferentes –"gran cantidad de información" versus "tratamiento a gran escala"- implica que el significado de ambas no sea necesariamente idéntico. De este modo, cabría pensar en que existirán situaciones en las que no quepa interpretar que se está realizando una evaluación de interesados a gran escala, y por tanto, no será necesario nombrar un delegado de protección de datos, pero en los que el responsable sí pueda argumentar que el volumen de datos objeto de tratamiento es de magnitud suficiente como para no responder a un derecho de acceso generando una copia de absolutamente todos los datos.

En este caso, quedaría a la opinión subjetiva del responsable cuándo se produce esta situación.

3.1.4. *Más riesgo, menos protección*

En cuarto lugar, determinados contextos como la prestación de servicios de la sociedad de la información, el uso de redes sociales o de aplicaciones móviles conllevan la generación, recogida y almacenamiento de grandes cantidades de datos y metadatos. En muchas ocasiones, esta información primaria es posteriormente sometida a analítica para ampliar el conocimiento del responsable lo que, por último, revierte en la creación de perfiles o la toma de decisiones sobre el interesado. Es decir, los servicios digitales actuales hacen cada vez mayor uso del flujo de datos que fue descrito en las fases del big data. Así, precisamente aquellos tratamientos que más riesgo e incomprensión pueden causarle al interesado quedan sujetos a un menor nivel de protección y de control.

3.1.5. *Falta de capacidad para especificar*

En quinto lugar, recordemos que el considerando 63 no indica que en estos casos no opere el derecho de acceso, sino que el interesado debe poder especificar qué información desea, ya sea concretando qué tipo de información desea conocer o sobre qué actividades de tratamiento.

Pues bien, el interesado medio razonable no dispondrá, en una gran cantidad de casos, del conocimiento ni aptitudes necesarias para ser capaz de especificar a qué información concreta desea acceder o sobre qué actividades del tratamiento desea obtener información. A mayor abundamiento, pareciera que el responsable puede ejercer una negativa al ejercicio del derecho y a aportar información alguna en tanto el usuario no responda en dichos términos específicos.

Pensemos en el usuario de una aplicación móvil que recoge un amplio abanico de datos personales para multitud de finalidades, entre ellas, la realización de perfiles y la subsecuente personalización del servicio. Si este usuario desea ejercer un derecho de acceso ¿debe especificar de antemano su interés en recibir información sobre la toma de decisiones automatizadas y la lógica aplicada para la concreta finalidad de elaboración de perfiles? Parece congruente pensar que un usuario medio carezca del conocimiento siquiera para poder realizar dicha petición, incluso cuando hubiera sido informado, en el momento de la descarga de la app, de la posible creación de perfiles, conforme a los arts. 13 y 14 RGPD.

3.1.6. *El responsable también debe concretar*

La lógica indicaría que el responsable debiera, cuanto menos, sujetarse a la obligación de facilitar el acceso a un principio de información mínima, así como guiar al interesado en la petición de la información específica sobre la que desea ejercer su derecho. Sin embargo, nada se dice en el RGPD de esta obligación, de modo que es previsible la práctica generalizada de los responsables no siga esta pauta.

El art. 12.2 RGPD impone al responsable la obligación de facilitar el ejercicio de los derechos por parte del interesado. Pues bien, de ello puede

extraerse que, ante un ejercicio de derecho de acceso relativo a una gran cantidad de información, el responsable debe remitir al interesado aquella información a que se refiere el art. 15.1 en la medida de lo posible (aquella relativa a los fines del tratamiento, las categorías de datos tratadas, destinatarios, lógica aplicada en caso de existencia de decisiones automatizadas o posibles consecuencias, etc.), así como cualquier otra información acerca de las actividades del tratamiento que sea suficiente para que este sea capaz de concretar la petición de acceso de manera efectiva.

Es decir, el responsable deberá garantizar que revela información lo suficientemente precisa y transparente que permita al interesado realizar la labor de concretar su derecho de acceso. De este modo, el interesado recibe información en diferentes momentos. En primer lugar, la información requerida en los arts. 13 y 14 RGPD, que debe ser provista antes del inicio del tratamiento, es decir información *ex ante*. En segundo lugar, aquella información aportada tras el tratamiento y durante el ejercicio del derecho de acceso conforme al art. 15 RGPD, con el objetivo de permitir al interesado poder especificar el alcance del derecho ejercido, o lo que podríamos bautizar como información *in media res*. En tercer lugar, aquella información y datos personales que el interesado recibe como respuesta final a su derecho de acceso, esto es, información *ex post*.

3.2. Relación entre los derechos de acceso y de portabilidad

El ejercicio de un derecho de acceso faculta al interesado a recibir una copia de los datos personales objeto del tratamiento. Dicha copia deberá facilitarse “en formato electrónico de uso común” cuando la solicitud de acceso hubiera sido realizada por medios electrónicos.

Por su parte, como vimos anteriormente, el derecho de portabilidad faculta al interesado, entre otras cosas a recibir una copia de los datos “en un formato estructurado, de uso común y lectura mecánica”.

A simple vista, existen claras similitudes entre ambos derechos, hasta el punto de poder parecer reiterativos. Por ello, cabría preguntarse ¿es el derecho de portabilidad una variante específica del derecho de acceso? ¿Cuál es la relación entre ambos derechos?

En ocasiones se argumenta que el derecho de portabilidad complementa al derecho de acceso del interesado en la medida en que le permite acceder a sus datos personales en un formato reutilizable y moverlos entre diferentes servicios.[513] En efecto, el derecho a obtener una copia de los datos personales tratados por el responsable -y que cumplan los requisitos del art. 20 RGPD- complementa al derecho de acceso a los datos personales del art. 15 RGPD. De hecho, durante el proceso legislativo de redacción del RGPD, el informe del Comité LIBE sobre el borrador de Reglamento proponía incluir el derecho de portabilidad dentro del art. 15, sobre derecho de acceso, de forma que la portabilidad quedaba relegada a una vertiente del derecho de acceso.[514] Sin embargo, se aprecian diferencias entre ambos derechos.

3.2.1. *Tipo de datos*

El derecho de portabilidad únicamente concierne a los datos aportados por el interesado y aquellos observados, mientras que el derecho de acceso no se limita en este sentido.

Como hemos analizado, uno de los límites principales del derecho de portabilidad es precisamente el hecho de que este no cubre los resultados de una actividad de perfilado ni los datos inferidos sobre el interesado. Pues bien, parece que a través del ejercicio de un derecho de acceso el interesado sí tendría derecho a conocer esta información. En este mismo

[513] GRUPO DE TRABAJO DEL ARTÍCULO 29 (2017): *Guidelines on the right to data portability* (WP 242 rev.01), de 5 de abril, p. 5. Adoptadas por el Comité Europeo de Protección de Datos; AUTORITAT CATALANA DE PROTECCIÓ DE DADES (2018): *Dictamen en relación con la consulta formulada por un ayuntamiento sobre el ejercicio del derecho a la portabilidad en el ámbito del ayuntamiento*, CNS 54/2018, de 22 de octubre.

[514] FERNÁNDEZ-SAMANIEGO, Javier y FERNÁNDEZ-LONGORIA, Paula (2016): "El derecho a la portabilidad de los datos", en José Luís Piñar Mañas (dir.), Reglamento General de Protección de Datos: Hacia un nuevo modelo europeo de privacidad, Madrid, Reus, p. 265 y ss.

sentido se expresan voces reconocidas como Javier Aparicio[515] y así también lo ha entendido tradicionalmente el legislador español quien ya en el Reglamento de desarrollo de la anterior LOPD (RLOPD)[516] indicaba que el derecho de acceso conlleva aportar la información y datos resultantes de cualquier elaboración o proceso informático (art. 29. 3 RLOPD).

Por este motivo, ante la situación por la que una persona haya recibido información que considera escasa en respuesta a un ejercicio de portabilidad, esta podrá ejercer un derecho de acceso, obligando al responsable a proporcionar un nivel más detallado de datos.[517]

3.2.2. *Base de legitimación*

El derecho de acceso es ejercitable independientemente de la base de legitimación, mientras que, como vimos, el derecho de portabilidad únicamente se aplica bajo ciertas bases. Este extremo tiene consecuencias de trascendencia.

Ya hemos analizado por qué la restricción de las bases de legitimación supone un gran límite al derecho de portabilidad. De hecho, esto es visto como uno de los grandes beneficios de los responsables para la utilización del interés legítimo como base del tratamiento. Asimismo, como vimos, parece que esta exclusión no es del todo comprensible en términos de pura técnica jurídica. En todo caso, este límite es plenamente aplicable, lo que significa que los interesados tendrán un veto a portar este tipo de información, relevante para sus intereses.

---

[515] APARICIO SALOM, Javier (2019): "Derecho de oposición y decisiones individuales automatizadas. Limitaciones (Arts. 21-23 RGPD. Art. 18 LOPDGDD)" en Javier López Calvo (coord.), *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD*. Madrid, Wolters Kluwer, p. 184.

[516] Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

[517] GRUPO DE TRABAJO DEL ARTÍCULO 29 (2017): *Guidelines on the right to data portability* (WP 242 rev.01), de 5 de abril, p. 7. Adoptadas por el Comité Europeo de Protección de Datos.

Sin embargo, aquél interesado que encuentre dificultad para poder obtener una copia de los datos referidos a él a través del ejercicio de un derecho de portabilidad contará, al menos, con la capacidad de obtener dicha copia a través de un derecho de acceso incluso cuando el tratamiento se base en el interés legítimo del responsable.

3.2.3. *Formato de los datos*

El derecho de acceso incluye la prerrogativa de obtener los datos en un "formato electrónico de uso común" cuando la solicitud se hubiera hecho por medios electrónicos, mientras que el derecho de portabilidad conlleva obtener los datos en un "formato estructurado y de lectura mecánica".

Así, un interesado que ejerce su derecho de acceso a través de medios no electrónicos, por ejemplo, por correo postal, podrá recibir la información en papel. Si hubiera realizado la solicitud a través de un correo electrónico habilitado al efecto por el responsable, podrá obtener la información en un archivo adjunto a un email en, por ejemplo, formato PDF no editable. Este modo de acceder a la información no sería idóneo en caso de que el interesado quisiera ejercer su derecho de portabilidad, pues un PDF no es un formato estructurado de lectura mecánica.

El motivo de esta discrepancia a la hora de recibir la información al ejercer estos derechos se encuentra en el fundamento propio de cada uno de ellos. El derecho de acceso nace como una garantía de la persona que le permita ejercer una capacidad de control sobre los datos, y por ello la información que reciba debe ser fácilmente accesible y legible por la persona. Para ello, un archivo en, por ejemplo, formato PDF permitiría cumplir con esta función. Por su parte, el derecho de portabilidad se basa en la idea básica de permitir que sea otro responsable quien pueda acceder y hacer uso de la información cuando el interesado así lo desee, y por ello los datos portados deben ser legibles a través de medios mecánicos.

En cualquier caso, aquellos formatos que no son mecánicamente legibles, como un PDF, dificultan el ejercicio de un control efectivo por parte del interesado. En efecto, si bien un formato PDF cumple estrictamente con lo

legalmente requerido -esto es, aportar la información al interesado en un formato electrónico de uso común-, no es el modo óptimo de dar respuesta a una solicitud de acceso. Todo ello es cuanto más cierto debido a que, generalmente, el responsable almacena la mayor parte de los datos personales asociados a una persona en formatos estructurados tales como ficheros compuestos por filas y columnas. Este modo de almacenar los datos es el que permite extraer mayor valor y analizar la información y es quizás el medio más eficiente de recoger y conservar tipos de datos específicos como metadatos.

3.3. La importancia del derecho de acceso

Todo lo anterior ayuda a explicar el papel tan relevante que el derecho de acceso tiene para el interesado en la protección de los datos personales que le conciernen, especialmente en un momento en el que cada vez es mayor la proporción de datos inferidos (versus los datos originales brutos) que se tratan de cada uno de nosotros, con consecuencias de mayor alcance. Asimismo, es previsible pensar que cada vez será mayor la cantidad y proporción de tratamientos soportados en bases de legitimación diferentes al consentimiento, y especialmente de tratamientos basados en interés legítimo. Por ello, aquellos derechos aplicables con independencia de cuál sea la base del tratamiento adquieren, si cabe, mayor relevancia.

Lo visto hasta ahora permite obtener la conclusión preliminar de que, a pesar de sus limitaciones, el derecho de acceso también puede llegar a ser un salvoconducto para el interesado, pues permite bordear algunas limitaciones de otros derechos como el de portabilidad y concretar el principio de transparencia, especialmente en lo que se refiere al tratamiento de datos creados por el responsable a través de medios automatizados y a partir de modelos algorítmicos.

Hemos analizado algunas de las principales implicaciones de los derechos de acceso y portabilidad en relación con la utilización de tecnologías big data y la elección de diferentes bases de licitud del tratamiento, así como

la relación entre estos derechos. A continuación, nos centraremos en otra importante disposición también relacionada con estos aspectos.

4. Decisiones individuales automatizadas

La regulación de las decisiones automatizadas no es nueva en la ordenación de la protección de los datos personales, sino que ya se encontraba en la Directiva de 1995, cuyo art. 15 reconocía el derecho de los individuos a no ser sometidos a decisiones basadas únicamente en un tratamiento automatizado que tuvieran efectos jurídicos sobre estos o les afectase de manera significativa. No obstante, se trataba de una disposición poco conocida e infrautilizada.[518] Este hecho ha cambiado con la llegada del RGPD, que contiene cuatro provisiones directamente aplicables a este tipo de tratamiento, y han recibido gran atención y cuya interpretación está lejos de ser uniforme.

Los cuatro artículos del RGPD que mencionan expresamente los tratamientos de datos que conlleven la toma de decisiones totalmente automatizadas son, por un lado, el art. 22 (desarrollado mediante el considerando 71). Este artículo establece un derecho a no ser objeto de decisiones automatizadas. Por otro lado, los artículos 13, 14 y 15, dedicados respectivamente a los derechos de información y acceso, contemplan deberes de transparencia en relación con este tipo de tratamientos.

Existe un ferviente debate en torno a diversas cuestiones relacionadas con la toma de decisiones automatizadas, desde el alcance del deber de transparencia del responsable hasta la existencia o no de un derecho del interesado a recibir una explicación sobre decisiones automatizadas que se hayan tomado sobre él. En este epígrafe nos adentramos en algunas de estas cuestiones.[519]

---

[518] ZARSKY, Tal (2017): "Incompatible: The GDPR in the Age of Big Data", en *Seton Hall Law Review*, Vol. 47, No. 2.

[519] Para un análisis más profundo en torno a otras cuestiones relacionadas con decisiones algorítmicas ver: WACHTER, Sandra; MITTELSTADT, Brent; FLORIDI, Luciano (2016):

4.1. La redacción poco clara del artículo 22 RGPD

El artículo 22 RGPD, abajo reproducido, utiliza una redacción enrevesada y poco clara que ha suscitado enormes esfuerzos interpretativos y debates.

Este artículo consagra un derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en el interesado o le afecte significativamente de modo similar.

Este derecho se exceptúa en tres circunstancias: cuando así lo reconozca la legislación de un Estado miembro, cuando el interesado hubiese prestado su consentimiento o cuando el tratamiento fuere necesario para la ejecución de un contrato. En el primer caso, la norma nacional habilitante debe contener medidas adecuadas para salvaguardar los derechos del interesado, aunque la poca concreción del apartado ha provocado que llegue a ser denominado una "escotilla de alcance impreciso" de la norma con capacidad para cristalizar sesgos, errores o discriminación.[520] En los otros dos casos, será el responsable el que deba indicar las medidas de salvaguarda que ha adoptado para proteger los derechos de los interesados, que deberán ser, como mínimo, el derecho del interesado a obtener intervención humana por parte del responsable, a expresar su punto de vista y a impugnar la decisión.

Por último, la toma de decisiones automatizadas del art. 22 únicamente podrán basarse en categorías especiales de datos del art. 9 RGPD cuando exista consentimiento explícito o interés vital del interesado y, del mismo modo, deberán estar sujetas a garantías adecuadas.

"Why a right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation", en *International Data Privacy*, Vol 7, No. 2; VEALE, Michael; EDWARDS, Lilian (2018): "Clarity, Surprises, and Further Questions in the Article 29 Working Party Draft Guidance on Automated Decision-Making and Profiling", en *Computer Law & Sexurity Review*, Vol. 34, No. 2; MALGIERI, Gianclaudio; COMANDÉ, Giovanni (2017): "Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation", en *International Data Privacy Law*, Vol. 7, No. 4.

[520] DE LA QUADRA-SALCEDO FERNÁNDEZ DEL CASTILLO, Tomás (2018): "Retos, riesgos y oportunidades de la sociedad digital", en Tomás de la Quadra-Salcedo y José Luis Piñar (dirs.), Sociedad digital y Derecho, Madrid, BOE-Red.es, p. 58.

La interpretación de los diferentes términos ambiguos del art. 22. conllevará que el art. 22 sea aplicable o no, así como el alcance y utilidad de todas sus garantías asociadas.

Artículo 22. Decisiones individuales automatizadas, incluida la elaboración de perfiles

1. **Todo interesado tendrá derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado**, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar.
2. El apartado 1 no se aplicará si la decisión:
   a. es necesaria para la celebración o la ejecución de un contrato entre el interesado y un responsable del tratamiento;
   b. está autorizada por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento y que establezca asimismo medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, o
   c. se basa en el consentimiento explícito del interesado.
3. En los casos a que se refiere el apartado 2, letras a) y c), el responsable del tratamiento adoptará las medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, ***como mínimo el derecho a obtener intervención humana por parte del responsable, a expresar su punto de vista y a impugnar la decisión***.
4. Las decisiones a que se refiere el apartado 2 no se basarán en las categorías especiales de datos personales contempladas en el artículo 9, apartado 1, salvo que se aplique el artículo 9, apartado 2, letra a) o g), y se hayan tomado medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado.

Considerando 71

(71) El interesado debe tener derecho a no ser objeto de una decisión, que puede incluir una medida, que evalúe aspectos personales relativos a él, y que se base únicamente en el tratamiento automatizado y produzca efectos jurídicos en él o le afecte significativamente de modo similar. (…) En cualquier caso, dicho tratamiento debe estar sujeto a las garantías apropiadas, entre las que se deben incluir la información específica al interesado y el derecho a obtener intervención humana, a expresar su punto de vista, ***a recibir una explicación de la decisión tomada después de tal evaluación*** y a impugnar la decisión. Tal medida no debe afectar a un menor.

4.2. ¿Derecho o prohibición?

Muchas de las conclusiones en relación con la transparencia y cómo ofrecer información sobre decisiones automatizadas son extrapolables al contexto de esta tesis: por ejemplo, informar al usuario sobre tratamientos complejos, novedosos, cambiantes y el reconocimiento de la dificultad que ello crea para prestar consentimiento.

Un posible modo de interpretar la naturaleza del art. 22 es entender que este consagra un derecho a que el interesado manifieste una negativa a que sus datos sean objeto de tratamiento con la finalidad de tomar decisiones totalmente automatizadas que le afecten. Esta postura ha sido defendida por parte de algunos juristas.[521]

La primera consecuencia de esta aproximación sería que el interesado debería ejercitar de manera activa su potestad para hacer efectivo el art. 22. De este modo, el responsable podría llevar a cabo tratamientos de toma de decisiones totalmente automatizadas o de creación de perfiles sin necesidad de cumplir con los requisitos del art. 22, y únicamente tras la petición del interesado, restringiría este tipo de tratamientos a aquellos casos exceptuados. Así, por ejemplo, un responsable podría llevar a cabo actividades automatizadas de elaboración de perfiles con base en su interés legítimo -siempre que ello cumpliera con todo lo dispuesto en el art. 6.1.f) RGPD-. Cuando el interesado manifestase discrepancias y ejercitase su derecho conforme al art. 22, el responsable debería detener el tratamiento o encontrar alguna excepción, por ejemplo, solicitar el consentimiento. De este modo, esta interpretación favorece en gran medida la posición de los responsables del tratamiento.

Bajo esta interpretación, en la práctica, el art. 22 se configuraría de modo similar al derecho de oposición. Es decir, el responsable podría iniciar

[521] Véase, a título de ejemplo, APARICIO SALOM, Javier (2019): “Derecho de oposición y decisiones individuales automatizadas. Limitaciones (Arts. 21-23 RGPD. Art. 18 LOPDGDD)” en José López Calvo (coord.), *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD*. Madrid, Wolters Kluwer.

tratamientos que culminasen con decisiones automatizadas, y debería abstenerse de ello una vez que el individuo comunicase su negativa. Esto provocaría que fuese el responsable quien ostentase la responsabilidad de valorar si se cumplen las condiciones que permiten ejercitar el derecho del art. 22, y decidiese si debe ser atendido o no. En consecuencia, ello podría propiciar que el responsable tuviese incentivos para dificultar el ejercicio de este derecho, así como para no ser transparente en lo que se refiere a la información sobre la existencia misma de las decisiones automatizadas o la lógica aplicada (arts. 13, 14 y 15).

En esencia, este modo de interpretar el art. 22 generaría graves perjuicios para el interesado y diluiría en gran medida la protección que el propio artículo pretende aportar. Sin embargo, parece que esta no era la intención del legislador al redactar la disposición, y que, por tanto, debe ser interpretada de otro modo.

La interpretación del art. 22 como una prohibición expresa aportaría una protección más reforzada para los intereses de los sujetos.

Visto como una prohibición, el art. 22 RGPD impide al responsable llevar a cabo procesos de toma de decisiones automatizadas del apartado primero salvo en tres circunstancias: que cuente con el consentimiento explícito del interesado, demuestre la necesidad del tratamiento para ejecutar un contrato o cuente con una habilitación legal. Así, el art. 22 opera por defecto, sin necesidad de que el interesado ejercite su derecho o actúe. Esta es, de hecho, la postura del GT29, ahora CEPD,[522] y la posición finalmente asumida por la mayor parte de agentes.[523]

[522] GRUPO DE TRABAJO DEL ARTÍCULO 29, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679* (WP 251 rev.01), de 6 de febrero. Adoptadas por el Comité Europeo de Protección de Datos.

[523] A título de ejemplo, véase WACHTER, Sandra; MITTELSTADT, Brent; FLORIDI, Luciano (2016): "Why a right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation", en *International Data Privacy*, Vol 7, No. 2; CONSEJO DE LA UNIÓN EUROPEA (1992): *Amended proposal for a Council Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data* COM(92) 422 final - SYN 287, de 15 de octubre.

De este modo, la confusa estructura del art. 22 habilita al interesado a exigir del responsable que finalice el tratamiento en los casos no permitidos, por ejemplo, cuando la base utilizada hubiese sido el interés legítimo. Más que el ejercicio de un derecho en sentido estricto, lo que el interesado estaría reclamando es la terminación de un acto ilícito, nulo de pleno derecho. Así, esto supone en primer lugar que el responsable ha incurrido en una infracción sancionable del RGPD. En segundo lugar, esto podría tener un efecto en cadena y suponer que cualquier efecto jurídico derivado de dicha decisión y la cadena de decisiones posteriores a esta sean consideradas nulas de pleno derecho, y no únicamente anuladas. Los efectos de esto aguas abajo pueden ser diversos, complejos y difíciles de gestionar para el responsable.

Por su parte, aquellos tratamientos de decisiones automatizadas basadas en el consentimiento o la necesidad para la ejecución contractual deberán llegar a su fin cuando el interesado retire su consentimiento o finalice el contrato.

De este modo, entendido como una prohibición, comienzan a apreciarse diferencias entre el derecho de oposición y el derecho a no ser objeto de decisiones basadas únicamente en el tratamiento automatizado.

En primer lugar, el derecho de oposición despliega el efecto de finalizar el tratamiento para una finalidad concreta desde el momento en que se ejerce, mientras que el derecho del art. 22 supone la terminación del tratamiento de manera retroactiva, desde el momento en que este se inició, en caso de que este hubiera tenido lugar fuera de los casos explícitamente permitidos por la norma.

Segundo, el derecho de oposición es relativo, tal y como vimos en el capítulo anterior, pues el responsable posee la capacidad para reexaminar si ostenta motivos legítimos imperiosos por los que el tratamiento deba continuar. Por su parte, el “derecho” a no ser objeto de decisiones automatizadas es absoluto, por cuanto el interesado ostenta la garantía de que el tratamiento no debe producirse fuera de los casos permitidos o que,

en su caso, deba finalizar inmediatamente, restaurarse la situación anterior e imponerse una sanción al responsable.

Sin embargo, algunas de las garantías mencionadas en el art. 22.3 sí podrían asemejarse a una suerte de derecho de oposición. En efecto, el apartado tercero del art. 22 indica que, cuando el tratamiento se base en el consentimiento o contrato, el responsable debe garantizar, como mínimo que el interesado tenga derecho a obtener intervención humana, expresar su punto de vista e impugnar la decisión. Pues bien, precisamente la capacidad de expresar su punto de vista, unida a aquella de impugnar la decisión, juegan un papel similar a la capacidad del interesado de oponerse a una finalidad del tratamiento por motivos relacionados con su situación particular. Sin embargo, estas garantías operan con el objetivo de cuestionar o modificar el sentido de una decisión particular una vez esta ha sido tomada, pero no en el sentido de cuestionar la licitud del tratamiento per se, una diferencia que no es meramente teórica.

4.3. Excepciones y bases de licitud

El apartado segundo del art. 22 indica que la prohibición genérica a la toma de decisiones totalmente automatizadas que tengan un impacto sobre el interesado podrá salvarse en tres circunstancias: cuando exista una habilitación legal, cuando el interesado hubiese prestado su consentimiento explícito o cuando el tratamiento sea necesario para ejecutar un contrato entre el interesado y el responsable. En los tres casos, el tratamiento debe contar con medidas adecuadas de salvaguarda.

4.3.1. *Habilitación legal*

En el primer caso, la norma comunitaria o nacional que permita el tratamiento debe contener dichas medidas de salvaguarda que deben ser “adecuadas”. Es notable que el RGPD no exige que sean “específicas”, hecho que sí exige en otros preceptos. Así, se abre la posibilidad de que la norma que habilite el tratamiento podría esbozar una serie de garantías y

remitirse a una norma de desarrollo u otro instrumento jurídico para desarrollar y especificar dichas medidas.

Esta excepción abre la puerta a que sean los Estados miembros quienes decidan permitir, por ejemplo, tecnologías de reconocimiento facial para determinadas finalidades o cámaras de control de velocidad que envíen de forma automática una multa cuando el conductor infringe los límites, etc., siempre sujeto a garantías que salvaguarden la licitud y lealtad del tratamiento.

4.3.2. *Consentimiento y ejecución contractual*

En los otros dos casos debe ser el propio responsable quien determine cuáles son las medidas de salvaguarda adecuadas, a partir del conocimiento que se le presupone del tratamiento y de sus consecuencias. En este caso, el RGPD tampoco menciona que las medidas deban ser "específicas", sin embargo, parece que así debiera ser.

En primer lugar, porque el propio párrafo tercero del art. 22 ya propone un elenco mínimo de garantías específicas que deberán ser garantizadas en todo caso por el responsable, amén de que pueda incrementarlas. Dichas garantías son el derecho del interesado a obtener intervención humana, expresar su punto de vista e impugnar la decisión automatizada.

En segundo lugar, porque el responsable que lleve a cabo este tipo de decisiones estará obligado en muchas ocasiones a realizar acciones previas tales como una evaluación de impacto conforme al art. 35 RGPD donde, en aplicación del principio de responsabilidad proactiva, deberá haber detallado qué posibles medidas se implementarán para mitigar los riesgos analizados.

4.3.3. *¿Otras bases de licitud?*

El art. 22 parece excluir el interés legítimo como base de licitud para aquellos tratamientos de decisiones automatizadas, incluida la elaboración de perfiles, que reúnan las características del apartado primero -que se

trate de tratamientos totalmente automatizados y que produzcan efectos jurídicos o de otro modo significativos para el interesado-.

Parece, asimismo, que el motivo de ello podría no tener un fundamento jurídico claro, sino ser fruto del proceso largo, complejo y tedioso de redacción y negociación de enmiendas durante el proceso de elaboración del RGPD que dio como resultado final un compromiso político. De hecho, durante el proceso legislativo que culminó con la creación del RGPD, una de las propuestas incluía la posibilidad de llevar a cabo la toma de decisiones automatizadas basadas en el interés legítimo del responsable.[524] Otra enmienda proponía no limitar la toma de decisiones automatizadas en función de la base de legitimación, sino en función de los efectos negativos de la decisión, prohibiendo aquellas que desencadenaran un resultado desleal ("*unfair*") o discriminatorio.[525] Finalmente, esta provisión fue suprimida, eliminando la posibilidad de que el art. 6.1.f) pueda ser una de las bases que sustente la toma de decisiones totalmente automatizadas.

En este sentido, puede decirse que el borrador de Reglamentoe-Privacy sigue esta misma estela, sobre la que aquellos tratamientos a los que se presupone un grado de sensibilidad o riesgo mayor deban ser autorizados por el interesado mediante su consentimiento o la firma de un contrato, o por los Estados miembros a través de su desarrollo legislativo.

---

[524] PARLAMENTO EUROPEO, COMISIÓN DE INDUSTRIA, INVESTIGACIÓN Y ENERGÍA (2013): *Opinión para la Comisión de Libertades Civiles, Justicia y Asuntos de Interior sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo 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)* (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)), de 26 de febrero. Enmienda 185.

[525] PARLAMENTO EUROPEO, COMISIÓN DE MERCADO INTERIOR Y PROTECCIÓN DEL CONSUMIDOR (2013): *Opinión para la Comisión de Libertades Civiles, Justicia y Asuntos de Interior sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo 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)* (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)), de 28 de enero. Enmienda 130.

Sin embargo, el consentimiento o la ejecución de un contrato pueden no cubrir todos los aspectos relacionados con la toma de decisiones automatizadas, y en este sentido, restringir el ámbito de aplicación de las decisiones automatizadas podría llegar a ser contraproducente. Por ejemplo, en relación con el desarrollo de la conducción autónoma, pensemos en el uso necesario de datos referentes a peatones u otros conductores, que no han prestado su consentimiento ni firmado un contrato.[526] Por otro lado, la dependencia de una habilitación legal puede retrasar la utilización de nuevos desarrollos tecnológicos.

Por todo ello, una buena aproximación sería la ampliación de las bases de licitud en relación con el art. 22 RGPD para incorporar el interés legítimo, siempre sujeto a garantías debidas y estrictas. Esto abriría la puerta al uso del interés legítimo como base del tratamiento para actividades relacionadas con inteligencia artificial, big data y otras tecnologías sin supervisión humana durante la que hemos descrito como Fase 3-Aplicación con las precauciones necesarias para proteger a los interesados.

4.4. ¿Cuándo existe una decisión automatizada del artículo 22?

La confusión creada por la redacción del art. 22 no finaliza. Además de los problemas interpretativos en torno a la naturaleza propia del art. 22, y una vez hemos logrado definir que se trata de una prohibición sujeta a excepciones en los que se permite la toma de decisiones automatizadas, nos encontramos ante otros problemas.

La prohibición opera solo respecto de aquellas decisiones potencialmente más lesivas, definidas en el apartado primero del art. 22 como “decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en [el interesado] o le afecte significativamente de modo similar”. Es decir, deben darse de forma

[526] HOFFMAN, David; MASUCCI, Riccardo (2018): “Intel’s AI Privacy Policy White Paper. Protecting individuals’ privacy and data in the artificial intelligence world”, en *Intel Corporation*.

cumulativa varios requisitos para que una decisión específica quede sujeta al art. 22.

Queda fuera del ámbito de este trabajo comentar pormenorizadamente todas las posibilidades que estos términos ambiguos crean, baste aquí con resumir algunas de las conclusiones principales a las que han llegado el GT29, ahora CEPD, y la doctrina.

4.4.1. *Decisión "únicamente" automatizada*

Resulta de grandísima importancia poder concretar qué tipo de tratamientos cumplirían esta decisión, pues una visión rígida provocaría que la existencia de una persona humana que tuviera atribuidas funciones formales de revisión de decisiones algorítmicas provocara que el tratamiento no fuese únicamente automatizado y por tanto no sujeto a la protección del art. 22. Para ello, las directrices del GT29 han concluido que aquellas actuaciones humanas que carezcan de contenido real y simplemente se dediquen a aprobar decisiones algorítmicas sin una revisión real sigan siendo consideradas únicamente automatizadas. Asimismo, el GT29 propone ciertos criterios de control, como comprobar el número de veces que la persona decide desviarse de la decisión tomada por el sistema.[527]

Sin embargo, el cumplimiento de estos requisitos no es sencillo de verificar por parte de la autoridad de control,[528] e incluso tampoco de cumplir por parte del responsable. Por ejemplo, en ocasiones, la persona que debe revisar las conclusiones del sistema automatizado no conoce el funcionamiento del algoritmo ni los motivos que le llevaron a una decisión

[527] GRUPO DE TRABAJO DEL ARTÍCULO 29, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679* (WP 251 rev.01), de 6 de febrero. Adoptadas por el Comité Europeo de Protección de Datos, p. 23.

[528] No obstante, en ocasiones anteriores ya ha sido puesto de manifiesto cómo multitud de autoridades de control nacionales de los Estados miembros tienen asumidas potestades de control y sanción que apenas ejercitan en la práctica. Antonio Troncoso ha llegado a afirmar que, en ese contexto "no existe realmente una tutela efectiva del derecho fundamental a la protección de datos personales en el ámbito europeo". TRONCOSO REIGADA, Antonio (2010): "La protección de datos personales. Una reflexión crítica de la jurisprudencia constitucional", en *Cuadernos de Derecho Público*, No. 19-20.

concreta, pues la complejidad de los modelos algorítmicos hace esta tarea cada vez más difícil.

4.4.2. *Decisiones que producen efectos jurídicos o significativamente similares*

Existen ciertos escenarios en los que existe un claro efecto jurídico o un efecto similar. Por ejemplo, cuando una decisión algorítmica conlleva la concesión o denegación de un crédito. Otros supuestos, serán no significativos, como la utilización de un perfil para el envío de publicidad personalizada.[529]

Sin embargo, existen áreas grises de más difícil concreción. Así, por ejemplo, si en lugar de determinar la denegación de un crédito, la consecuencia del uso de un modelo totalmente automatizado es la concesión de dicho crédito con un determinado tipo de interés, que pudiera ser ligeramente superior al interés que se hubiera obtenido de otro modo, ¿es dicho efecto suficientemente significativo como para provocar la aplicación del artículo 22?

En esencia, el art. 22 presenta un mosaico de posibles interpretaciones, términos ambiguos y dificultades acrecentadas por la complejidad técnica de los sistemas algorítmicos. En este escenario, podría llegar a ser relativamente sencillo para un responsable argumentar que un tratamiento determinado no cumple con los requisitos ambiguos que introduce el art. 22 y así, quedar exento de preservar el conjunto de garantías que crea el art. 22 para proteger al interesado frente a situaciones especialmente complejas que le afectan.

[529] EDWARDS, Lilian; VEALE, Michael (2017): “Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking For”, en *Edwards, Duke Law & Technology Review*, No.16, Vol. 18.

4.5. Relación entre los derechos de acceso, información y la toma de decisiones automatizadas[530]

El art.22 no es la única disposición orientada a procesos de toma de decisiones automatizadas. Los artículos 13, 14 y 15 RGPD, que versan sobre el derecho de los sujetos a la información y acceso, establecen por primera vez que se informe del hecho de la existencia de mecanismos de decisión automatizada en el momento de la recogida de los datos, así como de las posibles consecuencias de dicho tratamiento.

De este modo, los derechos de información y de acceso son uno de los elementos de base esenciales para que el interesado obtenga conocimiento sobre el hecho mismo de que está siendo objeto de decisiones automatizadas, así como de las posibles implicaciones de estas. Este conocimiento será, por su parte, la base para que el interesado ejerza otras potestades del art. 22, como cuestionar una decisión automatizada cuyos efectos son significativos para su vida. Así, existe una relación bidireccional entre el art. 22 y los arts. 13, 14 y 15 RGPD.

En lo referente a estos últimos, la redacción en los tres artículos (arts. 13.2.f), 14.2.g) y 15.1.h) del RGPD) es idéntica y establece que debe facilitarse al interesado la información siguiente:

> "(…) la existencia de decisiones automatizadas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, *información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas* de dicho tratamiento para el interesado".

[530] Parte del contenido de esta sección ha sido objeto de publicación en GIL GONZÁLEZ, Elena (2017): "Aproximación al estudio de las decisiones automatizadas en el seno del Reglamento General Europeo de Protección de Datos a la luz de las tecnologías big data y de aprendizaje computacional", en *Revista española de la transparencia*, No. 5.

De nuevo, estos artículos adolecen de ambigüedades cuyo estudio merece la pena, en concreto, en torno a qué debe considerarse información "significativa".

4.5.1. *Información compleja*

Una primera dificultad que el responsable puede encontrar al ejecutar su obligación de informar deriva directamente de la complejidad de la tecnología cuya lógica y consecuencias debe exponer.

Como ya hemos señalado, el funcionamiento del sistema algorítmico puede ser difícil de comprender, y en consecuencia, la lógica subyacente puede ser complicada de explicar. Por su parte, los efectos futuros de la tecnología y sus consecuencias no siempre son claros. El responsable debe hacer un esfuerzo por detallar las consecuencias en la medida en que estas haya podido ser diligentemente previstas. Esta complejidad ha sido resaltada por parte de los mismos responsables, por ejemplo, por la tecnológica Intel.[531]

A ello hay que añadirle la creciente complejidad de informar tratamientos de datos que puedan potencialmente envolver a terceras partes. Pensemos, por ejemplo, en la gran opacidad que rodea el mercado de datos y el funcionamiento de la publicidad comportamental que funciona mediante subastas de espacios publicitarios en páginas webs de terceros en tiempo real. Mucha de la información disponible reviste de un carácter altamente técnico, que resulta complejo para el administrador de la página web sobre la que tiene lugar esta actividad de tratamiento de datos.

Así, se crea la paradoja de que, por un lado, los responsables alegan la dificultad de informar a los interesados con mayor nivel de detalle sobre actividades sobre las que no ejercen un alto nivel de control,[532] pero por

[531] HOFFMAN, David; MASUCCI, Riccardo (2018): "Intel's AI Privacy Policy White Paper. Protecting individuals' privacy and data in the artificial intelligence world", en *Intel Corporation*.

[532] En este sentido, el paradigmático que las últimas resoluciones del TJUE amplían el concepto de responsable del tratamiento. Por ejemplo, en la reciente sentencia en el Asunto C-40/17, Fashion ID, el TJUE argumenta que los administradores de sitios web ejercen corresponsabilidad por actividades sobre las que en realidad no ejercen control, en concreto, qué datos se recogen y transmiten a una red social cuando la página web de dicho administrador incluye botones de la red social. La ubicación de responsabilidad se

otro, se coloca al interesado en la posición de corroborar haber recibido la información suficiente y significativa.

Algunas de estas conclusiones ya han sido expuestas cuando hablamos de las limitaciones de la prestación del consentimiento en entornos de tratamientos de datos masivos. Estas situaciones son incluso más ciertas cuando se refieren al momento concreto de la Fase 3-Aplicación, por cuanto se trata del momento en el que actividades hasta ahora restringidas al entorno digital despliegan efectos en la realidad material de las personas.

Del mismo modo que señalábamos entonces, para el interesado medio razonable una explicación técnica y detallada de la lógica o funcionamiento del algoritmo perdería sentido, ya que sería incomprensible. Por este motivo, se vuelve, de nuevo, imprescindible, encontrar medios en los que las obligaciones de transparencia consigan el objetivo de facilitar el control y el ejercicio de garantías y derechos de los interesados.

De hecho, con base en el art. 12 RGPD, el responsable tiene obligación de tomar las medidas oportunas para que el interesado reciba y comprenda toda la información relevante para el ejercicio de sus derechos y, en concreto, en informarle de manera inteligible (art. 12.1) y de facilitarle el ejercicio de dichos derechos (art. 12.2). En este sentido, está claro que la escasez de información no cumpliría con la obligación de aportar información significativa al interesado. Por otro lado, el diseño de notificaciones largas diseñadas con el objetivo de esconder información relevante entre una avalancha de información inocua o inútil, práctica bautizada como opacidad estratégica,[533] no sería válida para cumplir el requisito de que la información relativa a la existencia, funcionamiento y consecuencias de decisiones automatizadas sea “significativa”.

realiza sobre la aseveración de que la decisión de incluir un botón social constituye una influencia clara que desencadena el tratamiento de datos.

[533] KAMINSKI, Margot E. (2019): “The right to explanation, explained”, U of Colorado Law Legal Studies Research Paper No. 18-24, en *Berkeley Techology Law Journal*, Vol. 34, No. 1, p. 214.

4.5.2. *Elemento temporal*

Además de lo ya expuesto, como fue adelantado, en lo que se refiere a la información relativa a decisiones automatizadas que el interesado tiene derecho a recibir, la redacción del art. 15 replica en gran parte aquella de los arts. 13 y 14. Esto abre la cuestión de determinar si esta redacción idéntica o casi idéntica debe interpretarse de modo que la obligación del responsable sea también idéntica.

Es necesario detenernos a matizar las diferencias del deber de información en función del espacio temporal en el que este deber puede ser atendido. En primer lugar, podríamos hablar de información proporcionada *ex ante*, de forma previa a cualquier tipo de acción, es decir, el lapso de tiempo anterior a la creación de un modelo algorítmico y, por tanto, anterior también a la toma de cualquier decisión automatizada sobre una persona concreta. En segundo lugar, podríamos hablar de información *ex post*, que se refiere a aquella proporcionada tras la modelación del algoritmo, la ingesta de los datos de una persona específica y la toma de una decisión automatizada sobre dicha persona.

Recordemos que la información de los arts. 13 y 14 debe aportarse en el momento de la recogida de los datos o, en su caso, antes del tratamiento de los datos para un fin diferente al que motivó la recogida. Esto podría hacer pensar que es innecesario un derecho de acceso del art. 15, puesto que no es más que una nueva oportunidad del interesado de solicitar información que debería tener disponible en virtud de otros artículos del Reglamento.

Ciertamente, en ocasiones, el tipo de información a remitir en cumplimiento de los arts. 13-14, por un lado, y del art. 15, por otro lado, será igual o similar. Pensemos, por ejemplo, en informar sobre el derecho a presentar una reclamación ante la autoridad de control.

Sin embargo, en otras ocasiones la información no debería ser la misma. Por ejemplo, la categoría o el tipo específico de datos personales objeto del tratamiento puede evolucionar cuando se realizan inferencias de datos

acerca del sujeto o perfiles. En dichos casos, la información de la que dispone el responsable antes del inicio del tratamiento, recogida en su política de privacidad o cualquier otro medio, será más limitada que la información de la que disponga una vez el tratamiento ha comenzado. De este modo, el cumplimiento de las obligaciones de información y transparencia, así como el derecho de acceso deben adaptarse a la realidad del dinamismo del flujo de datos.

Es decir, el mero hecho de informar *ex ante*, conforme a los arts. 13 y 14, excluye la posibilidad de informar, siquiera en términos genéricos, por ejemplo, sobre aquellos datos nuevos obtenidos por el responsable mediante inferencia estadística, fruto de insertar el conjunto de información de una persona determinada en los parámetros de un algoritmo prediseñado para observar posibles correlaciones y extraer nuevos conocimientos sobre el individuo.

Si el responsable posee ese nivel de información en un momento posterior, la obligación de que en dicho momento posterior aporte "información significativa" le obliga a ampliar aquella que aportó *ex ante*.

De este modo, el derecho de acceso del art. 15 se configura, en palabras de Aparicio como una cautela para la "prevención de la acumulación de datos y las desviaciones de finalidad, puesto que (…) el principal riesgo que existe en el tratamiento de datos de carácter personal es la acumulación de información que puede arrojar, como precipitado, un retrato de la personalidad del individuo, el perfil personal". Estas palabras adquieren aún más relevancia en la sociedad de la información y, concretamente, en entornos big data, donde la toma de decisiones automatizadas y las prácticas de creación de perfiles se multiplican. Por ello, el derecho de acceso tiene como finalidad que el sujeto conozca la información referente a él que está siendo objeto de tratamiento, así como las circunstancias que lo rodean.

Así, el derecho de acceso se configura como la oportunidad de ser informado de manera significativa, a petición del interesado, sobre lo

relativo al tratamiento de datos personales en cualquier instante posterior a la recogida de los datos, que puede ser previo o posterior a la toma de decisiones, automatizadas o no, sobre el sujeto. Recordemos, además, que una de las funciones principales del derecho de acceso es servir de valor instrumental para que el interesado pueda ejercitar otros derechos y garantías. Pues bien, únicamente cuando el responsable amplía la información que le fue dada al interesado en un momento anterior, conforme a las nuevas circunstancias, puede cumplirse esta función.

En conclusión, parece que el ejercicio de un derecho de acceso es la oportunidad perfecta para imponer al responsable del tratamiento la obligación de aportar información con el máximo nivel de transparencia, incluyendo de este modo conocimientos no disponibles en momentos anteriores, tales como aquellos datos obtenidos por medio de inferencia estadística que serán parte de los modelos algorítmicos y podrán influenciar el sentido de una decisión automatizada que cause efectos significativos al sujeto.

Esto supondría, en la práctica, interpretar en un sentido más amplio el texto del art. 15.1.h) (derecho de acceso) que aquél de los arts. 13.2.f), 14.2.g) (información), a pesar de tener todos ellos una redacción idéntica, todo ello en atención al momento en el que se aplica cada disposición.

Esta opinión es compatible con la visión que parece desprender el RGPD sobre el tratamiento de datos personales. En efecto, el RGPD visualiza el tratamiento como un proceso dinámico que se mantiene vivo en el tiempo. Por este mismo motivo, por ejemplo, el registro de actividades del tratamiento o las evaluaciones de impacto son documentos que deben ser actualizados cuando las circunstancias así lo requieran. Del mismo modo que la documentación interna del responsable, la información que este proyecte al exterior no puede verse como un texto estático en el tiempo.

A pesar de estos argumentos, el GT29, ahora CEPD, ha manifestado, en sus directrices sobre decisiones individuales automatizadas y elaboración de perfiles que el art. 15 otorga un derecho a los interesados a recibir la

misma información sobre decisiones individuales automatizadas idéntico a aquél de los artículos 13.2.f), 14.2.g) y que, de hecho, cuando un individuo ejerce su derecho de acceso, ya debería haber recibido del responsable esta información en aplicación de los arts. 13 y 14.[534]

4.5.3. *Elemento subjetivo*

Además de lo anterior, existe otro motivo por el que la información que se requiere al ejercitar un derecho de acceso (art. 15 RGPD) difiere básicamente de aquella que fue aportada en un momento anterior en cumplimiento de las obligaciones de información del responsable (arts. 13 y 14).

El sujeto al que la información va orientado es diferente en función de cuándo deba prestarse dicha información y del objetivo principal al que sirva. No diferenciar este aspecto es un error que llevará a consecuencias indeseadas para los interesados.

Por naturaleza, la información que debe ser prestada *ex ante*, se refiere al tratamiento en términos genéricos y sirve a dos objetivos principales: al valor intrínseco de adquirir conocimiento y control sobre los aspectos que rodean al tratamiento, y al valor instrumental de permitir al interesado accionar otras garantías. Por este motivo, la información prestada conforme a los arts. 13 y 14 RGPD está dirigida al interesado medio razonable que ostenta el derecho de información de manera pasiva.

Por su parte, aquella información proporcionada en un momento posterior, especialmente cuando se debe al ejercicio proactivo de un derecho de acceso por parte del interesado, acentúa el valor instrumental de la información. Ello es así porque el interesado generalmente ejerce sus derechos con el objetivo de conocer más detalles sobre su situación particular con miras a verificar si se está produciendo algún incumplimiento. Por este motivo, la información prestada con motivo del ejercicio activo de

[534] GRUPO DE TRABAJO DEL ARTÍCULO 29, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679* (WP 251 rev.01), de 6 de febrero. Adoptadas por el Comité Europeo de Protección de Datos, p.29-30.

un derecho de acceso del art. 15 RGPD tiene como destinatario principal al interesado específico que decide ejercitar su derecho. De hecho, solo de este modo, a partir de información personalizada y una copia de los datos personales objeto de tratamiento, es como el interesado puede alcanzar el grado de control que pretende garantizar el derecho de acceso, así como servir de base para el posible ejercicio de otros derechos o el inicio de acciones.

4.5.4. *Información significativa*

Cabe preguntarse, por tanto, qué debe entenderse por información significativa sobre la lógica aplicada. El RGPD no cuenta con parámetros que ayuden a evaluar o interpretar la significatividad, sino que es un concepto que queda abierto.

Asimismo, ha quedado argumentado que el término "significativo" debe adaptarse a las circunstancias del caso concreto y partir de la base de que el tratamiento de datos es un flujo vivo y dinámico.

Por este motivo, y atendiendo a todas las reflexiones anteriores, podemos esquematizar qué debe entenderse por información significativa en función de qué obligación o derecho esté siendo objeto de cumplimiento. Para ello, los tres parámetros principales a los que debe atenderse son el "cuándo", el "para qué" y el "para quién" de la información.

	ARTS. 13-14	**ART. 15**
CUÁNDO	*Ex ante*	En cualquier momento, incluido *ex post*
PARA QUÉ	Obtención de control y Valor instrumental	Valor instrumental **>** Obtención de control
PARA QUIÉN	Interesado medio razonable	Interesado específico, que ejerce su derecho

Gráfico 5: Requisitos para considerar que existe información "significativa" en el sentido de los art.s 13, 14 y 15 RGPD.

Fuente: Elaboración propia.

Así, según estos parámetros, conforme a los arts. 13 y 14, el responsable cumplirá su obligación de aportar información significativa sobre la lógica aplicada y las consecuencias previstas de la toma de decisiones automatizadas cuando esta sirva a la generalidad de interesados medios razonables para conocer sobre el tratamiento y así obtener un grado sustancial de control que, en un momento posterior, pueda servirles para accionar determinadas garantías. Un ejemplo de cómo esto podría trasladarse en la práctica ha sido ya recogida por De la Quadra-Salcedo, que propone que todo algoritmo destinado a la elaboración de perfiles incluya una memoria previa que contenga información sobre la finalidad y objetivos que persigue el algoritmo de creación de perfiles, así como la enumeración de las variables más significativas en el proceso de toma de decisiones, todo ello sin desatender la protección de los secretos empresariales.[535]

Por su parte, bajo el art. 15, información significativa debe ser vista como aquella que permite acceder a una comprensión por parte del interesado individual sobre aspectos que han influido en la decisión concreta de la que ha sido objeto. Esta información debe ser suficiente para que el interesado pueda accionar, por ejemplo, las garantías del art. 22.3 de expresar su punto de vista sobre la decisión o impugnarla, así como ejercer un derecho de rectificación o iniciar acciones legales, por ejemplo, por discriminación.

4.5.5. *Cuestiones abiertas*

Las aristas del art. 22 son múltiples. En este capítulo hemos abordado solo algunas de ellas, desde la naturaleza propia del "derecho" a no ser objeto

[535] DE LA QUADRA-SALCEDO FERNÁNDEZ DEL CASTILLO, Tomás (2018): "Retos, riesgos y oportunidades de la sociedad digital", en Tomás de la Quadra-Salcedo y José Luis Piñar (dirs.), Sociedad digital y Derecho, Madrid, BOE-Red.es, p. 54. De hecho, De la Quadra-Salcedo también parece referirse de forma implícita a las fases aquí descritas cuando menciona que as decisiones automatizadas del tipo que aquí nos ocupan pueden estar basadas no solo en datos personales del proprio interesado, sino en perfiles elaborados a partir de datos de millones de sujetos ajenos al interesado.

de decisiones automatizadas hasta cómo debe concretarse la debida transparencia en materia de decisiones automatizadas y cómo estos factores se relacionan con otros derechos del RGPD tales como el de oposición, acceso o información. No obstante, existen otros muchos temas que quedan fuera del ámbito de este trabajo pero que no deben ser desatendidos.

Se trata de cuestiones controvertidas, cuya discusión se mantiene abierta y que son objeto de profundos debates y que aquí serán únicamente mencionadas.

Así, la aplicabilidad práctica de las garantías del art. 22 plantea inconvenientes. Pensemos, por ejemplo, en el derecho del interesado, conforme el art. 22.3 a solicitar la obtención de revisión humana de una decisión previamente tomada a través de medios únicamente automatizados cuando esta se hubiese basado en el consentimiento del interesado o en la necesidad para la ejecución de un contrato con este.

Para hacer efectiva esta garantía, es necesario que dentro de la organización del responsable al menos una persona tenga capacidad para comprender el funcionamiento del sistema algorítmico y pueda emplear su criterio para modificar una decisión de este.[536] Sin embargo, esta labor se hace cada día más compleja a medida que los medios técnicos, el tipo de datos y su volumen incrementan. De hecho, muchos sistemas llegan a describirse como cajas negras o espejo de un solo sentido.[537]

[536] HILDEBRANDT, Mireille (2016): "The new Imbroglio: living with machine learning algorithms", en Janssens, L. (ed), *The Art of Ethics in the Information Society, Mind you*, Ámsterdam: Amsterdam University Press.

[537] MOEREL, Lokke; PRINS, Corien (2016): "Privacy for the homo digitalis: Proposal for a new regulatory framework for data protection in the light of Big Data and the internet of things", en SSRN Electronic Journal, 2784123; KUNER, Christopher; SVANTESSON, Dan Jerker B.; CATE, Fred H.; LYNSKEY, Orla; MILLARD, Christopher (2017): "Machine learning with personal data: is data protection law smart enough to meet the challenge?", en *International Data Privacy Law*, Vol 7, No. 1; PASQUALE, Frank (2015): *The black box society: The secret algorithms that control money and information*, Cambridge, Londres: Harvard University Press; DIAKOPOULOS, Nicholas (2014): "Algorithmic-Accountability Reporting: on the investigation of Black Boxes", en *Tow Center for Digital Journalism*.

Por su parte, existe un debate ferviente en torno a la existencia o no de un derecho a recibir una explicación *ex post* acerca de una decisión automatizada concreta. El origen de tan intenso debate es el hecho de que esta garantía aparece mencionada en el considerando 71, pero no fue trasladada al art. 22 -ni a ningún otro, al menos de modo expreso-. Mientras parte de la doctrina ha defendido la no existencia de este derecho,[538] otros critican esta postura y argumentan que su existencia se extrae de la interpretación del derecho a obtener información significativa sobre la lógica algorítmica conforme a los arts. 13-15.[539]

En esencia, el art. 22 RGPD abre innumerables escenarios diferentes y está siendo objeto de profundo estudio sin conclusiones claras, aunque siempre sobre la base de una necesaria responsabilidad y control algorítmicos.[540]

4.6. Relación entre el derecho de portabilidad y la toma de decisiones automatizadas

Como vimos al inicio del capítulo, el art. 20 RGPD requiere que para ejercer un derecho de portabilidad el tratamiento se haya efectuado por medios "automatizados".

El RGPD únicamente recoge dos casos en los que confluyan al mismo tiempo los requisitos de la necesidad de que el tratamiento sea automatizado y que la base de legitimación sea el consentimiento o la ejecución de un contrato. Uno, ya mencionado, es el art. 20 sobre

[538] WACHTER, Sandra; MITTELSTADT, Brent; FLORIDI, Luciano (2016): "Why a right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation", en *International Data Privacy*, Vol 7, No. 2.

[539] SELBST, Andrew D.; Powles, Julia (2017): "Meaningful Information and the Right to Explanation", en *International Data Privacy Law*, Vol. 7, No. 4.

[540] Para una visión práctica sobre las dificultades de los interesados de ejercer las garantías derivadas del art. 22 y el derecho a recibir una explicación sobre una decisión individual automatizada, ver el interesante trabajo de MITJANS SERVETO, Maria (2019): "Exercising GDPR data subjects' rights Empirical research on the right to explanation of news recommender systems", Master´s thesis, Universidad Católica de Lovaina.

portabilidad de datos. El segundo es el art. 22, sobre el derecho a no ser objeto de decisión basada únicamente en el tratamiento automatizado.

4.6.1. *Similar, pero diferente*

La fórmula utilizada por el art. 20 es en parte coincidente pero no idéntica a aquella utilizada en el art. 22,[541] por cuanto esta última requiere que el tratamiento sea "únicamente" automatizado, esto es, sin intervención humana.

En concreto, aquellas disposiciones relativas a la toma de decisiones únicamente automatizadas, incluyendo la elaboración de perfiles sobre intereses, fiabilidad o comportamiento exigen que la base del tratamiento únicamente pueda ser el consentimiento o la ejecución de un contrato. Esto es, si el art. 22 RGPD se interpreta como una prohibición[542] de llevar a cabo tratamientos únicamente automatizados salvo que se cumplan las excepciones que menciona, puede concluirse que el RGPD no obliga a aplicar esta disposición cuando el tratamiento se basare en el interés legítimo del responsable.

Analizaremos algunos aspectos del art. 22 más adelante en este capítulo, pero por el momento ya podemos analizar, a través de ejemplos, algunas situaciones que pueden darse en relación con la concurrencia del derecho de portabilidad y de no ser objeto de decisiones automatizadas.

[541] Véase también el considerando 71.

[542] Esta conclusión es cierta si el art. 22 se interpreta como una prohibición y no como un derecho.

	Caso 1	Caso 2	Caso 3	Caso 4	Caso 5
Datos facilitados por el interesado	no	sí	sí	sí	sí
Tratamiento “únicamente automatizado”	sí	no	no	sí	no
Tratamiento no únicamente automatizado	sí	sí	sí	sí	no
Consentimiento o ejecución contractual	sí	no	sí	sí	sí
Portabilidad	NO	NO	SÍ	SÍ	NO
No ser objeto de decisiones automatizadas	SÍ	NO	NO	SÍ	NO

Gráfico 6: Concurrencia de derechos de portabilidad y a no ser objeto de decisiones automatizadas.

Fuente: Elaboración propia.

Caso 1. Una empresa de comercio minorista utiliza el historial de compras de los usuarios, así como datos de fuentes externas para elaborar un perfil de cada cliente a través de medios totalmente automatizados, basándose en el consentimiento de estos. Es decir, estamos ante un tratamiento regido por el art. 22 RGPD, pues es se ha realizado un perfilado por medios únicamente automatizados siendo las bases permitidas el consentimiento o la necesidad de ejecutar un contrato. Por su parte, los datos resultantes no son aquellos aportados por el interesado o directamente observados. En conclusión, se cumplen dos de los tres requisitos para ejercer el derecho de portabilidad y, por tanto, el usuario no puede portar los datos relativos a su perfil. Por su parte, el interesado sí ostenta aquellos derechos derivados

del art. 22 RGPD tales como oponerse a dicha decisión, obtener intervención humana, recibir información sobre la lógica aplicada.

Caso 2. Con motivo de la celebración del día del libro, una librería utiliza el historial de compras del último año de sus clientes para elaborar de manera automatizada un perfil de cada uno de ellos. El perfil es después es revisado por el responsable y se utiliza para decidir sobre qué tipo de productos se emitirá una promoción personalizada. Para ello, la librería se basa en su interés legítimo. En este caso, se cumplen dos de las condiciones del derecho de portabilidad (datos aportados por el interesado y tratamiento automatizado). Sin embargo, no se cumple la condición de que la base del tratamiento sea el consentimiento o la ejecución contractual. Por tanto, el interesado no tiene derecho a ejercer la portabilidad de sus datos.

Adicionalmente, el individuo no tendrá derecho a oponerse a las decisiones que se deriven de este tratamiento o a obtener información sobre la lógica aplicada, pues el tratamiento no es “únicamente” automatizado y por tanto no entra en el ámbito de aplicación del art. 22 RGPD.

Caso 3. Una entidad de seguros de responsabilidad civil elabora un perfil de potenciales clientes de manera automatizada, aunque sometido a revisión humana posterior, a partir de los datos que estos aportan a través de un formulario como paso previo necesario para la ejecución contractual. En este caso, se cumplen los tres requisitos exigidos para el ejercicio del derecho de portabilidad y el interesado podrá migrar esta información a otro proveedor.

Sin embargo, el individuo no tendrá derecho a oponerse a las decisiones que se deriven de este tratamiento conforme al art. 22, pues el tratamiento no es “únicamente” automatizado.

Caso 4. Una entidad bancaria pone en marcha un servicio que permite a los usuarios solicitar créditos por internet. El usuario introduce ciertos datos solicitados por el sistema que son analizados de manera automática para responderle inmediatamente si se le concede un préstamo y, en su caso,

el tipo de interés. Se trata de un caso de toma de decisiones únicamente automatizadas que despliega un efecto jurídico sobre el interesado, realizado únicamente a partir de datos directamente obtenidos del individuo con su consentimiento o por necesidad para ejecutar una relación contractual con este. En este caso, el individuo sí podrá ejercer su derecho de portabilidad, así como su derecho a no ser objeto de este tratamiento y solicitar, entre otras, intervención humana o el resto de garantías del art. 22 RGPD.

Caso 5. De manera similar al caso anterior, una entidad bancaria pone a disposición de sus clientes un servicio rápido de concesión de microcréditos. Tras introducir los datos, el usuario obtiene una previsión preliminar que le será confirmada en un plazo de 48 horas por un empleado de la entidad. El empleado recibe del sistema una recomendación que valora antes de trasladar la decisión final al interesado. En este caso, estamos ante un tratamiento de datos en la que la toma de decisiones implica medios automatizados, pero con intervención humana. bajo consentimiento o necesidad para la ejecución contractual. En este caso, el individuo sí podrá ejercer su derecho de portabilidad, pero no su derecho a no ser objeto de este tipo de tratamiento conforme al art. 22. Así por ejemplo, el interesado puede recibir una negativa a la concesión de un crédito sin disponer de un derecho a expresar su punto de vista y aportar información que considere relevante que no hubiese tenido posibilidad de aportar durante el proceso automatizado.

Como se aprecia de los casos anteriores, en la gran mayoría de los casos el interesado verá sus intereses disminuidos, pues no tendrá derecho a ejercer todos los derechos que el RGPD prevé. La necesidad de concurrencia de diversos requisitos, a pesar de que no se aprecie un motivo claro que lo justifique, juega un papel claramente contrario a los intereses de los usuarios de servicios automatizados, cada día más comunes para finalidades más diversas y de mayor impacto.

5. Conclusiones

En estas páginas hemos analizado algunas de las implicaciones de los derechos de portabilidad (art. 20), acceso (art. 15), el derecho a no ser objeto de decisiones automatizadas (art. 22) y los derechos de información (art. 13-14), así como la relación entre estos derechos. Todo ello en el contexto específico de tratamientos de datos personales basados en la utilización de tecnologías de datos masivos.

Algunos derechos, como el de portabilidad, son nuevos en el cuerpo normativo de la protección de datos personales. Otros derechos, como el de no ser objeto de decisiones automatizadas, apenas se encuentran desarrollados a nivel práctico. Por último, otros derechos como el de acceso, no es nuevo ni falto de desarrollo práctico *per se*, pero sí en relación con ciertos aspectos que el desarrollo tecnológico plantea de manera más novedosa.

Como hemos podido observar, las nuevas realidades tecnológicas suponen en ocasiones un reto para el correcto ejercicio de estos derechos. Pensemos, por ejemplo, en la falta de interoperabilidad de sistemas, hecho que obstaculiza la portabilidad de datos, o la dificultad de los responsables de proporcionar información completa pero comprensible sobre decisiones automatizadas.

Por otro lado, otros derechos podrían llegar a quedar limitados en función de la interpretación que se haga de ellos. Ejemplo de ello es cómo se efectuará la limitación del derecho de acceso cuando el responsable trate una gran cantidad de información, o cómo debe el responsable hacer frente a su obligación de proporcionar información significativa sobre la lógica de tratamientos únicamente automatizados. Esto es especialmente relevante respecto de la toma de decisiones automatizadas. La literalidad de los arts. 13-15 y 22 respecto de este tipo de tratamientos parece dar mucha importancia a la transparencia y a la protección de los sujetos en relación con la toma de decisiones automatizadas. Sin embargo, la gran cantidad de conceptos indeterminados permite encajar interpretaciones con diversos

grados de flexibilidad o restricción que en última instancia determinarán la amplitud de los derechos de los interesados y su capacidad para conocer la existencia de decisiones automatizadas, el funcionamiento de los sistemas que las toman y las garantías que pueden ejercitar para solicitar una revisión o la oposición a este tipo de decisiones.

En otras ocasiones, sin embargo, parece que las limitaciones de estos derechos responden más a acuerdos durante la fase de creación del RGPD que a una razón jurídica sólida. Por ejemplo, el legislador ha circunscrito el ejercicio de diversos derechos únicamente a los datos y tratamientos sometidos a la voluntad del interesado, bajo la premisa de que dichos derechos protegen la capacidad de control del interesado respecto de aquellos tratamientos basados previamente en dicha capacidad de control. Ejemplo de ello es el ejercicio del derecho de portabilidad o de oposición a la toma de decisiones automatizadas, que únicamente cabe ejercer cuando la base de legitimación del tratamiento fue el consentimiento y o la necesidad para la ejecución de un contrato. Esto es cierto a pesar de que, como ha sido ampliamente argumentado a lo largo de este trabajo, el ejercicio pleno de dicha voluntad del individuo es reducido en entornos de alta complejidad técnica, impredecibilidad y tratamientos intensivos. Ello es así dado que la comprensión del tratamiento resulta difícil para el interesado medio, debido no solo a la inherente complejidad técnica, sino también a las limitaciones derivadas de derechos tales como la información sobre la toma de decisiones automatizadas, la dificultad para acceder a una explicación sobre la lógica aplicada, el acceso a los datos, etc.

Todo ello puede ocasionar claros perjuicios para los derechos de los interesados y su capacidad para actuar frente a posibles abusos del responsable o para, simplemente, acceder a información transparente acerca del tratamiento. Y no solo eso. Es, de hecho, el análisis de la interrelación de todos los derechos lo que puede arrojar conclusiones más preocupantes para las garantías del interesado. Pensemos por ejemplo en el uso de medios automatizados para buscar correlaciones entre datos y obtener nuevo conocimiento del interesado a través de procesos de

inferencia de datos. En función de cómo interprete el responsable el RGPD, este puede llegar a la conclusión preliminar de que no se está realizando un tratamiento que afecte de manera significativa al interesado, y por tanto, fuera del ámbito de aplicación del art. 22. En dicho caso, el responsable determinará que no se encuentra obligado a informar del uso de medios automatizados, ni por tanto a aportar información sobre la lógica algorítmica ni las consecuencias del tratamiento. De este modo, el interesado no es consciente de la intrusividad del tratamiento. Ello debilita su posición para especificar sobre qué tipo de datos desea ejercer un derecho de acceso, y posiblemente, no solicite el derecho respecto de aquellos aspectos que le resulten más invasivos. Por su parte, tampoco cuenta con un derecho para obtener una copia de dichos datos a través de un derecho de portabilidad. En consecuencia, se da una cadena de incongruencias, lagunas y ambigüedades que terminan por crear graves deficiencias en el sistema de derechos de los interesados.

Algo similar puede ocurrir, por ejemplo, cuando el responsable argumenta que no lleva a cabo tratamientos únicamente automatizados, de modo que no informa de la existencia de tratamientos del art. 22 y, asimismo, basa el tratamiento en su interés legítimo. Incluso cuando la ponderación de intereses se efectuase de manera correcta, el interesado termina de nuevo es una posición de desinformación en relación con los datos que sobre él han sido inferidos.

Todo ello se produce, además, en un momento en el que cada vez más servicios utilizan técnicas algorítmicas que permiten llevar a cabo actividades de inferencia de datos, perfilado y tratamientos con un mayor nivel de complejidad e intrusividad. Estos son, a su vez, utilizados para tomar decisiones sobre el interesado en ámbitos tales como el contenido que se le muestra en internet, los productos que se le recomiendan, las predicciones sobre su fiabilidad crediticia, riesgo de enfermedad, etc. Es decir, un interesado medio está de manera cotidiana rodeado de decisiones basadas en información probabilística sobre él de la que no es consciente,

de la que no siempre tiene derecho a pedir información o está en posición de hacerlo.

Todos estos factores pueden crear un "efecto Gruyere" en el sentido de constituir vacíos en la norma y provocar que multitud de situaciones de consecuencias relevantes queden fuera del alcance de conocimiento y control del interesado.

En otras palabras, se crea un ecosistema esencialmente asimétrico que perpetúa su posición de inferioridad de conocimiento. Así, lo que parecía un gran avance del RGPD en términos de nuevos y más reforzados derechos puede llegar a quedar enormemente diluido hasta el punto de fortalecer la posición del responsable, que opera bajo una falsa apariencia de transparencia y cumplimiento que puede esconder grandes vacíos. Ello es especialmente cierto respecto de aquellos datos secundarios o inferidos del usuario durante la Fase 3-Aplicación.

Sin embargo, otras normas sí reconocen ampliamente el valor de dichos datos secundarios, así como la necesidad de mantener un flujo de datos para obtener beneficios de la explotación de dichos datos. Ejemplo de ello es el Reglamento Business-to-Platform (B2P).[543]

El Reglamento B2P[544] pretende regular la relación entre plataformas digitales que actúan de intermediarias en las transacciones entre empresas usuarias de dichas plataformas y los consumidores finales. La razón de ello es vista en el hecho de que la capacidad de acceder y utilizar datos, incluidos datos personales, contribuye a la creación de valor en la economía de las plataformas digitales. De este modo, el Reglamento B2P permite, sujeto a parámetros de transparencia y licitud, que la plataforma y

[543] COMISIÓN EUROPEA (2018): *Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre el fomento de la equidad y la transparencia para las empresas que utilizan servicios de intermediación en línea* COM(2018) 238 final, de 24 de abril.

[544] El 22 de marzo de 2019 la Comisión, el Parlamento y el Consejo anunciaron el acuerdo sobre un nuevo Reglamento que regule la relación entre plataformas digitales que actúan de intermediarias en las transacciones entre empresas usuarias de dichas plataformas y los consumidores finales. COMISIÓN EUROPEA (2019): *Press release, Digital Single Market: EU negotiators agree to set up new European rules to improve fairness of online platforms' trading practices*, de 14 de febrero.

las empresas usuarias accedan a datos personales del consumidor final. Más concretamente, la plataforma tiene obligación de informar qué datos de las empresas usuarias y consumidores finales se recaban, así como informar a las empresas si tienen capacidad de acceder a dichos datos. Así, en función de cómo se desarrollen estas disposiciones en la práctica, parece que existe una tensión entre la buena acogida que parece darse a la reutilización de la información por parte de plataformas y empresas bajo el Reglamento B2P con las limitaciones concedidas a los usuarios para portar sus datos y de este modo reutilizarlos bajo el RGPD.

Asimismo, esta postura abierta con la reutilización de datos, incluidos datos personales, para la creación de valor en el contexto de la economía digital choca, de hecho, con la visión de la reutilización de datos mostrada en las normas sobre privacidad y protección de datos personales, y más concretamente, la propuesta de Reglamento e-Privacy y el RGPD.[545] De hecho, el legislador se encuentra ante la tensión de, por un lado, proteger el interés de disminuir dependencias de las empresas sobre las plataformas intermediarias y su efecto negativo sobre la competencia, y por otro lado, proteger la privacidad y los datos personales de los ciudadanos. Esto crea la situación en la que el legislador debe hacer frente la ponderación de intereses de las empresas basadas en datos y los derechos de los usuarios.[546]

Por todo ello, únicamente el tiempo podrá solventar ciertas limitaciones aquí expresadas y ayudar a darle un contenido práctico y un desarrollo efectivo a los derechos de los usuarios. Entre tanto, el ejercicio de los derechos del interesado no es sencillo para este. Tampoco es sencillo para este detectar cuándo sus derechos están siendo infringidos y así acudir a las autoridades de control. Por todo ello, la labor de los delegados de protección de datos cobra su sentido máximo, como garantes de los

[545] FATHAIGH Ronan Ó.; VAN HOBOKEN, Joris (2019): "European Regulation of Smartphone Ecosystems", en Data Protection Law Review, Vol. 5, No. 4, p. 14.

[546] FATHAIGH Ronan Ó.; VAN HOBOKEN, Joris (2019): "European Regulation of Smartphone Ecosystems", en Data Protection Law Review, Vol. 5, No. 4, p. 15.

derechos de los individuos en el seno de las organizaciones. También por este mismo motivo, se torna quizás más importante que nunca antes la capacidad de las autoridades de control de iniciar investigaciones de oficio, de implementar de manera efectiva mecanismos de cooperación y coordinación interestatales e incluso de guiar y orientar a los responsables de manera preventiva antes del inicio del tratamiento.

Para ello, el principal instrumento con que cuentan las autoridades de control es la potestad sancionadora. Una potestad que ha sido ampliamente reforzada por el RGPD gracias al sustancial incremento de los límites superiores pecuniarios que se le puede imponer a un responsable por incumplimiento del reglamento.

CAPÍTULO VII. PROPUESTAS

> "Es la naturaleza humana comenzar intercambios con el objetivo de obtener más de lo que está dispuesto a ofrecer a cambio. En ese sentido, la desigualdad es un hecho de la vida. Sin embargo, llega un punto en el que los desequilibrios de poder se vuelven tanto injustificables como insostenibles. (...) Los períodos de rápidos cambios tecnológicos tienden a aumentar estos desequilibrios. La disparidad crece constantemente entre aquellos que tienen el control de la tecnología y aquellos que son objeto del despliegue de esa tecnología". [547]

En los capítulos anteriores hemos analizado la evolución histórica de las tecnologías de tratamiento de datos y de la legislación de protección de datos personales, la figura del consentimiento y sus limitaciones, la figura del interés legítimo con sus luces y sombras, y cómo la base de licitud impacta en aquellos derechos más relevantes para que el interesado mantenga su capacidad de control sobre los datos personales.

En concreto, hemos concluido que el consentimiento tiene fuertes impedimentos para desplegar garantías en entornos digitales, imprevisibles y de difícil comprensión, y que el interés legítimo puede solventar algunas de estos límites.

Con estas premisas, en este capítulo cerramos el círculo aplicando todo el análisis anterior sobre las bases de licitud a las Fases en las que hemos definido los proyectos que aplican tecnologías de datos masivos. También extraeremos algunas ideas que trascienden el debate de la elección de la base de licitud, pero directamente ligadas con ello.

[547] BUTTARELLI, Giovanni (2019): "Deception by design?" en *ISMS Forum Spain: XXI International Information Security Conference*, Madrid, de 30 de mayo.

1. Conformando el puzzle

Como ha sido ya desarrollado en capítulos anteriores, un tratamiento de datos no es un proceso único, sino que puede estar compuesto de diferentes operaciones, que se desarrollan en fases. En concreto, la sistematización de los tratamientos big data que hemos descrito en este trabajo, se puede reflejar en tres fases: 1- Recolección de datos, Fase 2- Análisis y Fase 3-Aplicación.

Con lo expuesto hasta el momento obtenemos una visión panorámica del contexto en el que nos encontramos. ¿Cómo encajan estas piezas? ¿Existe la posibilidad de crear un escenario más equilibrado que reduzca los riesgos para los derechos de los interesados y mantenga la capacidad de actuación leal de los responsables?

1.1. Fase 1 del big data, recolección de datos

Recordemos, esta fase consiste en la recogida de datos personales durante la actividad cotidiana de las organizaciones, responsable o encargados del tratamiento. De este modo, la base jurídica que permitiría la recogida y almacenamiento de los datos primarios dependerá del caso concreto.

En determinadas circunstancias, el tipo de tratamiento o el tipo de datos recolectados implicará acudir a una base de licitud determinada, en cumplimiento de las normas vigentes. Así, por ejemplo, para la obtención de datos provenientes de cookies y otros rastreadores, el consentimiento del interesado puede cobrar especial relevancia. Esta aproximación es, además, conforme con los requisitos de la Directiva e-Privacy (así como del futuro Reglamento e-Privacy). De hecho, en la medida en que un responsable obtenga consentimiento requerido por la normativa de comunicaciones electrónicas, el consentimiento será también la base del tratamiento de datos personales conforme al RGPD. Tratar de legitimar el tratamiento conforme a otra base del RGPD -como por ejemplo, el interés legítimo- cuando el mismo tratamiento requiere de consentimiento conforme al marco e-Privacy sería una redundancia. Asimismo, también

genera una situación de deslealtad para el usuario del servicio, que confía en que, si el tratamiento se basa en su consentimiento, este podrá ser retirado sin que el responsable alegue a continuación que la base a partir de dicho momento será el interés legítimo.[548] Por otro lado, en muchas ocasiones la recolección de datos también podrá estar sostenida en la necesidad para cumplir con una obligación contractual o precontractual entre el interesado y el responsable del tratamiento.

Por último, en ocasiones, aquel responsable que recoge datos con la aquiescencia del interesado ya planea reutilizarlos con las finalidades secundarias propias de la Fase 2-Análisis sobre la base de un interés legítimo, casi siempre propio. En dicho caso, la información presentada al interesado en el momento de la recogida de dichos datos deberá incluir ya toda aquella información referida a las subsecuentes finalidades que tendrán los datos, con el grado de detalle que en dicho momento sea posible.

1.2. Fase 2 del big data, análisis y descubrimiento

Esta fase conlleva realizar un tratamiento de datos a través del uso intensivo de algoritmos para descubrir correlaciones, patrones de comportamiento y, en definitiva, conocimiento que se encontraba oculto en la complejidad de los datos y que no es patente a simple vista. Con este nuevo conocimiento se puede, por ejemplo, crear perfiles. En este momento, cabe señalar que la creación de perfiles es un proceso diferente que la aplicación de dichos perfiles.

La creación de perfiles se basa en descubrir nuevo conocimiento y en la capacidad de llegar a realizar inferencias y crear modelos de mayor o menor automatización. Por ejemplo, los datos pueden revelar la información de que aquellas personas que comparten determinadas características son propensas a consumir un producto específico o realizar

[548] INFORMATION COMMISSIONER'S OFFICE (2019): *Update report into adtech and real time bidding*, p. 17.

un consumo energético mayor a ciertas horas del día. También se pueden extraer conclusiones sobre cómo afecta una circunstancia específica en el comportamiento de los individuos agrupados en el mismo perfil. Por ejemplo, cómo afecta la edad, el nivel de formación y el lugar de residencia de una persona sobre la tasa de impago crediticio en una sucursal bancaria.

Al considerar el ámbito de aplicación y los límites de una finalidad concreta, el Convenio 108 y el Reglamento general de protección de datos se basan en el concepto de compatibilidad: se admite el uso de los datos para fines compatibles por razones del fundamento jurídico inicial. Por tanto, no se puede realizar un tratamiento ulterior de los datos de una manera inesperada, inapropiada o inaceptable para el interesado.[549] En este sentido, es necesario destacar que la noción de compatibilidad se basa en lo establecido en los arts. 5.1.b) y 6.4 RGPD.

Según estos, el tratamiento de datos con fines estadísticos no será considerado incompatible con la finalidad original del tratamiento. En atención a las circunstancias del caso concreto, cabría preguntarse si determinadas actividades de tratamiento que utilizan tecnologías big data para producir conclusiones a través de datos agregados podían definirse como finalidades estadísticas -o incluso tratamiento de datos anónimos, en cuyo caso, este queda fuera del alcance del RGPD-. Cuando dicho tratamiento pudiese ser considerado una finalidad estadística, el responsable ostentaría en todo caso la obligación de implementar garantías adecuadas, tales como la minimización de datos o la seudonimización (art. 89.1). Asimismo, cabe recordar que, según indica el considerando 162, para que pueda considerarse que el tratamiento tiene finalidad estadística, el resultado del tratamiento deben ser datos no personales, sino agregados, y que estos no sean utilizados posteriormente como base para la toma de

[549] AGENCIA DE LOS DERECHOS FUNDAMENTALES DE LA UNIÓN EUROPEA Y CONSEJO DE EUROPA (2019): *Manual de legislación europea en materia de protección de datos*, Ed. 2018, Luxemburgo, p. 140; CONSEJO DE EUROPA (2018): *Informe explicativo del "Convenio 108" modernizado para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal*, apartado 49.

decisiones que afecten a personas físicas concretas. Es decir, la elaboración estadística debe ser el fin último del tratamiento.

Sin embargo, el centro de interés de este trabajo son precisamente aquellos tratamientos de datos personales que sí afectaran a las personas físicas individuales. Por este motivo, lo más razonable será suponer que en la mayoría de ocasiones pueda existir incompatibilidad entre la finalidad primaria y la secundaria, siendo necesario ostentar una base de licitud diferente para el tratamiento de la Fase 2-Análisis.

En este momento, sería posible acudir al art. 6.1.f) RGPD como base de licitud.

Como ya vimos, dicho interés legítimo debe superar un test de necesidad. En concreto, el tratamiento debe ser necesario para satisfacer la finalidad del tratamiento, que ha debido ser previamente claramente especificada con anterioridad.

La manifestación clara y transparente de los intereses en lid, así como de los fines del tratamiento debe ser expresa y caminar en favor de una mayor predictibilidad en cuanto al tipo de actividad de tratamiento y sus posibles consecuencias. Todo ello a pesar de que, por su propia naturaleza, el resultado de la Fase 2-Análisis pueda ser impredecible en cuanto a su contenido.

Sin embargo, en el momento de la recogida de los datos (Fase 1) identificar todas las finalidades secundarias posteriores (Fases 2-Análisis y 3-Aplicación) en muchas ocasiones no es posible. Esto es más cierto cuando el tratamiento incluye el uso de tecnologías de análisis masivo de datos para descubrir patrones, correlaciones e información nueva a través de la cual se podrán manifestar utilidades de los datos no previstas, o no con un nivel suficiente de detalle.

Por este motivo, en la mayoría de las ocasiones no será posible utilizar una única base de legitimación para todo el proceso (Fases 1, 2 y 3). En otras palabras, el título de licitud que sirve para la recogida de los datos en un inicio no podrá legitimar, en muchos casos, tratamientos posteriores. Por

este motivo, desarrollar una explicación sobre la existencia de diferentes fases, y en concreto, la observación de la Fase 2 sirve al objeto necesario de reflejar la existencia de un período intermedio entre la recogida de los datos y la toma de decisiones sobre los interesados. Asimismo, esta fase aporta un nuevo momento para especificar las finalidades del tratamiento y aportar transparencia.

En ocasiones, se pretende justificar la existencia de legitimidad para llevar a cabo determinados tratamientos de datos bajo el mismo título de licitud que sirvió para la recogida de los datos. Desde un punto de vista de técnica jurídica, se trata en realidad de ampliar o estirar la cobertura del título de licitud de manera artificial. Por otro lado, en ocasiones, los responsables del tratamiento presentan las actividades de tratamiento consistentes en la analítica de datos para la creación de perfiles como una parte, no siempre informada, de otra actividad de tratamiento. De este modo, esto genera tratamientos implícitos de los que los interesados no son razonablemente informados.

Por ello, la asunción expresa de la Fase 2-Análisis y su base sobre el interés legítimo puede servir de solución garantista para el interesado a la par que suficientemente flexible para el responsable.

Por otro lado, cuantos mayores indicios existan de que el tratamiento de datos resulta inocuo o poco intromisivo, y de que el interés legítimo del responsable puede aportar un beneficio tangible, tanto para él a nivel individual como para la sociedad, mayor justificación habrá para poder concluir que el tratamiento está justificado. En este punto por tanto son muy relevantes las medidas de seguridad jurídico-organizativas que el responsable implemente con el objetivo de reducir el posible riesgo remanente que dicho tratamiento de datos implique para los sujetos. De hecho, en muchas ocasiones, las actividades de análisis de datos y modelización podrán ser llevadas a cabo utilizando datos anónimos, en cuyo caso, la actividad quedaría fuera del ámbito de aplicación de la normativa de protección de datos. Sin embargo, el avance técnico y la cada

vez mayor riqueza de las bases datos facilitan de manera creciente la capacidad de reidentificar información previamente anonimizada. Por este motivo, será prudente considerar a falta de certeza firme, el set de datos contendrá en realidad datos disociados o seudónimos. Por su parte, la tercera fase conlleva como norma general que la información se refiera a una persona concreta y, por tanto, el tratamiento de datos personales.[550]

Asimismo, las actividades de investigación, descubrimiento de información y análisis podrán ser ejecutadas en un entorno de pruebas, que debe estar debidamente aislado del entorno real. De este modo, aumentan las garantías de que el impacto sobre los interesados se reduciría enormemente.

1.3. Fase 3 del big data, aplicación del modelo

Durante la segunda fase se había obtenido conocimiento nuevo y detectado patrones genéricos sobre los datos. En muchas ocasiones, los resultados de la analítica de datos finalizan cuando la organización dispone de información estadística o agregada y crea modelos explicativos de la realidad.

En otras ocasiones, no obstante, los resultados de la fase de análisis se utilizan en un momento posterior para ser aplicados a personas concretas.[551] En la Fase 3-Aplicación, la información que la organización tiene a su disposición sobre un interesado particular es introducida en el modelo obtenido de la fase anterior, de modo que es posible categorizarle, incluirle en un perfil de población e inferir características suyas no conocidas pero que podría compartir con el grupo de población en el que ha sido incluido. De este modo, es posible actuar de manera personalizada.

[550] CONSEJO DE EUROPA (2011): *The protection of individuals with regard to automatic processing of personal data in the context of profiling, Recommendation CM/Rec(2010)13 and explanatory memorandum*.

[551] ZARSKY, Tal (2017): “Incompatible: The GDPR in the age of big data”, en *Seton Hall Law Review*, Vol. 47, No. 2, p. 1000.

Por este mismo motivo, esta fase es quizás la que más consecuencias tiene sobre la vida de las personas, ya sean positivas o negativas.

En caso de que esta fase conlleve una toma de decisiones automatizadas, o la aplicación de perfiles o actividades de personalización por medios únicamente automatizados que cumplan con los requisitos del art. 22, el tratamiento únicamente podrá ser legitimado por el consentimiento del interesado, un contrato o por ley. En el caso de que no existan tratamientos incluidos en el ámbito del art. 22, será posible alegar otras bases de licitud, tales como el interés legítimo. De hecho, ya vimos en el capítulo anterior cómo la interpretación de los términos del art. 22 podría causar que una gran cantidad de tratamientos quedaran fuera de su ámbito de aplicación.

En cualquier caso, es sensato imaginar que fruto del conocimiento obtenido por el responsable en la Fase 2, se hubiesen podido idear acciones, servicios o utilidades diferentes no predecibles en el momento de la recogida de los datos en la fase primera. Acciones cuyas finalidades e información no pudieron ser comunicadas al interesado con el nivel de exigencia que requieren los arts. 13 o 14 RGPD. Por ello, el momento anterior al tratamiento de datos de la Fase 3 es aquél en el que el responsable cuenta con la información más precisa sobre la finalidad del tratamiento, sus riesgos inherentes o las consecuencias para los interesados.

Imaginemos, así, que se produce una la toma de decisiones sobre el interesado que cumple los requisitos del art. 22, y para la que el responsable debe solicitar el consentimiento o la firma de un contrato, e informar consecuentemente. Este es, de hecho, el momento en el que el interesado puede ser informado de modo más completo y transparente, y le permite ejercer un verdadero control. Es decir, se trata de separar el momento en el que se solicita el consentimiento para la recogida de los datos y para la toma de decisiones automatizadas en desarrollo de finalidades secundarias. Así, dicho consentimiento puede recabarse

cuando el responsable cuenta con más información y el individuo aún no ha soportado el impacto de la decisión.[552]

En este momento, muchas de las consecuencias o riesgos han podido ser descubiertos y analizados en la Fase 2, antes de la cual no podrían haber sido previstos ni explicados. Esta postura también fue defendida por el ya extinto Grupo de Trabajo del Artículo 29,[553] manifestando que, si bien es cierto que el consentimiento se recaba en muchas ocasiones en el momento de la recogida de los datos, también se puede obtener en un momento posterior (lo que el Grupo denominó "*downstream consent*"), cuando la finalidad del tratamiento cambia.

Sin embargo, esta aproximación no soluciona todas las limitaciones del consentimiento que fueron analizadas en su capítulo correspondiente. En concreto, sigue persistiendo el hecho de que el interesado se ve colocado en una posición que le fuerce a actuar como ente de control del responsable para detectar y paralizar usos de los datos y tratamientos en ocasiones dañinos o abusivos. Por otro lado, y en relación con ello, también persiste el problema de que el interesado, si bien recibe información en el momento en el que el responsable puede ser más transparente, puede verse abrumado por la dificultad de esta y la carga de deber comprenderla para decidir.

Una primera vía de actuación frente a ello es reducir en lo posible las solicitudes de consentimiento. De hecho, algunas voces han defendido también la idea de que el consentimiento debe reservarse para aquellas situaciones en las que el responsable pretenda separarse de las normas o las expectativas razonables que el individuo tenga respecto de la protección de sus datos personales y en las que sea necesario que el individuo renuncie a sus derechos o acepte tratamientos que de otro modo no serían esperables. En este grupo podemos encontrar al Foro Económico

[552] CORMACK, Andrew Nicholas (2016): "Downstream consent: A Better Legal Framework For Big Data", en *Journal of Information Rights, Policy and Practice*, Vol. 1, No. 1.

[553] GRUPO DE TRABAJO DEL ARTÍCULO 29 (2011): *Dictamen 15/2011 sobre la definición de consentimiento* (WP187), de 13 de julio.

Mundial[554] y a diversos autores como Solon Baroccas y Helen Nissenbaum[555], o los Profesores Fred H. Cate y Viktor Mayer Schönberger[556]. Mediante este mecanismo, los individuos prestarían mayor atención cuando el consentimiento les sea requerido, de manera que este instrumento recupera parte de su valor real. Pidiendo el consentimiento para una intervención particular, el responsable resalta cuándo se llevará a cabo una actividad que podría suponer un riesgo para el individuo, y a la vez tiene información suficiente para delimitar los objetivos y fines del consentimiento, así como para informar de los beneficios que la intervención podría tener para la persona. De este modo, la mera solicitud de consentimiento sirve de alerta al interesado de que existe un posible riesgo, mayor de lo razonablemente esperado, que debe llamar su atención y ser sopesado. Así, el usuario se desprende de la carga de tener que interpretar o diferenciar entre peticiones de consentimiento para tratamientos razonablemente inocuos y para tratamientos de mayor impacto.

Por su parte, aquellos tratamientos cuyo riesgo pueda ser mitigado podrán basarse, como regla general, en interés legítimo.

2. Una visión holística de la protección de datos. Del individualismo a la colectividad

A lo largo de todo el texto, nos hemos referido en múltiples ocasiones a un factor que hemos mencionado de manera reincidente en todos los capítulos: la existencia de asimetrías de información y desequilibrios de

[554] FORO ECONÓMICO MUNDIAL Y THE BOSTON CONSULTING GROUP (2012): "Rethinking Personal Data: Strengthening Trust", en *Proyecto Rethinking Personal Data*.

[555] BAROCCAS, Solon; NISSEBAUM, Helen (2014): "Big data´s End Run Around Anonymity And Consent", en *Privacy, big data and the public good. Frameworks for engagement*, Cambridge University Press, p.44-75.

[556] CATE, Fred H.; MAYER-SCHÖENBERGER, Viktor (2013): "Notice and consent in a world of Big data", en *International Data Privacy Law*, Vol. 3, No. 2.

poder entre los diferentes agentes que forman parte del ciclo de vida de los datos personales en procesos big data.

Estas asimetrías son uno de los factores en común que encontramos en la mayor parte de potenciales problemas y limitaciones que hemos identificado. Estas surgen como consecuencia de aquellos procesos técnicos que son cada vez más complejos de comprender, de un modo que no sucedía con anterioridad, son más impredecibles y que provocan dificultad para imaginar las consecuencias de su uso. Esto es, van intrínsecamente ligadas a aquellas características con las que hemos definido a las tecnologías big data o de recolección y tratamiento masivo de datos.

Dichas asimetrías causan deficiencias en el ejercicio de la capacidad de control de los interesados tal y como se ha entendido tradicionalmente. Esto es, el control de la persona, entendido como la potestad de llevar a cabo un proceso lógico de elección previa, que se sustenta sobre la base de que ha comprendido qué opciones se le presentan y sus implicaciones, y por ende, ligado a la manifestación de su consentimiento.

Estas asimetrías parecen sistémicas, en el sentido de que se manifiestan más allá de la elección de una base de licitud determinada. A pesar de ello, la elección de una base u otra puede acentuar o suavizar estos desequilibrios y a ello hemos dedicado el esfuerzo central de este estudio.

Pues bien, uno de los motivos que explican la creación y cristalización de las asimetrías a las que ya hemos hecho referencia es el hecho de que el derecho a la protección de datos es visto desde una perspectiva individualista.

Ello no es casual, pues este derecho tiene una clara vocación de individualidad. La propia concepción del derecho a la protección de datos personales encuentra sus raíces en una visión individual de la persona. Así pueden entenderse los inicios de este derecho en las construcciones

doctrinales del derecho a ser dejado en paz ("*right to be let alone*")[557] o el derecho a la privacidad, nacido como un límite a las injerencias sobre la vida privada[558] o incluso el derecho a la autodeterminación informativa. La evolución de estos conceptos hacia la definición actual del derecho a la protección de datos personales se fundamenta, asimismo, en el reconocimiento de la necesidad de proteger el poder de disposición de los datos referentes a cada persona.

Ello se hizo patente en la importante sentencia del Tribunal Constitucional 290/2000 de 30 de noviembre, por la que se reconocía la existencia del derecho a la protección de datos como ente autónomo. En dicha sentencia, el Tribunal indica que "*el contenido del Derecho fundamental a la protección de datos consiste en un poder de disposición y control sobre los datos personales que faculte a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, y que también permite al individuo saber quién posee esos datos personales y para qué (…)*".

Estas líneas resultan de gran importancia, pues la definición del derecho a la protección de datos no es baladí. A pesar de ello, el TJUE no ha definido con esta especificidad, y el RGPD tampoco contiene una definición. Atendiendo a la Sentencia de nuestro Tribunal Constitucional, el extracto revela la naturaleza del derecho a la protección de datos ligada intrínsecamente a la persona, a su capacidad de control y al ejercicio de la voluntad individual, y así lo ha entendido la doctrina.[559]

Sobre esta construcción se ha continuado desarrollando el derecho a la protección de los datos personales. Pongamos algunos ejemplos. El art. 21

---

[557] WARREN Samuel D.; D. BRANDEIS, Louis (1890): "Right to privacy", en *Harvard Law Review*, Vol. 4, No. 5, p. 193.

[558] PIÑAR MAÑAS, José Luís; CANALES GIL, Álvaro (2011): *Legislación de protección de datos*, 2ª ed., Madrid, lustel, pp. 26-27.

[559] PIÑAR MAÑAS, José Luís (2016): "El objeto del Reglamento", en José Luís Piñar Mañas (dir.), Reglamento General de Protección de Datos: Hacia un nuevo modelo europeo de privacidad, Madrid, Reus; MARTÍNEZ MARTÍNEZ, Ricard (2004): *Una aproximación crítica a la autodeterminación informativa*, Madrid, Civitas.

RGPD concede al interesado el derecho a oponerse “por motivos relacionados con su situación particular a que datos personales que le conciernan sean objeto de un tratamiento”. Por su parte, el art. 22 RGPD ya indica esta característica en el propio título, “Decisiones individuales automatizadas, incluida la elaboración de perfiles”. Dicho derecho puede ejercerse, entre otras circunstancias, cuando la decisión contestada por el interesado “produzca efectos jurídicos en él o le afecte significativamente de modo similar”. En la misma línea se encuentra la naturaleza propia del consentimiento, en tanto instrumento manifestación de la autonomía individual y el ejercicio de un poder de decisión sobre el tratamiento de los datos personales que se refieran a la propia persona. Incluso el ejercicio de ponderación del interés legítimo, que debe poner en una balanza los derechos y libertades fundamentales del interesado, considerado este como un ciudadano medio, pero en todo caso en términos individualistas.

Es importante garantizar la participación del interesado en la toma de decisiones sobre los usos y finalidades del tratamiento. Sin embargo, quizás ha llegado el momento de poder determinar que, en entornos complejos, impredecibles y de múltiples actores, esa garantía no se convierta en una carga. El sistema de gobernanza de los datos, así como el modo de aplicarlo debe evolucionar en la misma medida en que lo hace el desarrollo tecnológico.

Cierto es que el desarrollo conceptual de los derechos individuales, entre los que se encuentran los derechos de privacidad y protección de datos personales sí toman en consideración en cierta medida la perspectiva social y la importancia que garantizar estos derechos tiene en el bien general. No obstante, el objeto de protección es eminentemente individual.

Por otro lado, ha quedado ampliamente argumentado que en la era de las tecnologías big data, aprendizaje automatizado, Internet de las Cosas y economía basada en datos, el centro focal de la normativa debe ser el responsable y un sistema de obligaciones dirigido a este. Este cambio debe relevar la visión clásica de protección de datos centrada en la persona y

sus derechos que, si bien nunca deben ser desechados, su papel como la base esencial de la protección debe ser actualizado. Es de este modo como podemos conseguir que la protección sea real, efectiva y trascendente, no solo para un interesado concreto, sino para la sociedad en su conjunto.

Por último, hemos visto también como cada vez con mayor asiduidad el individuo medio se expone a situaciones en las que no es consciente del tipo de tratamiento de datos que se llevan a cabo ni manifiesta su voluntad de ningún otro modo. Esto se refiere no únicamente a los datos sobre la persona en concreto, sino también y especialmente, al conjunto total de datos. Esto es, la visión global del tratamiento.

Pues bien, pongamos en relación todos estos factores, que han aparecido de forma trasversal a lo largo de nuestro análisis, a la luz del objeto central de estudio, que ha sido la base de licitud del tratamiento.

Hemos argumentado la necesidad de un cambio de percepción en relación con la base de licitud del tratamiento, descargando el uso del consentimiento como regla por defecto para acudir en mayor medida al uso de un reforzado interés legítimo. En efecto, el consentimiento es un acto básicamente individualista, en la medida en que es solicitado a cada persona a título propio, y se otorga o se rechaza por este atendiendo a factores individualistas tales como ¿estoy dispuesto a acceder a permitir que un agente adquiera mayor conocimiento sobre mi a cambio de obtener, por ejemplo, un contenido más acorde con mis gustos? Cuando al individuo se le presentan diferentes opciones conforme a las que debe actuar, en muchas ocasiones este únicamente se toma a sí mismo y sus intereses particulares como objeto de protección. En pocas ocasiones el proceso de otorgar o denegar el consentimiento discurre de modo que el interesado se pregunte por los efectos de la recolección de datos, no sobre él, sino como parte de un conjunto masivo. Uno de los motivos puede verse en la falta de conocimiento de los individuos sobre las consecuencias del tratamiento de datos personales e información sobre este a nivel agregado. Y sin embargo,

es precisamente el efecto colectivo a gran escala el más pernicioso en el tiempo.

Pensemos ahora en aquellas ocasiones en las que la legitimación del tratamiento no se hace depender del asentimiento del individuo, sino que se acude a la existencia de un interés que trasciende la valoración personal de aquel cuyos datos son tratados. Así podría suceder cuando se acude al interés legítimo del art. 6.1.f) -o incluso a la existencia de un interés público del art. 6.1.e) RGPD-. En dichos casos, puede hacerse incluso más acuciante la necesidad de que el responsable de los datos comprenda el contexto y las consecuencias globales del tratamiento, así como facilitar a los interesados la comprensión. En efecto, el debido ejercicio de ponderación previo a la aplicación del interés legítimo como base del tratamiento debe observar factores, no solo individualistas, sino colectivos. Así, por ejemplo, el responsable debe atender al factor de la cantidad de datos recolectados o el impacto del tratamiento en sentido amplio, factores que, por otro lado, nadie tiene capacidad de conocer mejor que el propio responsable.

Tradicionalmente, las organizaciones cuentan con experiencia en la identificación y medición de riesgos y consecuencias tangibles tales como pérdidas financieras o aquellos causados por brechas de seguridad. Sin embargo, es necesario analizar un espectro más amplio de riesgos derivados de tratamientos de datos a gran escala. Estos riesgos pueden incluir desde la pérdida de confianza, efectos intimidatorios (el conocido como *chilling effect*), la cristalización de modelos de vigilancia masiva, amenazas a los sistemas democráticos, o las burbujas de filtros (“*filter bubbles*”).

Hasta ahora, hemos hecho referencia únicamente de manera implícita a dos consecuencias, que conviene destacar de manera explícita.

En primer lugar, es muy complejo comprender qué efecto tiene sobre la propia persona el tratamiento de datos personales que se refieren a terceros. En segundo lugar, sucede también que es muy complejo

comprender cómo afecta el tratamiento de datos de otras personas sobre uno mismo.

Sin duda, existen implicaciones cruzadas en la medida en que el tratamiento de datos de una persona permite elaborar modelos predictivos e inferencias estadísticas que aportan información sobre otras personas. Es lo que Baroccas y Nissebaum bautizaron como la "tiranía de la minoría".[560] En términos sencillos este concepto hace referencia a la capacidad de un responsable de poder inferir datos de una gran cantidad de individuos que no hayan pretendido revelarlos, todo ello a partir de los datos revelados de manera voluntaria por un grupo minoritario de personas. De este modo, mantener en un ámbito íntimo determinada información ya no depende únicamente de uno mismo, sino de las acciones del grupo con el que compartamos otros atributos que sí hemos dado a conocer.

Experimentos realizados han mostrado poder inferir determinados atributos de personas que no habían revelado esta información a partir de la observación de los mismos atributos en otros miembros del grupo. Por ejemplo, analizando los contactos de una persona en redes sociales y conociendo un conjunto de datos de un subgrupo, se puede inferir la titulación universitaria y el año de graduación de una persona,[561] su orientación sexual,[562] o incluso inferir con un alto grado de precisión que una mujer se encuentra en los primeros meses de su embarazo.[563]

Este problema se agrava por el hecho de que la inferencia de datos es una técnica deductiva que aporta un resultado basado meramente en la

[560] BAROCCAS, Solon; NISSEBAUM, Helen (2014): “Big data´s End Run Around Anonymity And Consent”, en *Privacy, big data and the public good. Frameworks for engagement*, Cambridge University Press, p.44-75.

[561] MISLOVE, Alan; et al. (2010): "You are who you know: inferring user profiles in online social networks", en *Proceedings of the third ACM international conference on Web search and data mining,* pp. 251-260.

[562] JERNIGAN, Carter; MISTREE, Behram FT (2009): "Gaydar: Facebook friendships expose sexual orientation", en *First Monday*, Vol. 14, No. 10.

[563] DUHIGG, Charles (2012): “How Companies Learn Your Secrets”, en *The New York Times*, de 16 de febrero.

probabilidad, pero no en la certeza. Recordemos que una inferencia, en el contexto que aquí se discute, es la generalización de que un factor ocurrirá siempre sobre la constatación de que este ha ocurrido en los casos observados con anterioridad. Sin embargo, es crucial no olvidar que una inferencia siempre implica la existencia de un margen de error, y que por tanto solo se manifiesta en términos de probabilidad, nunca de certeza. Es decir, el responsable que actúe sobre la base de un modelo de inferencia de datos trata como dato personal y cierto información de la que no tiene evidencia segura. Sin embargo, los datos inferidos sobre una persona se tratan como ciertos y son base para la toma de decisiones que afectan al individuo y, en un sentido más amplio, al grupo social.

A pesar de todo ello no existe un elenco de derechos o instrumentos de protección efectivos con respecto a los datos inferidos, incluso en vista de la creciente importancia que estos toman en la elaboración de modelos, el enriquecimiento de bases de datos y la toma de decisiones. Especialmente preocupante es también el hecho de la mercantilización de información basada en la creación de inferencias y perfiles con un número amplísimo de terceros. El acceso a paquetes de datos por parte de terceros agentes se produce sin que estos tengan información sobre la fiabilidad de dichas inferencias ni espíritu crítico sobre la veracidad de los datos que sirvieron de base para elaborarlas. Mas aún, incluso en el caso de que un tercero mostrase interés por comprender el proceso de elaboración de un modelo concreto y la creación de inferencias, la posibilidad real de acceder a la información relevante o incluso de comprenderla con un nivel de detalle suficiente como para cuestionarla es mínima. En otras palabras, no existe una protección práctica fuerte frente a una de las prácticas más extendidas y base del modelo económico digital: la creación intensiva de inferencias y sobre la base de datos masivos.

De hecho, el factor que aquí merece ser destacado es la gran influencia que tienen sobre el resto del grupo las decisiones de una persona en relación a los sus propios datos personales.

Eso es posible gracias a técnicas tales como la minería de texto realizada sobre los comentarios en redes sociales, así como el análisis de los contactos de cada persona, su predisposición a reaccionar ante el contenido que se le presenta, o las búsquedas que realizan en internet, etc.

Así, por ejemplo, el análisis de los datos asociados a una persona permite clasificar a dicho individuo conforme a diferentes parámetros de personalidad, tales como la propensión a la ansiedad, comportamientos obsesivos, tendencias depresivas, la extraversión, la curiosidad intelectual o la preferencia por la exposición a nuevas experiencias.[564]

Es, de hecho, la combinación de técnicas de recopilación, agregación y análisis de datos junto con técnicas para dirigir la motivación de grandes grupos de personas lo que entraña potenciales problemas de falta de libertad a gran escala y a largo plazo. Ello es debido a que un conjunto de datos lo suficiente rico acerca de una persona permite conocer sus motivaciones, miedos, ante qué ideas reacciona, su grado de influenciabilidad y, en consecuencia, cuántas veces necesita ser expuesto a un mensaje para comenzar a adquirir un pensamiento y una actitud que determinen sus actos posteriores. A todo ello se añade, por un lado, el uso sibilino de dichas técnicas, y por otro, la falta de comprensión de los individuos de la existencia y el objetivo de este tipo de actividades. Ello, trasladado a la masa, forja corrientes de pensamiento creadas de manera artificial sin generar un sentimiento de falta de libertad. Resaltaba Murillo de la Cueva que sin límites claros, aquellos que recopilan y tratan datos personales, ya sean poderes públicos o privados, “contarán no sólo con un conocimiento potencialmente pleno de la vida de cada uno de nosotros, sino que lo utilizarán para tomar decisiones que nos afectarán directa o indirectamente pero siempre de manera decisiva. El resultado será que

[564] MCCRAE, Robert; JOHN, Oliver P. (1992): "An introduction to the five-factor model and its applications", en *Journal of personality*, Vol. 60, No. 2, pp. 175-215.

estará en peligro el libre desenvolvimiento de nuestra vida e, incluso, nuestra propia identidad".[565] Es la manipulación del libre albedrío.

Todo ello hace cada vez más patente el hecho de el tratamiento de datos personales es un fenómeno de creciente complejidad que adquiere un alcance cada vez mayor que trasciende y escapa de la esfera de la persona concreta.

Los avances tecnológicos y las prácticas de recolección y uso datos personales de los últimos años han intensificado los riesgos y amenazas sobre la privacidad y el ámbito personal de los individuos, pero no han supuesto un cambio de paradigma sustancial. Ello porque el riesgo medido a nivel individual no es novedoso.

Sin embargo, las personas actuamos generalmente conforme a intereses particulares -en el mejor de los casos-, o sin conocimiento de las implicaciones posibles de nuestras decisiones en entornos digitales. Ya expresaba Rousseau hace más de 250 años que, "[s]i no hubiese intereses diferentes, apenas se dejaría sentir el interés común, que nunca hallaría obstáculo".[566]

La sociedad actual necesita un enfoque colectivo de los datos personales y su protección. Protección que, por su parte, merece mantener la categoría de derecho fundamental, esto es, no entendido únicamente como un derecho ligado a la mercantilización de los datos. En otras palabras, se hace necesario reconceptualizar el derecho a la protección de datos personales para incorporar un derecho a la protección de datos colectivos o una perspectiva colectiva del derecho a la protección de datos. Esto permitiría la definición de una nueva oleada de derechos relacionados con la prevención de la manipulación.[567]

---

[565] MURILLO DE LA CUEVA, Pablo Lucas (2007): "Perspectivas del derecho a la autodeterminación informativa" en Revista de Internet, Derecho y Política, No. 5.

[566] ROUSSEAU, Jean-Jacques (1762): *El contrato social*.

[567] En un contexto diferente, en concreto, en relación con los posibles riesgos sobre la protección de datos que puede provocar el tratamiento de datos personales durante la pandemia de Covid-19, Ricard Martínez ha defendido la necesidad de interpretar los

En relación con esta visión, por ejemplo, ya en 2012 Raab y Wright[568] introdujeron el concepto de evaluación de impacto de la vigilancia ("*surveillance impact assessment*"), como respuesta a la crítica de que las evaluaciones de protección de datos se centran en una visión individual del derecho. De este modo, el término vigilancia puede evocar conceptos más amplios que incluyen, entre otros, el impacto del tratamiento de datos sobre grupos y categorías de grupos, así como la sociedad y el sistema político. Es decir, la propuesta de Raab y Wright gira en torno a la idea de introducir en el análisis bienes jurídicos colectivos como el impacto social, político, ético o incluso psicológico.

3. Quiebra de confianza

Ya hemos visto cómo los usuarios de servicios en línea han constatado la existencia de fatiga en relación con ciertas prácticas extendidas de recolección y tratamiento de datos personales y el funcionamiento de servicios digitales. En estas prácticas caben, entre otras, el uso de patrones oscuros con los que se pretende que el usuario muestre su acuerdo con determinadas prácticas, la falta de transparencia, la creciente sensación de vigilancia o la sospecha de que los datos son utilizados para finalidades no anunciadas a los interesados. Más allá de prácticas concretas, el propio funcionamiento de determinadas tecnologías y su complejidad tienen como consecuencia que el interesado se replantee su capacidad de control de los datos personales.

Esto ha provocado una consecuencia que trasciende cada incidente particular: ha provocado una ruptura de confianza en el sistema digital. La confianza se ha quebrado respecto de aquellos que desarrollan una

derechos fundamentales teniendo en cuanto "el sentido de comunidad". MARTÍNEZ MARTÍNEZ, Ricard (2020): Privacidad de los empleados. Prevención de riesgos y salud pública en la pandemia, Foro APEP.

[568] RAAB, Charles D.; WRIGHT, David (2012): "Surveillance: Extending the Limits of Privacy Impact Assessment", en David Wright y Paul de Hert (eds.), *Privacy Impact Assessments*, Dordrecht, Springer; WRIGHT, David; RAAB, Charles D.: "Constructing a surveillance impact assessment", en *Computer Law & Security Review*, Vol. 28, No. 6, pp. 613-626.

actividad económica que hace uso de datos, muchos de ellos personales, así como del funcionamiento mismo del modelo económico digital basado en el tratamiento intensivo de datos.

Al mismo tiempo, los usuarios son conscientes de la dificultad de actuar contra estos modelos, pues ello se hace a riesgo de quedar fuera del funcionamiento de instrumentos sociales hoy en día básicos tales como la comunicación en redes sociales, la compra por internet o el acceso a información a través de medios digitales.

Esta situación no es nueva, sino que se ha ido constatando poco a poco a través del tiempo.[569] De hecho, en la Unión Europea, el RGPD parece tener como objetivo el restablecimiento del equilibro entre usuarios y prestadores de servicios digitales, es decir, reequilibrar la relación responsable del tratamiento-interesado. El considerando 7 del RGPD alude abiertamente a la importancia de generar la confianza necesaria para el desarrollo de la economía digital en el mercado interior.

El interesado ya no hace depender su confianza de la capacidad de control entendido como ser informado y posteriormente preguntado acerca de si autoriza o no determinados tratamientos, pues en muchas ocasiones no alcanza a comprenderlos. Por ello, el concepto tradicional de control como objetivo de la normativa de protección de datos debe desarrollarse y repensarse.

La elección de la base de licitud para el tratamiento de datos personales resulta solo una de las múltiples facetas que muestran la ruptura de confianza del ciudadano sobre los responsables. En este trabajo, nos hemos centrado básicamente en esta manifestación. En efecto, las

[569] Sobre la confianza institucional y la necesidad de restablecer el "punto de equilibrio de la relación de confianza" ver ESTELLA DE NORIEGA, Antonio (2019): "Hacia una Teoría del Derecho como Credibilidad". *Discurso de toma de posesión como Académico Correspondiente de la Real Academia de Doctores de España*.
"[La confianza] se trata de un bien precioso, como el oro, al que es difícil acceder y más difícil todavía extraer. Es, también, un bien fungible, rápidamente fungible, diría yo. La confianza se dilapida velozmente y es difícil de recuperar, una vez dilapidada. La confianza siempre involucra, al menos, a dos personas, o dos jugadores, por emplear la terminología de la elección racional y la teoría de juegos: la persona en la que se confía y la persona que confía".

limitaciones del consentimiento como medio de legitimación bajo el RGPD, así como en la anterior Directiva se deben, en gran parte, a que el interesado no encuentra una sólida base de fiabilidad en aquellos que le solicitan el consentimiento. Por este motivo, el interés legítimo como base de licitud podría verse como una alternativa que permitiría volver a generar confianza en que el responsable, como máximo conocedor de los pormenores del tratamiento, ha debido tomar en consideración un amplio abanico de intereses y derechos de todas las partes involucradas en el tratamiento de datos, de modo que no se deje a la mera valoración del interesado para expresar su aceptación.

Sin embargo, el interés legítimo, en su reflejo actual en el art. 6.1.f) RGPD, contiene ambigüedades que han sido analizadas. Asimismo, esta base de licitud deja diversas cuestiones abiertas a la valoración subjetiva del responsable, tales como la valoración de la existencia de un interés imperioso que haga decaer el derecho del interesado a oponerse al tratamiento. A pesar de todo, no se trata de limitaciones inamovibles.

Por este motivo, la guía de buenas prácticas anexa tiene el objetivo de iniciar un debate en torno a la creación de estándares ampliamente reconocidos que potencialmente puedan llegar a servir a dos finalidades. En primer lugar, la implementación por parte del responsable de un conjunto de buenas prácticas favorecerá la posición de su interés legítimo en el ejercicio de ponderación que requiere el art. 6.1.f) y, por tanto, incrementará la posibilidad de que este precepto pueda finalmente legitimar el tratamiento. En segundo lugar, la adecuación del responsable a una batería de buenas prácticas que incrementen el nivel de transparencia, de estándares éticos y refuerce el ejercicio de derechos ayudaría a regenerar la confianza del sistema sobre los modelos económicos digitales y los procesos de toma de decisiones basados en datos.

En relación con ello, ya vimos en los primeros capítulos que la normativa de protección de datos ha evolucionado desde una aproximación pasivo-reactiva hacia una visión proactiva. El principio de *accountability* o, en su

traducción al español, responsabilidad proactiva es quizás el reflejo más claro de ello. Sin embargo, el análisis de datos que se da en entornos de alta complejidad, sobre el que pueden repercutir grandes beneficios, pero también mayores riesgos, exige un paso más para restaurar la confianza de las personas en el ecosistema digital.

En este tipo de contextos, los efectos de la norma en la práctica son muy dependientes de factores abiertos como la interpretación de conceptos jurídicos indeterminados, la falta de experiencia, el rápido desarrollo técnico a mayor velocidad que el desarrollo normativo, etc. Por ello el responsable del tratamiento debe ser, no solo proactivo sino preactivo. La preactividad es la capacidad de asegurar que se den las condiciones necesarias para que un resultado ocurra, a través de pequeñas acciones que proyectan consecuencias a medio o largo plazo. En términos sencillos, anticiparse.

Un enfoque preactivo del responsable podría incluir responder a ciertas cuestiones que no se plantean en términos de mero cumplimiento normativo en la actualidad. Por ejemplo ¿qué nuevos usos le pueden dar los consumidores a nuestro producto? ¿Qué nuevos efectos sobre la privacidad puede ello conllevar? ¿Cuál es la dirección hacia la que se orienta el desarrollo de nuevas tecnologías? ¿Puede ello crear nuevas formas de ataques de terceros intrusos? ¿Hay algún ángulo diferente desde el que observar el nuevo desarrollo que queremos presentar en el mercado? Esta metodología conlleva aplicar un pensamiento que aúne análisis, creatividad e intuición. En este sentido, el Derecho no debe ser una barrera a la innovación, sino el camino para la innovación responsable.

Esta puede ser una vía de estudio y desarrollo en los próximos años. Por el momento, este trabajo pretende ser solo un primer paso en esa dirección, y por ello, la guía de buenas prácticas aquí presentada tiene en cuenta aspectos que superan lo estrictamente requerido por la norma.

A pesar de que el modelo aquí propuesto sienta el foco de vigilancia sobre la forma de actuar de los responsables y la necesidad de control de las autoridades, no debemos olvidar las prerrogativas de los interesados. El

RGPD otorga un amplio marco de derechos, algunos de los cuales se introdujeron de manera novedosa con el RGPD y otros se reforzaron.

El último eurobarómetro[570] destacaba que más del 67% de los ciudadanos comunitarios conoce la existencia del Reglamento General de Protección de Datos, aunque de entre ellos, cerca de la mitad no conoce qué es. En términos similares, una amplia mayoría del 73% conoce al menos uno de sus derechos, pero el porcentaje de ciudadanos que manifiesta haber escuchado sobre la existencia de todos sus derechos es mucho menor, concretamente de un 31%, siendo el derecho a oponerse a ser objeto de decisiones automatizadas el más desconocido y el menos ejercitado. Esto es especialmente relevante pues, además, el desconocimiento aumenta drásticamente en el grupo de personas que enfrenta problemas para pagar sus deudas -y por tanto sobre las que, por ejemplo, la toma de decisiones automatizadas para calcular las condiciones de un préstamo pueda generar mayor impacto-.

El desarrollo y la innovación que las técnicas de *big data*, la minería de datos o el *cloud computing* implican serán una fuente de beneficios sociales y económicos que no debemos desaprovechar. Por eso se hace necesario buscar soluciones que permitan flexibilizar el tratamiento de datos, al mismo tiempo que se protegen los derechos de los individuos, y focalizar las limitaciones al tratamiento de los datos en función del contexto específico en lugar de hacerlo de manera generalizada. Solo de este modo podremos favorecer los usos positivos del nuevo conocimiento al tiempo que se restringen los usos nocivos para los individuos.

El sistema aquí defendido necesita un alto grado de madurez de los responsables de datos, así como un fuerte compromiso para adoptar estándares de seguridad elevados. Esto refuerza de nuevo la idea de que ya no es el usuario el centro de responsabilidad de los datos, sino las organizaciones que quieren hacer uso de ellos.

---

[570] COMISIÓN EUROPEA (2019): *Special Eurobarometer 487ª, The General Data Protection Regulation.*

No cabe olvidar que la sociedad actual evoluciona más rápido que nunca antes en la historia, y estos cambios deben manifestarse también a nivel jurídico. Para ello, es imprescindible que juristas y reguladores realicen el esfuerzo de acercarse y comprender los entornos tecnológicos, del mismo modo que aquellos profesionales técnicos deben concienciarse y formarse en aspectos legales. Queda mucho camino por recorrer, pero sin duda la promulgación del nuevo Reglamento europeo de protección de datos es el fruto de un esfuerzo por estrechar ambos escenarios.

Por último, no sin razón, algunos de los mayores exponentes de nuestro Derecho vuelven la vista hacia las bases de lo que debe ser el Ordenamiento jurídico para tratar los retos del presente. En estas bases, no se encuentra otra cosa que lo que en cada momento se conforme como la concepción moral de la sociedad.

Así quiero recuperar las palabras de Gregorio Peces-Barba, de quien tuve el placer de recibir mi primera lección en la Facultad de Derecho hace ya unos años: “No se debe desconocer, sin embargo, la raíz ética que está en los cimientos de los conceptos de derechos y deberes fundamentales, y que explica la confusión y la identificación de sus dimensiones ética y jurídica. Sí parece conveniente reservar lo jurídico para aquellas normas aprobadas por los órganos y por los procedimientos establecidos en la norma de identificación de normas de un Ordenamiento positivo, y en esta materia, no todo lo que ese Derecho positivo calificase como derecho o deber fundamental podría considerarse como tal. Sólo lo sería aquel Derecho que fuera coherente con la moralidad crítica que ha elaborado el concepto de derechos fundamentales o derechos humanos con la pretensión de incorporarlos al Derecho positivo, única dimensión en la cual adquieren los derechos su pleno desarrollo. De ahí la importancia de la indagación sobre esa moralidad crítica que llamo filosofía de los derechos fundamentales”.[571]

[571] PECES-BARBA MARTÍNEZ, Gregorio (1987): *Derechos Fundamentales*.

Peces-Barba estudió la relación entre moral y Derecho positivo, y en concreto, en relación con los derechos fundamentales. Fue además Padre de la Constitución, base de la emana en nuestro Ordenamiento nacional la construcción de la protección de datos personales, sin la que este estudio no Por su parte, José Luís Piñar, en su análisis sobre los retos de la técnica y la disrupción en el sistema jurídico, ha reiterado que, en los momentos de retos concretos y específicos debemos volver a la ética y a los principios. Rescataré de sus palabras las siguientes: "El Derecho debe ahora dar respuesta a retos derivados de una innovación rápida y constante en un mundo global y digital. Para ello ha de volver a los principios e ir de la mano de la ética"[572] y "Derecho e innovación no son incompatibles, sino que pueden y deben convivir, partiendo siempre de la importancia que tiene basar la protección de la privacidad en principios jurídicos fundamentales que tengan en cuenta los elementos esenciales de la relación entre privacidad e innovación en la sociedad actual".[573]

4. Conclusiones

El análisis de los capítulos anteriores nos he dejado un conjunto de premisas: en primer lugar, el consentimiento como base de licitud presenta limitaciones de muy compleja solución en entornos de tecnologías impredecibles y difíciles de comprender por los interesados. En cambio, el interés legítimo es una alternativa con potencial para subsanar algunas de estas limitaciones, aunque sin obviar que también tiene aristas y deja cuestiones abiertas.

[572] PIÑAR MAÑAS, José Luís (2018): "Derecho. Ética e innovación tecnológica", en *Revista española de derecho administrativo*, No. 195, pp. 11-30.

[573] PIÑAR MAÑAS, José Luís (2017): "Sociedad, innovación y privacidad, Información Comercial Española", en *ICE: Revista de economía*, No. 897, pp. 67-76.

En este capítulo hemos podido realizar una propuesta de elección de base de legitimación para tratamientos que utilizan tecnologías de datos masivos.

La Fase 1- Recolección tiene como objeto principal la recogida de datos y su preparación para el tratamiento. En esta, pueden concurrir diferentes bases de licitud en función de las circunstancias de cada caso. Por su parte, la Fase 2- Análisis implica tratar los datos con medios técnicos que permitan descubrir correlaciones, patrones de conducta, crear información nueva y realizar inferencias con las que construir un modelo algorítmico general. En esta fase, el interés legítimo puede servir de base de licitud.

La última fase, Fase3- Aplicación implica tratar los datos de una persona concreta, introducirlos en el modelo genérico construido en la fase anterior y obtener conocimiento, inferencias y conclusiones sobre esta persona en concreto. En esta fase, el consentimiento podrá ser una base de licitud adecuada. Ello porque el responsable a tenido un margen -la fase 2- en el que obtener conocimiento sobre las consecuencias del modelo, el tipo de nueva información creada etc. que solo en este momento puede comunicar de manera completa y transparente.

A continuación, hemos analizado un contexto más amplio que aquél únicamente formado por las bases de licitud del RGPD, pero ligado con ello. El derecho a la protección de datos es naturalmente individualista, y sin embargo, los mayores riesgos de las tecnologías big data surgen del análisis combinado de información sobre personas que permitan extraer información agregada y actuar en masa. De este modo, el acercamiento hacia concepción colectiva de la protección de datos podría crear garantías donde que la visión personalista no llega.

Este debate es amplio, pero está reflejado en la forma en que operan las bases de licitud del tratamiento, a las que hemos dedicado nuestro estudio. Así, el consentimiento, tradicionalmente utilizado como base por defecto, tiene un carácter marcadamente individual. Cada uno de nosotros prestamos el consentimiento o no en función de una decisión que tomamos

sobre nuestros propios intereses, casi siempre, sin tener en cuenta los beneficios o riesgos del tratamiento agregado de la información sobre otras personas. Sin embargo, el interés legítimo es una base de licitud apta para incluir en su análisis y ponderación factores como el impacto del tratamiento a nivel colectivo.

Por último, concluimos que en los últimos años el avance tecnológico a una velocidad sin precedentes, acompañado de un cuerpo normativo rígido ha creado situaciones que han provocado una ruptura en la confianza de las personas en el modelo digital. En nuestra opinión, solicitar el consentimiento a pesar de las graves deficiencias y poner así la carga de la responsabilidad en el interesado no ayudará a solventar el problema. El interés legítimo, aplicado de manera leal y estricta sí podría restaurar esta confianza.

CAPÍTULO VIII. CONCLUSIONES FINALES

En los últimos años hemos asistido a acontecimientos de gran profundidad en materia de protección de datos. Desde la actualización de las principales normas en la materia hasta escándalos y sanciones a grandes corporaciones por incumplimientos de la normativa. Por otro lado, el avance tecnológico es exponencial, de modo que la rapidez de los cambios y de los nuevos retos surgidos con ellos hacen que debamos replantearnos ciertas cuestiones sólidamente asentadas en materia de protección de datos, como la tradicional prevalencia del consentimiento como base de licitud bajo la idea de que es la que mejor garantiza los derechos de la persona.

A lo largo de todo el camino que han creado estos capítulos hemos ido desbrozando diferentes elementos que pretenden dar respuesta a las cuestiones siguientes:

¿Es el consentimiento como base de licitud un instrumento ampliamente efectivo para la protección de datos de carácter personal en entornos de utilización de tecnologías big data? ¿En su caso, puede el interés legítimo resolver las principales limitaciones del consentimiento?

Revisar conceptos ya existentes bajo un prisma diferente

El objetivo principal de este trabajo ha sido llenar el vacío existente en relación con el estudio profundo de la figura del interés legítimo como base de licitud con potencial y flexibilidad suficiente como para ser capaz de solucionar algunas deficiencias observadas en los últimos años en el funcionamiento del ecosistema digital.

Para ello, el fruto final de la contribución es impulsar un debate en torno a la necesidad de plantear conceptos ya existentes, pero bajo un prisma totalmente diferente. El prisma que nos dan las novedades introducidas por el RGPD y realidad tecnológica actual.

El derecho a la protección de datos se encuentra en la base de otros derechos, como aquél al desarrollo de la personalidad de forma libre y sin verse obligado a seguir el pensamiento mayoritario marcado por la sociedad o un tercero. Por ello, la protección efectiva de este derecho tiene una importancia trascendental.

Asimismo, el derecho a la protección de datos no se opone al tratamiento de datos personales, sino a su uso injustificado o abusivo. Para ello, el cumplimiento del principio de licitud es un elemento esencial del cuerpo normativo.

Las primeras normas de protección de la información personal y de datos personales se referían a la computación y la informática en términos de creación de riesgos (como el Convenio 108 del Consejo de Europa). Sin embargo, esta concepción evolucionó en el reconocimiento del valor económico de los datos, por lo que las normas posteriores ya incluían en sus objetivos favorecer la circulación de datos (véase las Directrices de la OCDE sobre protección de la privacidad y flujos transfronterizos de datos personales de 1980 o la Directiva de protección de datos de 1995). En la actualidad, el RGPD mantiene el doble objetivo de proteger a las personas y facilitar la libre circulación de datos.

Los mayores beneficios y riesgos del big data surgen de la agregación de datos y su aplicación a nivel colectivo

Este doble objetivo de la norma es relevante, pues en la actualidad se crean y tratan más cantidad de datos que nunca antes en la historia, creando beneficios y riesgos a partes iguales. En concreto, los procesos big data presentan sus mayores beneficios por el hecho de que los datos son agregados y tratados de manera masiva para representar parcelas de la realidad de forma más completa. Por ello mismo también presentan riesgos específicos derivados, por un lado, del hecho de que los resultados de un proceso analítico son impredecibles y complejos de comprender. Por otro lado, los procesos big data generan un riesgo derivado de la capacidad de

conocer los gustos y comportamientos de cada persona con un altísimo nivel de detalle, y sobre todo, conocer a una masa de población a nivel colectivo y actuar para modificar su comportamiento.

Necesitamos regenerar la confianza y solventar las asimetrías de información

Por estos motivos, el sistema de generación, recolección, tratamiento y análisis de datos presenta en la actualidad un problema de asimetrías de información entre los individuos y los proveedores de servicios o responsables que causa deficiencias en el ejercicio de control y la efectividad de los derechos de los interesados. Así, generar un entorno de confianza en el funcionamiento de los modelos económicos digitales se convierte en un objetivo primordial.

La sobreutilización del consentimiento ha potenciado sus limitaciones

Desde sus inicios, las normas de protección de datos personales han otorgado una importancia central al consentimiento como fuente de licitud, aunque este nunca fue concebido como la única base de licitud. Esta predisposición es, además, mucho más aguda en España que en otros Estados miembros.

El principal motivo de la popularidad del consentimiento ha sido la percepción de que es el medio que proporciona una mayor capacidad de control por parte de una persona sobre sus datos personales. Consecutivamente, se construye el argumento de que solicitar el consentimiento equivale automáticamente a otorgar a la persona una garantía probada de que el tratamiento se basa en una adecuada protección de los interesados. Sin embargo, si se utiliza de manera incorrecta, el control del sujeto se convierte en ilusorio. Ciertamente no se

trata de un instrumento perfecto, y de hecho su utilización por defecto y de forma tan intensa potenció sus limitaciones.

El consentimiento impone la responsabilidad sobre el interesado

Hemos analizado las principales limitaciones del consentimiento. Una de ellas es el hecho de que sitúa el foco de atención y de responsabilidad sobre el interesado, ya que presupone que antes de consentir la persona ha leído la información que se le presenta, la comprende y toma su propia decisión. Esto se cumple en entornos estables, sencillos de comprender y previsibles.

El consentimiento no funciona en entornos cambiantes, complejos e intensivos en datos derivados de actividades cotidianas

Sin embargo, la digitalización y, en concreto, los entornos técnicamente muy avanzados, permiten recoger cantidades masivas de datos por medios desapercibidos, cambiantes y complejos. En estos contextos, las solicitudes de consentimiento son continuas, para aplicaciones más diversas y con consecuencias más complejas. Además, esto sucede durante el transcurso de actividades cotidianas cuyo proceso mental o de decisión no está relacionado directamente con decidir sobre el futuro de los datos personales. Así, la práctica indica que pocos usuarios leen o comprenden la información, sino que se limitan a aceptar las condiciones que se les presentan de forma irreflexiva y casi automática sin entender el contexto del tratamiento.

A pesar de ello, parece que el legislador comunitario sigue manteniendo una preferencia por el consentimiento frente a otras bases. Por ejemplo, el RGPD ha reforzado las condiciones del consentimiento y las obligaciones de información, y el consentimiento se utiliza de manera preferente a otras bases para legitimar tratamientos como la toma de decisiones

automatizadas, las transferencias internacionales de datos o como una de las circunstancias que permiten ejercer un derecho de portabilidad.

Incluso cuando el consentimiento cumple todos los requisitos formales -lo que hemos definido como el estándar del interesado medio razonable-, no cumple el estándar subjetivo. Se vuelve contra el subjeto

Debido a lo anterior, incluso cuando el consentimiento cumple todos los requisitos formales -lo que hemos definido como el estándar del interesado medio razonable-, su utilidad desaparece y no garantiza que la persona concreta manifieste su capacidad de control -es decir, no cumple lo que hemos denominado el estándar subjetivo-. E incluso aunque se mantuviera la capacidad de control de la persona, solicitar el consentimiento no aporta ningún tipo de verificación sobre cómo se tratan los datos. Es decir, contrario a lo que en ocasiones parece defenderse, el consentimiento por sí solo no aporta una protección adecuada sobre los datos personales.

De este modo, ceñirse al consentimiento ignorando estas graves limitaciones supone responsabilizar a la persona por la toma de decisiones para las que no está preparada, de forma que el consentimiento se le vuelve en contra. En los últimos años un número cada vez mayor de voces también han resaltado los problemas del consentimiento.

Exploramos alternativas: el ambiguo interés legítimo

Por todo ello, en lugar de reforzar el consentimiento, en nuestra opinión las garantías de los interesados podrían quedar mejor protegidas a través de alternativas, y en concreto, aquí hemos analizado el interés legítimo.

El actual art. 6.1.f) RGPD establece el interés legítimo como una de las bases de licitud del tratamiento. Este precepto ha sido heredado de la Directiva de 1995 sin apenas modificaciones. Se trata de un precepto algo ambiguo, poco desarrollado en comparación con títulos de licitud como el

consentimiento y ha constituido el elemento central de este estudio. Se basa en la existencia de un interés, que debe ser legítimo, interpretado ello de forma amplia. El signo distintivito de esta base es la realización de una ponderación entre tales intereses legítimos que persigue el tratamiento (del responsable o un tercero), con los intereses, derecho y libertades de la persona cuyos datos son tratados.

El ejercicio de ponderación ¿el mayor inconveniente o la mayor fortaleza?

Esta ponderación es fuente de algunas de las principales críticas al interés legítimo, pero es precisamente lo que genera un momento único por el que el responsable adquiere la obligación de considerar los efectos del tratamiento, si este es necesario para la finalidad y cuál es el ámbito de afectación sobre los interesados. Se trata de un ejercicio de madurez que debe quedar documentado por escrito, lo que potencialmente puede crear mayores garantías que otras bases de licitud.

El legislador y la autoridad de control española han sido especialmente combativos con el interés legítimo

Antes de comentar las limitaciones del interés legítimo, hay que destacar que la tradición jurídica en España ha sido especialmente combativa contra el interés legítimo, y en concreto, en favor del consentimiento.

Nuestro Tribunal Constitucional ha declarado que la capacidad de control es un elemento esencial del derecho a la protección de datos. Sobre esta base, se consideró que el consentimiento sería la mejor forma de expresar dicho control. Así, nuestro ordenamiento traspuso la Directiva de 1995 creando restricciones que no tenían correspondencia en la norma comunitaria de forma tal que, en lugar de replicar la existencia de varias bases de licitud, se creó una jerarquía de bases de tres pisos: el primero de ellos por orden de prevalencia lo ocupó el consentimiento, que se

configuró como regla general -cuya aplicación además se expandió en la práctica a través del consentimiento tácito-. El segundo piso lo conformaban las demás bases de licitud, excepto el interés legítimo, que se configuraban como excepciones a la regla general. Por último, el interés legítimo ocupaba el escalón inferior, pues su aplicabilidad fue reducida en la LOPD a través de la creación de requisitos más estrictos que los que contenía la Directiva, lo que de hecho, llegó a suponer que el precepto fuera invalidado por el TJUE.

Asimismo, la postura, incluso actual, de la AEPD es contraria a la aplicación del interés legítimo en entornos de tratamiento de datos a gran escala. Por ejemplo, hemos analizado algunas resoluciones en las que, por vía interpretativa, la Agencia añade requisitos adicionales para aplicar el art. 6.1.f) RGPD en actividades tales como el perfilado de datos. Por último, la actual LOPDgdd contiene una lista de casos que operan bajo presunciones de interés legítimo, aunque son tratamientos básicos (como el almacenamiento y acceso de datos de contacto profesional).

Sobre la base de todo lo anterior, apoyamos la postura de no crear actitudes rígidas que descarten el uso del interés legítimo, en concreto, para actividades de tratamiento masivo de datos.

El interés legítimo puede resolver diversas debilidades del consentimiento, pero también tiene limitaciones

Del amplio estudio realizado en este trabajo, consideramos que la evolución digital nos obliga a reconsiderar el interés legítimo con nuevos ojos, pues tiene potencial para suplir algunas limitaciones del consentimiento y crear ventajas para los interesados y responsables.

Hemos analizado las principales críticas y limitaciones del interés legítimo, algunas de las cuales han sido contestadas en los capítulos anteriores y pueden ser suplidas, mientras que otras quedan como cuestiones abiertas.

La criticada ambigüedad del interés legítimo es en realidad flexibilidad, coherente con la adaptabilidad que pretende el RGPD

En primer lugar, una de las principales reticencias que despierta el interés legítimo es su ambigüedad y la falta de criterios normativos claros sobre cómo ha de aplicarse, que podría utilizarse para crear un cajón de sastre y mostrar como lícito un tratamiento que no lo sería bajo las garantías de otras bases de licitud. Esto viene apoyado en el hecho de que el responsable determina el resultado de la ponderación de intereses, actuando como juez y parte.

En nuestra opinión, esta ambigüedad es en realidad flexibilidad, y esta es precisamente una de las características principales que ensalza el modelo de protección de datos creado RGPD, y, de hecho, alabada.

Algunas de las principales disposiciones novedosas del RGPD se basan precisamente en presentar únicamente orientaciones genéricas al responsable, para que sea este quien se adapte las obligaciones al caso concreto y garantice un nivel adecuado de protección a los interesados.

El principal ejemplo de ello es el nuevo principio de responsabilidad proactiva (*accountability*, art. 5.2 RGPD), un concepto esencialmente abierto basado en la necesidad de que el responsable tome medidas adecuadas para el cumplimiento de las obligaciones de protección de datos, que no deben ser concretadas *a priori* (de hecho, es positivo que así sea), así como de demostrar su cumplimiento. Otros ejemplos, que deben regir especialmente los tratamientos a través de nuevas tecnologías son el enfoque basado en riesgos, la obligación de realizar una evaluación de impacto en ciertas circunstancias - concretamente, cuando sea probable que el tratamiento entrañe un riesgo alto para los interesados, y especialmente cuando se utilicen nuevas tecnologías (art. 35 RGPD)-, o la elección de medidas de seguridad y garantías adecuadas al riesgo (art. 32 RGPD).

La flexibilidad, lejos de ser maleabilidad o capacidad de distorsionar el Reglamento, debe ser entendida como la adaptabilidad que permite

alejarse de obligaciones encorsetadas que quedan desactualizadas de forma rápida, especialmente en entornos tecnológicos.

El interés legítimo sí permite ejercer control sobre el uso de los datos personales

En segundo lugar, también se critica del interés legítimo el hecho de que desprende al interesado de su capacidad de control y le deja en manos de un juicio de intereses realizado por el responsable. En realidad, nuestro análisis concluye que se trata de una falacia. Para empoderar a la persona no es necesario ejercer una capacidad de control entendida de modo reducido como únicamente una toma de decisiones *ex ante* (lo que ocurre en el consentimiento). Existen medios diversos ya codificados en la norma que permiten ejercer control, tales como el derecho de oposición, de acceso, de portabilidad o la transparencia. Se tratan, todas ellas, de cuestiones analizadas a lo largo de estas páginas.

Es cierto que la evaluación del interés legítimo se refiere a un interesado medio razonable, no a cada persona en particular. Sin embargo, una persona también puede hacer valer sus circunstancias individuales, que pudieron no ser tomadas en cuenta en la ponderación de intereses, a través del derecho de oposición. Este permite que el interesado cuestione la ponderación y adquiera control.

La expectativa razonable del interesado no debe ser el factor central de la ponderación de intereses. En su lugar, cobra más sentido el impacto sobre el interesado

Por otro lado, basar la evaluación de interés legítimo en factores subjetivos como la expectativa razonable del interesado puede ser contraproducente si llega el momento en que los usuarios se sienten constantemente monitorizados, hasta el punto de crearse una expectativa de vigilancia. Este factor dejaría de ser un elemento de protección en favor del interesado. Por

ello, proponíamos considerar el impacto del tratamiento sobre el interesado como el elemento de mayor peso en la ponderación de intereses.

El interés legítimo no permite crear una falsa sensación de licitud; al contrario, reintegra la responsabilidad en la figura del responsable

En tercer lugar, otra crítica al interés legítimo surge de la percepción de que permitiría legalizar situaciones de otro modo ilícitas, pues el responsable no es controlado en la aplicación de esta base.

Sin embargo, el interés legítimo se basa en la obligación de realizar una evaluación y ponderación previa, que es una labor dura y tediosa que debe quedar por escrito, siendo susceptible de control por las autoridades o tribunales. Esto eleva el umbral de responsabilidad y exige que sea el responsable del tratamiento quien deba demostrar que tuvo en cuenta los intereses y derechos de los interesados, y que actuó en consonancia. Además, se alinea con el principio de responsabilidad proactiva en el sentido de que aquél que trate los datos debe hacerse responsable de las consecuencias que genere. De este modo, desplaza la responsabilidad del interesado -donde la depositaba el consentimiento-, y la vuelve a situar sobre el responsable, restableciendo el equilibro entre aquellos que deseen tratar datos personales y aquellos cuyos datos son tratados.

Por otro lado, la percepción de que el interés legítimo daría lugar a otros incumplimientos asociados no parece cierta. Independientemente de la base de licitud elegida, el responsable debe cumplir con todos los principios y obligaciones del RGPD, desde la limitación de la finalidad, la minimización de datos o la limitación del plazo de conservación o proporcionar información transparente.

El Reglamento pretende favorecer la armonización interpretativa. Para ello, los Estados miembros deben estar abiertos a acercar posturas sobre el interés legítimo

En quinto lugar, conceptos abiertos como el de interés legítimo y su evaluación crean riesgos de fragmentación interpretativa en diferentes Estados miembros. Por ejemplo, respecto a Estados miembros más abiertos a aplicar el interés legítimo como base jurídica para el tratamiento de datos en relación con la utilización de tecnologías big data o la realización de actividades como, por ejemplo, elaboración de perfiles. No se trata de una crítica únicamente contra el art. 6.1.f) RGPD.

Sin embargo, el hecho de que el instrumento jurídico del RGPD sea la figura de un Reglamento obliga a los Estados miembros a alcanzar una mayor armonización. Por ello, es razonable argumentar que España debe hacer un esfuerzo por no anclarse en una postura férrea. Todo ello no obsta, sin embargo, para que un Estado miembro no pueda ejercer un cierto margen de actuación o intervención mediante su Derecho nacional -eso sí, significativamente más restringido que en el caso de transposición de una Directiva-.

En cualquier caso, es posiblemente pronto para poder anticipar las consecuencias de este escenario. De producirse un cambio de postura en la autoridad de control española o incluso entre los profesionales de la protección de datos, este necesita tiempo. Como último resorte, la jurisprudencia del TJUE puede resultar en pautas a través de las cuales las opiniones de diferentes Estados miembros se armonicen, aunque esta vía toma años y por tanto no es capaz de generar respuestas inmediatas a los retos actuales. Entre tanto, las directrices del Comité Europeo de Protección de datos, los códigos de conducta o las guías de buenas prácticas pueden servir de salvoconducto.

Límites del interés legítimo: posible parcialidad del responsable, falta de ciertas obligaciones de transparencia y derecho de oposición obscuro

A pesar de los factores favorables del art. 6.1.f) y de aquellas críticas mostradas en las líneas anteriores que pueden ser contestadas, nuestro análisis ha revelado algunas cuestiones o limitaciones que quedan abiertas bajo la literalidad del RGPD.

En primer lugar, es cierto que la ponderación de intereses mantiene un riesgo de parcialidad del responsable, que decide en primera instancia sobre el resultado, aunque pueda ser controlado posteriormente. En segundo lugar, el responsable no está obligado a publicar o ejercer transparencia respecto de la ponderación de intereses, dificultando la comprensión del interesado del tratamiento y dificultando la elaboración de argumentos para ejercitar su derecho de oposición. En tercer lugar, el ejercicio del derecho de oposición es susceptible de ser complejo de ejercitar para el interesado o desatendido por el responsable. El responsable mantiene un margen para no conceder el derecho por motivos imperiosos, y puede aprovechar el desconocimiento y complejidad del entorno tecnológico y del tratamiento para actuar de forma desleal y no garantizar los derechos del interesado. Únicamente aquellos interesados más motivados o con mayor conocimiento iniciarán una vía administrativa o judicial contra estas prácticas.

Presentación de guía de buenas prácticas de uso del interés legítimo en entornos big data

Por todo lo visto, puede concluirse que el recurso al art. 6.1.f) RGPD como base jurídica para legitimar el tratamiento de datos personales en relación con el uso de tecnologías de tratamiento masivo de datos debe ser considerado como una opción de peso. Aplicada con las debidas garantías, esta base es capaz de mantener la capacidad de control de los interesados sobre sus datos, pues estos mantienen un derecho de oposición cuyo

rechazo debe ser fuertemente fundado por el responsable. En un intento de suplir las limitaciones abiertas ya señaladas, así como de orientar en la consideración de garantías adecuadas y en factores de evaluación del interés legítimo, incluimos como Anexo I una guía de buenas prácticas de interés legítimo para entornos de tratamiento de datos masivos. En ella se proponen medidas como la publicación de la evaluación de interés legítimo, la concesión de un derecho de *opt-out* previo al tratamiento o un derecho de oposición prevalente por defecto.

Otros derechos del RGPD muestran síntomas de ser poco efectivos, debidos a cuestiones técnicas, interpretativas o compromisos políticos

Tras analizar el art. 6.1.f) RGPD y el derecho de oposición (art. 21), nuestro estudio se centró en la relación de esta base con otros derechos que hemos considerado de importancia capital, pues el avance técnico supone en ocasiones un reto para el correcto ejercicio de estos derechos. En concreto, hemos analizado algunas de las implicaciones de los derechos de portabilidad (art. 20), acceso (art. 15), el derecho a no ser objeto de decisiones automatizadas (art. 22) y los derechos de información (art. 13-14), así como la relación entre todos ello; siempre en el contexto específico de tratamientos de datos personales basados en la utilización de tecnologías de datos masivos.

Nuestras conclusiones en este sentido han sido bastante desalentadoras. Por un lado, existen cuestiones puramente técnicas por las que un derecho pueda no ser efectivo, como la falta de interoperabilidad de sistemas, que dificulta el derecho de portabilidad.

Por otro lado, la interpretación de ciertos conceptos puede provocar una limitación en el ejercicio de los derechos. Por ejemplo, el derecho de acceso puede limitarse cuando el responsable trate una “gran cantidad de información” (art. 15), exigiendo que el interesado concrete sobre qué datos desea el acceso. También, el individuo debe recibir conforme a los arts. art.

13,14,15, información “significativa” sobre la lógica que rige las decisiones plenamente automatizadas definidas en el art. 22. La interpretación de los múltiples conceptos puede conllevar desde un alto grado de protección hasta una dificultad de los interesados de conocer siquiera que se están tomando decisiones automatizadas, su funcionamiento o las garantías que pueden ejercer.

Además, algunas limitaciones a estos derechos parecen deberse a acuerdos o compromisos durante la elaboración de la norma, más que a motivos puramente jurídicos. Por ejemplo, la norma no permite el ejercicio de ciertos derechos cuando el tratamiento se basa en el interés legítimo, como el derecho de portabilidad o de oposición a la toma de decisiones automatizadas.

Los problemas de estos derechos se acentúan cuando se observan de forma conjunta

El análisis de la interrelación de estos derechos es donde se muestran las preocupaciones más profundas. Por ejemplo, si el responsable argumenta que no lleva a cabo tratamientos únicamente automatizados, sobre la base de la interpretación del poco claro art. 22, no tiene obligación de informar sobre la lógica aplicada. En este caso, el tratamiento puede basarse en el interés legítimo, lo que aumentaría el nivel de responsabilidad, y le obligaría a crear garantías suficientes, aunque el interesado sigue sin tener derecho a ser informado de la lógica algorítmica y no es consciente de la intrusividad del tratamiento. Todo ello en un momento en que el uso de decisiones parcial o totalmente automatizadas es continuo. Sin esta información, el interesado está en una posición muy débil para ejercer un derecho de acceso, pues si se tratan grandes cantidades de datos el interesado debe concretar qué datos desea. Esto por su parte dificulta el ejercicio de su derecho de portabilidad. Por su parte, el tipo de datos que se pueden adquirir a través del derecho de portabilidad y su formato es también limitado.

Así, el interesado medio tiene, no solo dificultad para comprender los efectos tratamiento, sino incluso para conocer que dicho tratamiento existe y detectar cuándo sus derechos pueden estar siendo infringidos. Para ello, la labor del delegado de protección de datos, la autoridad de control y, en última instancia los tribunales, será de gran importancia.

Se crea una cadena de lagunas que perpetúan las asimetrías de información o "efecto Gruyere"

En consecuencia, se da una cadena de incongruencias y lagunas y que terminan por crear graves deficiencias en el sistema de derechos de los interesados y ayuda a perpetuar un ecosistema asimétrico. Es lo que hemos bautizado como "efecto Gruyere", pues crea vacíos en la norma que diluyen la protección del individuo. Estos aspectos han sido también tenidos en cuenta en la guía de interés legítimo del Anexo I.

Propuesta de solución: división del proceso en fases con diferentes bases de licitud

Con la visión de todas las consideraciones anteriores, nuestra propuesta consistía en considerar una base de licitud diferente para cada momento del ciclo de vida de un proyecto de tratamiento masivo de datos. Así, en la Fase 1- Recolección, que consiste en la recogida y preparación de datos, pueden existir diferentes bases de licitud en función de la circunstancia. La Fase 2- Análisis, conlleva explorar correlaciones, patrones y elaborar modelos algorítmicos en un entorno de pruebas con medidas técnicas de protección. En esta, el interés legítimo tiene un encaje perfecto. Por último, la Fase 3- Aplicación consiste en aplicar el modelo ya creado sobre una persona en concreto y tomar decisiones sobre ella. Para esta fase, el consentimiento podrá ser, de nuevo, una base de licitud adecuada. Ello porque en la Fase 2 el responsable tiene la oportunidad de crear conocimiento, hacer pruebas y anticipar consecuencias, y todo este conocimiento puede ser transmitido de forma transparente al usuario.

Necesitamos una visión colectiva de la protección de datos que trascienda la individualidad. La mayor adopción del interés legítimo puede servir a estar fin, pero es solo la punta del iceberg

Por último, retornamos a la que fue una de nuestras primeras conclusiones: el hecho de que los mayores riesgos del tratamiento masivo de datos se manifiestan a nivel colectivo, en la capacidad de conocer y orientar el comportamiento de una masa de personas. Por este motivo, el derecho de protección de datos se beneficiaría de una evolución por la que no solo se tuviera en cuenta a la persona desde una perspectiva individualista, sino que adquiriese una visión colectiva.

En relación con ello, la base de licitud es únicamente una muestra de este riesgo. El consentimiento es una base eminentemente individualista (pues la persona otorga o deniega su consentimiento normalmente atendiendo a factores que le afectan a sí misma). Por su parte, el interés legítimo permite que el responsable deba considerar los efectos colectivos del tratamiento y establecer garantías de protección.

En la actualidad, parece apreciarse una quiebra en la confianza en el sistema digital y en nuestra opinión, el RGPD -y más concretamente el interés legítimo- tiene el potencial para repararla.

El interés legítimo debe ser tomado con la mente abierta, no como una puerta abierta a todo

En conclusión, nos encontramos ante una realidad acelerada y diversa que requiere de soluciones flexibles para no paralizar el funcionamiento del sistema.

En los capítulos anteriores hemos argumentado que el art. 6.1.f) RGPD es una base de legitimación alineada con el espíritu del nuevo Reglamento que la hace viable específicamente en tratamientos que utilicen tecnologías de tratamiento masivo de datos.

En esencia, el interés legítimo debe ser considerado con la mente abierta, pero no como una puerta abierta a cualquier tipo de tratamiento.

"*Estoy tratando de liberar tu mente, Neo. Pero solo puedo mostrarte la puerta. Tú eres el que tienes que atravesarla*".[574]

[574] Película Matrix, 1999.

ANEXO I. BUENAS PRÁCTICAS PARA LA APLICACIÓN DEL INTERÉS LEGÍTIMO

Una visión de conjunto sobre cómo funciona el título de legitimación del art. 6.1.f) RGPD nos ha permitido identificar algunos de sus puntos fuertes, en especial aquellos que solucionan las principales limitaciones de otras bases como el consentimiento del interesado. Sin embargo, también han quedado detectados determinados aspectos que pudieran dar lugar a consecuencias negativas para los interesados.

Al efecto conjunto de estas consecuencias negativas nos hemos referido como “efecto Gruyere” en el sentido de que se asemejan a vacíos en la norma cuyo resultado conjunto es potencialmente muy lesivo.

Teniendo en cuenta el análisis realizado en las páginas y capítulos anteriores, así como la falta de directrices amplias sobre el interés legítimo, proponemos un conjunto de recomendaciones de buenas prácticas para orientar por aquellos responsables que lleven a cabo los tipos de tratamientos a los que nos hemos referido como big data sobre la base de su interés legítimo a la luz del RGPD. Estas directrices pretenden servir de guía para la aplicación del art. 6.1.f) RGPD en aras a la solución de las limitaciones identificadas, y tomando como principal ventaja la flexibilidad de la figura del interés legítimo.

Las directrices han sido elaboradas sobre la base del estudio previo y las conclusiones de este trabajo que, no obstante, no poseen un carácter completo. Por tanto, deberán ser ampliadas convenientemente para reflejar de manera más precisa aspectos que han quedado fuera del ámbito de estudio de este trabajo tales como posibles transferencias internacionales, la conservación de los datos, la utilización de categorías especiales de datos o la aplicación de diversos principios como el de exactitud de los datos, así como derechos tales como el de supresión o rectificación. Por otro lado, ciertas cuestiones, tales como lo relativo al derecho a no ser objeto de toma de decisiones automatizadas, están tratadas, pero sin intención de constituir unas directrices completas, pues el análisis profundo

de la gran complejidad del tema y su extensión no son el objeto principal de este trabajo.

Asimismo, dadas las diversas aplicaciones de tecnologías de datos masivos en sectores específicos de actividad, cabe resaltar que estas directrices tienen un carácter genérico.

Guía de buenas prácticas para la aplicación del interés legítimo como base de tratamientos a través de tecnologías big data

- Esta base de licitud requiere lo que se ha establecido como una **evaluación en tres fases, que debe realizarse caso por caso**. En primer lugar, debe existir un interés del responsable del tratamiento o de un tercero, que deberá ser legítimo. En segundo lugar, debe superarse un juicio de necesidad. En tercer lugar, debe realizarse un balance de intereses o juicio de ponderación que ponga en un lado de la balanza los intereses legítimos del responsable del tratamiento o de un tercero y en el otro los intereses, derechos y libertades de los interesados.
- **Como paso previo, y de modo informal, el responsable puede hacer a modo de autoevaluación un "test de confianza"**. Con ello, se busca identificar si el responsable se sentiría cómodo o seguro revelando de forma transparente cuáles son las finalidades del tratamiento, sus intereses, los datos que se tratarán y las consecuencias o repercusiones. Si un ejercicio sincero de transparencia pudiera crear incomodidad o vergüenza al responsable, es probable que el interés legítimo no sea la base de licitud más apropiada. Esta no puede ser una base de legitimación de tratamientos obscuros que de otro modo no podrían ser lícitos.
- En aras de la seguridad jurídica, el responsable debe tomar en consideración en qué medida las autoridades de protección de datos se muestran conformes con el uso del interés legítimo como base de licitud

para tratamientos de datos masivos con técnicas intensivas y complejas.

- El responsable debe ser consciente de que, en la mayoría de las ocasiones, **el art. 6.1.f) RGPD -interés legítimo- conlleva intrínsecamente una labor más tediosa, ardua, larga y necesitada de recursos que otras**. También puede ser estar más expuesta a un criterio discordante por parte de la autoridad de control. Por este motivo, el responsable no debe acudir a este precepto salvo que pueda demostrar de manera sólida que cumple cada uno de sus requisitos.
- El uso del interés legítimo como base del tratamiento conlleva vestir con un grado extraordinario de responsabilidad a quien realice el tratamiento, que debe mostrar un **"sentimiento ético"**, y no la mera intención de cubrir un requisito mínimo legal.
- **El principio de responsabilidad proactiva** en relación con el interés legítimo puede interpretarse en el sentido de que **eleva el umbral de responsabilidad** del responsable del tratamiento para demostrar la existencia de dicho interés legítimo y su validez como base del tratamiento.[575]
- **El responsable ostenta la carga de la prueba de que el interesado medio razonable ha podido adquirir un nivel razonable de comprensión**, entre otros, sobre el tratamiento, qué datos serán tratados o los posibles riesgos para el interesado.
- A pesar de lo obvio de esta afirmación, cabe recordar que el responsable tiene la **obligación de respetar todos los principios relativos al tratamiento de datos**, sea cual sea la base jurídica. Así, cuando la base de licitud del tratamiento sea el interés legítimo, el responsable debe atenerse a estos principios, entre los que cobran

[575] De modo similar, en respeto al principio general del Derecho "*ubi commodum, ibi et periculum*", cuando el desarrollo de la tecnología incrementa el riesgo de una actividad, el máximo beneficiado debe responder de dichos riesgos.

especial relevancia aquellos de limitación de la finalidad, minimización de datos o limitación del plazo de conservación.

- **Descentralizar la tarea de la realización del ejercicio de ponderación puede añadir objetividad e independencia a la evaluación de interés legítimo**. Así por ejemplo, el responsable puede tener asignada la labor de identificar cuál es el interés legítimo que pretende satisfacer el tratamiento, concretar las circunstancias del tratamiento así como las posibles repercusiones detectadas para el interesado. Una persona diferente del responsable, por ejemplo, un Delegado de Protección de Datos, podría asumir la labor de llevar a cabo la ponderación de intereses y pronunciarse sobre su resultado. Aun cuando la decisión final y la responsabilidad recaigan sobre el responsable, la evaluación ganaría en independencia.

  Según este enfoque, el responsable (que puede ser, por ejemplo, el jefe del Departamento Comercial de una organización o el jefe del proyecto) argumentaría cuáles son los intereses y por qué pueden considerarse legítimos. Por otra parte, todos los agentes que participen en el proyecto tendrían que informar sobre los posibles riesgos para los intereses y derechos de los interesados. Esto puede incluir, no sólo al responsable del tratamiento, sino también a otras personas o equipos que desempeñan funciones auxiliares, como el Departamento Jurídico, el Departamento de Tecnología de la Información, el responsable de la seguridad de la información o un comité de ética. Por último, correspondería al Delegado de Protección de Datos (en caso de que exista) examinar todos los argumentos, aportar sus criterios adicionales y adoptar una conclusión. En caso de que no haya un DPO dentro de la organización, nuestra recomendación es elegir a una persona con suficiente experiencia e independencia para ejecutar esta tarea. El responsable podrá desviarse de las conclusiones del DPO, pero deberá documentar sus motivaciones.

- **La realización de una evaluación de impacto** puede servir de base y aportar luz sobre qué base de legitimación es la más apropiada.
- Para que la aplicación del interés legítimo en operaciones complejas garantice la protección del interesado, en necesario **tomar en cuenta otras posibles limitaciones de la normativa de protección de datos**. La transparencia y explicabilidad algorítmicas son aspectos especialmente relevantes.

DETERMINAR CUÁL ES EL INTERÉS LEGÍTIMO

- El interés es el valor u objetivo general que el responsable del tratamiento desea cumplir a partir de la actividad de tratamiento. Debe ser real, presente -es decir, no meramente especulativo-, y suficientemente específico y articulado. Puede tratarse de un interés individual, de un tercero o socialmente amplio.
- Dicho interés debe ser legítimo, esto es, que no contradiga las normas jurídicas, comunitarias o nacionales (de mayor o menor rango, incluso la jurisprudencia) ni los valores sociales predominantes. Puede tratarse de cualquier bien jurídico reconocido como tal por un sistema, ya sea este económico, legal, de hecho, o moral, aunque no es necesario que exista una habilitación legal expresa que defienda ese interés.
- **El responsable no debe utilizar fórmulas ambiguas que no permitan identificar cuál es el interés buscado**. Ejemplo de este tipo de fórmulas son: Tratamos tus datos sobre la base de nuestros intereses legítimos, “que incluyen x,y,z” o “podemos tratar tus datos, por ejemplo, para nuestro interés legítimo”. Estás fórmulas crean situaciones en las que el interesado no puede identificar claramente cuál es la base de licitud o cuáles son los intereses supuestamente perseguidos. Esto dificulta o impide ejercer su capacidad de control o determinar si le amparan derechos como el de oposición.
- Bien es cierto que, en ocasiones, la redacción y la delimitación exacta de las finalidades del tratamiento podrán no ser sencillas. Ello no obsta

para que el responsable no realice un ejercicio sincero de transparencia que concluya con un nivel de determinación, al menos, adecuado para hacer saber a los interesados sobre qué tratamientos pueden ejercer derechos tales como el de oposición.

- El responsable debe ser capaz de **vincular cada actividad de tratamiento con una base de licitud correspondiente**. Prácticas como indicar en un apartado de la política de privacidad un conjunto de finalidades de tratamiento e intereses y por otro lado un compendio de bases de licitud utilizadas por el responsable no permite que el interesado conozca qué base legitima qué tratamiento.

  Tampoco es válida una redacción que pueda dar a entender que una misma finalidad queda vinculada a dos bases de licitud diferentes. Por ejemplo, si llevas a cabo determinadas funciones de personalización del servicio basadas en interés legítimo y otras basadas en el consentimiento, el responsable debe poder identificar qué funciones de personalización corresponden a cada base.

- **Cuando un tercero comunique al responsable la concurrencia de su interés legítimo** con el fin de que el responsable lleve a cabo un tratamiento, el responsable debe solicitar de dicho tercero toda la información necesaria que le permita valorar la existencia del interés legítimo, así como llevar a cabo un juicio de necesidad y la ponderación de intereses.

- El interés legítimo **debe existir y ser actual en el momento del tratamiento de los datos, y no futuro o simplemente hipotético**. Para ello, el responsable debe evaluar de forma periódica este factor.

- **Algunos ejemplos de intereses legítimos** mencionados en la Opinión sobre interés legítimo del extinto Grupo de Trabajo del Artículo 29, en las normas de protección de datos, o por la jurisprudencia son:

  ✓ Mercadotecnia directa por medio postal (GT29, considerando 47 RGPD).

- ✓ Prevención del fraude o de blanqueo de capitales intragrupo o entre compañías ajenas al grupo (GT29, considerando 47 RGPD y Consulta de la banca a la AEPD sobre interés legítimo).
- ✓ Transmisión de datos personales entre un grupo de organizaciones con fines administrativos internos -por ejemplo, para el tratamiento de datos de los empleados- (considerando 48 RGPD).
- ✓ Seguridad de las redes y de las tecnologías de la información (GT29, considerando 49 RGPD y TJUE-asunto Breyer).
- ✓ Indicación por parte del responsable del tratamiento de posibles actos delictivos o amenazas hacia la seguridad pública, junto con la transmisión de los datos personales pertinentes a una autoridad competente (considerando 50 RGPD).
- ✓ Acceso a datos de una persona por parte de un tercero para el inicio de acciones legales contra ella (GT29, asunto Rigas).
- ✓ Supervisión o monitorización de empleados con fines de seguridad o gestión (GT29).
- ✓ Protección de los bienes, la salud y la vida del responsable o los de su familia, que se derivan de la protección de un derecho fundamental como el derecho de propiedad y de la vida familiar (TJUE-asunto Rynes).
- ✓ Interés de tercero -la sociedad- de acceder a determinada información transparente como los sueldos de cargos gubernamentales o el destino de fondos públicos.
- ✓ Interés de terceros -la sociedad- de acceder a un registro público que contiene datos personales y societarios para garantizar seguridad jurídica (TJUE-asunto Manni).
- ✓ Interés de terceros -sujetos de derecho privado- de acceder a información o documentos (disposición adicional 10ª LOPDgdd).
- ✓ Incrementar la eficacia publicitaria a través de la creación de perfiles (TJUE-asunto Fashion ID).
- ✓ Sistemas de denuncia interna o *whistleblowing* (GT29).

- ✓ Intereses legítimos de las administraciones públicas cuando actúan fuera del ámbito de sus actividades (TJUE-asunto Breyer y art. 6.1.f) RGPD).
- ✓ Procesos de anonimización de datos (Fase 1-Recogida y preparación). (Consulta de la banca a la AEPD sobre interés legítimo).
- ✓ Procesos de seudonimización de datos, con garantías (Fase 1-recogida y preparación). (Consulta de la banca a la AEPD sobre interés legítimo).
- ✓ Actividades de perfilado básico de clientes (Fase 3) para el envío de comunicaciones comerciales a partir únicamente de información proveniente de la entidad -sin enriquecimiento con fuentes de datos externas- (Consulta de la banca a la AEPD sobre interés legítimo).
- ✓ Tratamiento de datos de contacto profesionales (art. 19 LOPDgdd-presunción *iuris tantum* de prevalencia de interés legítimo).
- ✓ Tratamiento de datos en relación con sistemas de información crediticia o ficheros de morosos, con garantías específicas (art. 20 LOPDgdd- presunción *iuris tantum* de prevalencia de interés legítimo).
- ✓ Tratamientos relacionados con determinadas operaciones mercantiles, como fusión o adquisición de una compañía o en procesos de *due diligence* (art. 21 LOPDgdd- presunción *iuris tantum* de prevalencia de interés legítimo).
- ✓ Protección de la propiedad intelectual, secretos comerciales o *know* how del responsable.

- **Algunos ejemplos de intereses legítimos que son susceptibles de necesitar mayor especificación o justificación de que cumplen los requisitos para ser válidos**:
  - ✘ Prestar un servicio innovador y personalizado.
  - ✘ Analizar el comportamiento de los usuarios para mejorar ofertas.
  - ✘ Mejorar el servicio.
  - ✘ Comercializar nuevas funciones.

EL CONCEPTO DE NECESIDAD

- Para evaluar la necesidad, debe tenerse en cuenta si el responsable del tratamiento puede **lograr razonablemente el mismo objetivo sin dicho tratamiento o por medios menos intrusivos**, equilibrando la proporcionalidad entre el tratamiento y la finalidad.
- **Concepto intermedio** que no requiere ser absolutamente **indispensable**, pero tampoco tan básico como solo deseable o **útil**. Por ejemplo, si existe otra manera de perseguir el mismo objetivo, pero esta requiere un esfuerzo desproporcionado, entonces el tratamiento tal como se concibe puede considerarse necesario.
- Ese concepto de necesidad ¿cumple con los principios del art. 5 RGPD, y en especial, aquellos de licitud, lealtad, minimización o calidad de los datos?

EL EJERCICIO DE PONDERACIÓN DE INTERESES

- La necesidad de llevar a cabo y documentar la realización de la ponderación de intereses es lo que distingue el art. 6.1.f) del resto de bases y **donde reside el potencial** de aportar un grado cualitativamente superior en la protección de los individuos y de flexibilidad para los responsables.
- **Debe ser valorado caso por caso**, sin que sea posible prescribir el resultado final de la ponderación. Es decir, el responsable no podrá argumentar que una ley nacional o precedentes anteriores analizados por la autoridad de control le permiten con carácter definitivo alegar su interés legítimo en el caso concreto.
- Este ejercicio de ponderación puede ser visto como una **evaluación de impacto simplificada**.
- El lado de la balanza contrario al interés legítimo del responsable o un tercero es el de los **intereses, derechos y libertades del interesado**. El responsable debe hacer un ejercicio diligente y sincero para detectar y medir los intereses, derechos y libertades del interesado medio, una

labor a la que normalmente está menos acostumbrado que a la detección y medición de intereses propios.

- **La ponderación debe tener pretensión de ser objetivable**, aunque parece inevitable que conlleve un cierto grado de parcialidad por parte del responsable. El responsable no debe utilizar su grado de subjetividad para dar un resultado falaz al balance de intereses.
- En la ponderación, la atención se centra sobre las **circunstancias específicas del tratamiento** tal y como el responsable es capaz de conocerlas **en relación con el interesado medio razonable**. El responsable no ostenta la obligación de prever los factores que afectan a las circunstancias específicas de cada interesado.
- **Factores**. Algunos elementos de ponderación afectarán con especial intensidad a fases concretas del tratamiento, mientras que otros tienen un carácter más transversal.
    - La naturaleza de los intereses de ambas partes. Se trata de un concepto amplio que abarca aspectos como los tipos de datos, si los intereses añaden un valor a los interesados o la sociedad, y no únicamente al responsable o un tercero, o prácticas que se inscriban en cuestiones aceptadas socialmente y que gocen de amplio reconocimiento y comprensión.
    - Riesgo de reidentificación de datos anonimizados.
    - Tratamiento de datos esporádico o continuo.
    - Existencia de prácticas intrusivas tales como el seguimiento a través de múltiples sitios web, dispositivos o localizaciones.
    - **Factores especialmente relevantes en la Fase 1-Recogida**:
        - La fuente de los datos. Los datos obtenidos de terceros pueden tener mayores implicaciones para los derechos del interesado que aquellos otros obtenidos de manera directa por el responsable en su relación con el interesado.

- La publicidad de los datos.
- Adquisición de datos directamente del interesado o a través de terceros. ¿En su caso, es posible obtener una prueba de que los interesados fueron informados y la cesión cuenta con base de legitimación?
- Si se recogen datos de terceros o de fuentes externas, la cantidad de fuentes terceras están nutriendo las bases de datos del responsable. En la cara opuesta de la monera, el número de destinatarios posibles, por ejemplo, la cesión de datos a un número amplio de terceros.
- Respeto a, entre otros, el principio de minimización de datos.

- **Factores especialmente relevantes en la Fase 2-Análisis**:
  - La utilización de medios automatizados y, en concreto, la capacidad tecnológica del responsable para llevar a cabo procesos de analítica de datos.
  - Existencia de tratamiento secundario de datos. ¿En ese caso, es posible argumentar que las finalidades son compatibles?
  - El volumen de los datos tratados: el tratamiento de cantidades masivas de datos personales o datos referidos a un número elevado de interesados.
  - Cuando se utilicen tecnologías big data es relevante recordar que las consecuencias más perjudiciales de los tratamientos nocivos de datos personales son más visibles a gran escala. El responsable debe tener en cuenta que el impacto colectivo es además superior y de diferente naturaleza a la suma de los impactos negativos individuales que el tratamiento causa sobre cada persona.
- **Factores especialmente relevantes en la Fase 3-Aplicación**:

- El responsable debe identificar si lleva a cabo toma de decisiones automatizadas o creación de perfiles del art. 22 RGPD, en cuyo caso, no podrá acudir al interés legítimo como base.
- Posibilidad de obtener nueva información de una persona a través de medios deductivos o inferencias.
- La dificultad de anticipar las consecuencias del tratamiento para los interesados.
- Nivel de detalle de los perfiles creados (general o detallado), exhaustividad del perfil (si permite describir un solo aspecto concreto de la persona o múltiples aspectos, de modo que puede crearse una imagen más completa del interesado).
- Implementación de medidas destinadas a garantizar que los datos, incluidos aquellos obtenidos por inferencia o perfilado, son veraces y actuales.

- **¿Quién es el interesado medio razonable?**
  - Si se trata de un grupo específico de población con características singulares, deben tomarse en cuenta.
  - El RGPD llama a prestar cuidado al hecho de que el interesado sea un niño.
  - Por analogía, otros grupos de población también deben recibir especial consideración: grupos de población sensible, vulnerables o con poca madurez tecnológica, tales como personas con discapacidad, personas de tercera edad, con escasos recursos o de bajo nivel educativo.
- **Expectativa razonable**:
  - Existencia de una relación previa responsable-interesado (por ejemplo, proveedor-cliente).

- El interesado medio razonable, ¿puede prever de forma plausible, que los datos objeto de tratamiento van a ser recogidos en el momento y contexto de la recogida, y pueden tener una expectativa razonable de que serán tratados para la finalidad a que se destinen?
- La transparencia aumenta la expectativa razonable del interesado. En todo caso, la información o la existencia de dicha expectativa razonable no justifica por sí sola que el resultado de la ponderación sea favorable al interés legítimo del responsable.
- La expectativa razonable del interesado es un factor dinámico que puede modificarse, por ejemplo, por la mayor adopción tecnológica en la sociedad. Por prudencia, nuestra recomendación es que este factor no debe sobre-enfatizarse.

- Si la ponderación de intereses arroja un resultado contrario al tratamiento, el responsable puede tomarlo como **resultado provisional**, adoptar nuevas medidas y garantías, y repetir la ponderación.
- **Impacto sobre el interesado y medidas de salvaguarda**:
  - El impacto del tratamiento puede ser uno de los factores más determinantes en la evaluación del interés legítimo.
  - Las medidas de salvaguarda aplicadas por el responsable del tratamiento (por ejemplo, para evitar la discriminación, la imparcialidad o la exactitud).
  - El RGPD no exige que el impacto sea nulo o inexistente, pero sí debe ser minimizado y justificado.
- **La implementación y debida descripción documental de las medidas de seguridad** de la organización ayudarán a crear un factor de ponderación en favor del interés legítimo del responsable.

- **Imposición de un requisito especialmente elevado en materia de garantías adecuadas de salvaguarda y de medidas de seguridad de la información** para reducir el posible riesgo remanente pueden ser determinantes para impulsar la balanza en uno u otro sentido. En concreto, sobre las medidas de seguridad:
    - Pueden consistir, entre otras, en: minimización de datos, seudonimización, anonimización, aumentar los niveles de transparencia, estándares de privacidad desde el diseño y por defecto, métodos de autenticación por factores múltiples, estricta concesión de derechos de acceso para reducir a lo rigurosamente necesario quiénes pueden acceder a la información dentro de la organización, reducción de plazos de conservación de datos, cifrado, etc. Establecimiento de medios sencillos de manifestar oposición al tratamiento, limitar el tratamiento de datos en la Fase 2-Análisis, que es el momento que desencadena el proceso técnico que posteriormente hará posible la combinación de datos y el descubrimiento de patrones. Limitación de las decisiones y aplicaciones que se desarrollen durante la Fase 3-aplicación.
    - Mantenimiento de las medidas de acuerdo con el estado del arte, especialmente cuando se utilizan tecnologías de datos masivos.
    - La determinación de las medidas de seguridad que deben recaer sobre el tratamiento es también un proceso dinámico.
    - Aunque la ponderación de intereses concluya a favor del tratamiento, el responsable siempre debe adoptar medidas paliativas dirigidas a minimizar el impacto sobre los derechos e intereses del interesado.
    - **Auditorías periódicas del set de datos de prueba, así como del modelo algorítmico o diferentes etapas del ciclo de vida del dato**, bien por parte de expertos independientes,

bien por parte de las autoridades de control. Estas auditorías tienen diferentes finalidades, como por ejemplo:

- Comprobar que las inferencias y decisiones tomadas sobre la base del uso de dicho modelo algorítmico se basen en datos fidedignos y de calidad, mejorando así la tasa de veracidad del conocimiento inferido, en cumplimiento del principio de exactitud de los datos.
- Prevenir la discriminación: para detectar y corregir posibles sesgos, tales como la existencia de parámetros directamente discriminatorios o la posibilidad de que ciertos factores actúen de variables proxy y sean encubiertamente discriminatorias.

LABOR DOCUMENTAL

- La obligación de realizar una ponderación de intereses y documentarlo es el paso que aporta un mayor grado de garantía al interesado cuando la base de licitud es el interés legítimo respecto de las demás bases.
- **Los tratamientos de datos con tecnologías big data exigirán de un alto nivel de detalle en la demostración de la existencia de la legitimidad del responsable del tratamiento**. Por ejemplo: la transparencia en torno a cómo se hizo la ponderación de los intereses, su proceso de revisión en el tiempo, evaluar cómo se han tenido en cuenta y ponderado los riesgos y los efectos negativos.
- La organización que lleva a cabo un tratamiento de datos basado en intereses legítimos debe **mantener actualizada su evaluación de interés legítimo como forma de justificación *ex ante***. Esto debe hacerse con especial énfasis en el equilibrio de intereses, que podría cambiar debido a nuevas circunstancias, como el tratamiento de nuevos datos, la inferencia de nuevos datos (o categorías de los mismos), la observación de nuevos riesgos o la constatación de que algunas consecuencias no se midieron en primer lugar. La documentación de

evaluación podrá ser revisada *a posteriori*, por ejemplo por la autoridad de control, de modo que el responsable queda vinculado a sus conclusiones.

- **Un alto grado de detalle en la documentación** generada aportará evidencias al responsable para poder demostrar la solidez con que fue realizado la ponderación de intereses, que se tomaron en cuenta todos los posibles intereses, derechos, libertades y riesgos de cada una de las partes involucradas, y que su contraposición se llevó a cabo con criterios de licitud, responsabilidad proactiva y ética.
- En el contexto de uso de tecnologías de datos masivos, la complejidad del proceso puede conllevar que el contenido de la evaluación del interés legítimo se asimile más a aquel de una evaluación de impacto. Sea como fuere, ambos documentos -la evaluación de impacto de protección de datos y la evaluación de interés legítimo- **deben tener intención real de detectar y mitigar riesgos, y no ser un mero documento de cumplimiento normativo** vacío de significado.
- Además, el registro de actividades de tratamiento es un documento que puede servir de base y ayuda para el responsable que necesite trazar un mapa del ciclo de vida de los datos de la organización para la posterior realización de una evaluación de interés legítimo.
- **La documentación detallada del proceso de creación de la evaluación del interés legítimo**, incluida la asignación de las funciones y responsabilidades, es pertinente. Por lo tanto, aconsejamos una ilustración documental exhaustiva de las discusiones, argumentos y factores que ayudaron a inclinar la balanza de una manera u otra. Esto puede constituir una prueba crucial para el responsable o la organización en caso de que las autoridades de control examinen más a fondo la documentación, así como una prueba del cumplimiento de los principios de lealtad (art. 5.1.a) y responsabilidad proactiva (art. 5.2). Asimismo, **el documento debería permitir determinar cuál fue el camino**

argumentativo por el que se concluyó que el interés legítimo sería la base de legitimación, y por tanto, ser auditable en un momento posterior.

- **El documento debe mantenerse vivo en el tiempo**. De manera periódica, el responsable debe reevaluar que no han devenido circunstancias que invaliden en resultado del ejercicio de ponderación. Considerar esto como un documento vivo es beneficioso en varias circunstancias, por ejemplo:
    - Durante una investigación de las autoridades de protección de datos, a fin de demostrar que se han evaluado y medido todos los factores pertinentes para garantizar los intereses, derechos y libertades de los interesados y se han mitigado los riesgos.
    - Durante el curso de un procedimiento judicial ante tribunales nacionales o internacionales que se ocupen de resolver en materia de protección de datos.
    - Durante la evaluación de la aplicabilidad del derecho de oposición.
    - Durante la compra o venta de datos o la cesión de datos a otras empresas de un grupo.
    - Durante un proceso de diligencia debida (*due diligence)* en el curso de la venta de la empresa.
    - Para evitar daños a la reputación en caso de que surja un problema en la opinión pública.
    - Para mantener la seguridad jurídica dentro del propio responsable del tratamiento de datos, para evaluar que, aparte de la base legal del tratamiento de datos personales, se han observado todos los demás principios de la RGPD, como la responsabilidad, la minimización de datos, la equidad o la transparencia.
- **Es recomendable incluir la actualización y revisión de la evaluación del interés legítimo en el flujo de trabajo de las organizaciones**, al mismo nivel que, por ejemplo, el examen y la actualización de las medidas de seguridad. Esto permitiría formalizar la labor, estableciendo

una revisión periódicamente definida. La frecuencia de la revisión debería tener un doble enfoque: i) el documento debe examinarse y actualizarse cada vez que se produzca un cambio en las corrientes de datos o en las prácticas de la organización, y ii) independientemente de ello, el documento debe someterse a un examen cada pocos meses (cuya especificación diferirá en cada caso, pero podría ascender, por ejemplo, a 6 meses o un año).

- Establecimiento de canales de comunicación y recepción de comentarios con colectivos interesados, que podrán ser tomados en cuenta para la actualización del ejercicio de ponderación y la implementación de garantías adicionales.

TRANSPARENCIA

- La transparencia contribuye a reducir el espacio para la falta de expectativas razonables del interesado de que un tratamiento se lleve a cabo en las circunstancias específicas. Por lo tanto, esto aportará beneficios de, al menos, dos maneras: por un lado, la información transparente será un factor motriz que puede ayudar a concluir que el interés legítimo puede ser la base de licitud, mientras que ayudará a demostrar que se cumplieron todos los requisitos legales en caso de que se impugne la decisión. Por otro lado, la transparencia también ayuda al individuo, por ejemplo, a ejercer un control *ex post* contra dicha ponderación de intereses, a cuestionarlo o a expresar su situación particular con vistas a ejercer su derecho de oposición. Asimismo, esta práctica sirve al responsable en el cumplimiento del principio de responsabilidad proactiva.
- El responsable debe, en todo momento, cumplir debidamente su deber de información conforme a los arts. 13 y 14 RGPD. Por ejemplo, conforme a los arts. 13.1.d) y 14.2.b), el responsable debe comunicar al interesado cuáles son los intereses legítimos que persigue él mismo o un tercero.

- Sin embargo, **presentar información completa conforme a los arts. 13 y 14 RGPD no garantiza que el responsable esté cumpliendo con el principio de transparencia**. El responsable debe poner su mejor esfuerzo en que el interesado realmente conozca el alcance del tratamiento, comprenda sus implicaciones y ostente una expectativa razonable de su existencia y alcance. Por ello, los estándares de información y transparencia deben ir más allá de los requisitos de las arts. 13 y 14 RGPD, que se interpretan como un umbral mínimo sobre el que construir otras iniciativas de mayor transparencia.
- **La publicación de la evaluación de interés legítimo**, o al menos, una versión simplificada de ella, que contenga información significativa. Ello podrá ser de gran provecho para los interesados, por ejemplo, a los efectos de poder fundar su ejercicio de derecho de oposición. Aunque esta medida no se desprende directamente de ninguna obligación contenida en el RGPD, se puede ver como una manifestación del principio de transparencia en relación con el de licitud y el de responsabilidad proactiva.[576]
- **Poner a disposición de los interesados los factores más relevantes y el peso otorgado a cada uno durante la ponderación en el proceso de evaluación de interés legítimo**. Esto también contribuiría a proporcionar información transparente a los interesados (de conformidad con el principio de transparencia del art. 5.1.a). Al hacerlo, se debería prestar atención a no revelar información comercial sensible.
- **Informar, en el momento de la recogida de los datos**, siempre que sea posible, sobre **las finalidades secundarias** tales como la analítica de datos para la búsqueda de patrones, correlaciones entre variables y

[576] En este sentido, novedosamente, el Comité Europeo de Protección de Datos, en sus directrices sobre los principios de protección de datos desde el diseño y por defecto, indica que una representación clave del principio de licitud es revelar la evaluación llevada a cabo sobre la ponderación de intereses cuando la base de licitud fuese el interés legítimo. COMITÉ EUROPEO DE PROTECCIÓN DE DATOS (2019): *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default*, p. 15, de 13 de noviembre. Disponible en: https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201904_dataprotection_by_design_and_by_default.pdf.

creación de modelos, la aplicación de ese conocimiento para la realización de perfiles, o el entrenamiento de modelos de aprendizaje automático, etc. Cabe recordar que en caso de que existan decisiones automatizadas en el sentido del art. 22 RGPD, el responsable no podrá acudir al interés legítimo como base.

- **Información sobre qué datos "nuevos" o inferidos son objeto de tratamiento** por parte del responsable, y, en la medida de lo posible, información genérica sobre el proceso analítico a través de los cuales se obtuvieron.
- **Transparencia sobre qué información es compartida con terceros: los datos obtenidos del interesado, aquellos otros observados o perfiles completos**. Especial grado de transparencia en lo que se refiere a las prácticas del responsable relativas a conceder acceso a los datos a terceros destinatarios.

EJERCICIO DE DERECHOS DEL INTERESADO

- Conforme al art. 12, "el responsable del tratamiento facilitará al interesado información relativa a sus actuaciones sobre la base de una solicitud con arreglo a los artículos 15 a 22". Es decir, parece existir una obligación del responsable de adaptar su actividad para poder garantizar el ejercicio de los derechos del interesado y facilitarlo.
- A continuación, se muestra una tabla-resumen sobre qué derechos son de obligado cumplimiento en función de cada base de licitud. Esta guía especificará buenas prácticas en relación con el derecho de acceso, portabilidad, oposición y -parcialmente- el derecho a no ser objeto de decisiones automatizadas.

Derechos de cada base legitimadora RGPD	Arts. 13-14 Información	Art. 15 Acceso	Art. 16 Rectificación	Art. 17 Supresión	Art. 18 Limitación	Art. 20 Portabilidad	Art. 21 Oposición	Art. 22 No decisiones automatizadas
Consentimiento							Retirada consentimiento	Retirada consentimiento
Contrato							x	
Obligación legal				x		x	x	x
Interés vital						x	x	x
Interés público				x		x		x
Interés legítimo						x		x

Derecho de oposición (art. 21 RGPD)

- Existen factores que, por afectar de manera particular a un interesado, no pueden ser tenidos en cuenta por el responsable en la realización de la evaluación de interés legítimo -y más concretamente durante la ponderación de intereses-. Estos factores conforman un "estándar subjetivo", esto es, relativo al interesado concreto.
- El RGPD otorga al interesado un derecho de oposición, para prevenir el inicio del tratamiento o detenerlo.
- El derecho de oposición se refiere a una finalidad del tratamiento específica pero no a los datos personales *per se*, y por tanto no conlleva necesariamente la supresión de los datos personales. Aquellos datos necesarios para otras finalidades, podrán continuar siendo tratados.
- El responsable debe llevar a cabo todas las acciones que le sean posibles para comunicar de manera efectiva a los interesados en qué consiste su derecho de oposición, cómo ejercitarlo y sus implicaciones.
- En todo caso, el responsable debe facilitar al interesado la labor de expresar sus motivaciones individuales para solicitar la oposición al tratamiento.
- El responsable debe actuar conforme al principio de lealtad en su respuesta al ejercicio de derechos por parte de los interesados. En concreto, no podrá utilizar la complejidad que rodea ciertos tratamientos y tecnologías como motivo para aportar justificaciones confusas con las que argumentar la existencia de un interés imperioso por el que se deniegue el derecho de oposición.

- Cuando el tratamiento se base en un interés legítimo propio, como regla general, el responsable deberá detener el tratamiento tras el ejercicio de un derecho de oposición, que debe interpretarse como de naturaleza cuasi-absoluta. Como escenario ideal, el responsable puede conceder el ejercicio de este derecho por defecto, asemejándolo a un medio de exclusión voluntaria y creando así un medio de control y expresión de la voluntad personal.
- Cuando el tratamiento se base en un interés legítimo de tercero, el responsable debe llevar a cabo una labor transparente y completa que justifique adecuadamente su decisión de conceder o denegar el derecho de oposición del interesado.
- En fundadas y reducidas excepciones el responsable podrá continuar con el tratamiento. Entre dichas excepciones, contará con especial relevancia la preservación de los derechos o intereses legítimos de terceros, ya sean estos personas físicas o jurídicas, que difieran del responsable o su grupo de empresas.
- **Incorporar herramientas eficaces que permitan a los usuarios ejercer su derecho de oposición de manera fácil**.
    - **Por parte del usuario**, esto puede hacerse, por ejemplo, mediante un aviso claro seguido de una dirección de correo electrónico, un panel de datos personales autogestionado o cualquier instrumento similar (por ejemplo, mediante los requisitos de protección de datos por diseño), mediante la creación de casillas que el usuario deba marcar para manifestar *opt-out* que se refieran a diferentes actividades de tratamientos o la presentación de un listado ejemplificativo de potenciales motivos de oposición que asistan al interesado a la hora de fundamentar el ejercicio de su derecho.
    - **Por parte del responsable del tratamiento**, esto puede entrañar la elaboración de instrumentos para mejorar la gestión de los datos dentro de la organización. Puede ser necesario un enfoque

tanto técnico como organizativo para garantizar que haya un control del lugar en que se almacena cada categoría de datos, quién tiene acceso a ellos y con qué fines. Ello se debe a que el ejercicio de un derecho de oposición por parte del interesado puede hacer que el tratamiento de ciertas categorías de datos sea ilícito para fines específicos, pero no para otros. El responsable del tratamiento debe disponer de cualquier medida pertinente que le permita actuar en consecuencia. Esto es particularmente importante en las organizaciones que se ocupan de diversas categorías de datos, almacenados en diferentes lugares dentro de un almacén de datos, en diferentes centros de datos, o que llevan a cabo múltiples operaciones complejas de tratamiento.

- Comunicación clara al interesado de que cesará el tratamiento sobre el que se opusieron y que, en su caso, determinados datos no son eliminados de la base de datos, sino que continuarán siendo tratados para dichas otras finalidades.
- **Argumentación clara y**, en la medida de lo posible, **adaptada al caso concreto, sobre los motivos imperiosos por los que el responsable deba denegar** el ejercicio del derecho de oposición del interesado. En todo caso, la denegación debe ser excepcional. El responsable asume la carga de la prueba de que el tratamiento debe continuar y de que su motivación no fue genérica, sino que tomó en cuenta el caso concreto. En la práctica, esto se traduce en que únicamente podrá continuar el tratamiento cuando los intereses legítimos del responsable fuesen excepcionalmente relevantes, en especial cuando el tratamiento se basa en intereses propios del responsable.
- **Establecimiento de un registro de solicitudes de ejercicio de derechos**, en el que se reflejen, respecto al derecho de oposición, la cantidad de ejercicios solicitados y denegados, los motivos y la justificación de su imperiosidad. Dicho registro podrá ser objeto de auditoría por parte de la autoridad de control o los tribunales. Como

mejor práctica, el responsable publicará un informe anual sobre la cantidad de derechos -y más concretamente, derechos de oposición- que han sido ejercidos por los interesados y cuántos han sido efectivamente atendidos por el responsable.

Derecho de acceso (art. 15 TGPD)

- El derecho de acceso tiene un papel de especial relevancia para permitir al interesado ejercer un control real sobre los datos personales que le conciernen, así como para facilitar el correcto ejercicio de otros derechos.
- El derecho de acceso otorga al interesado las siguientes potestades: por un lado, la capacidad de requerir al responsable confirmación sobre si se está realizando un tratamiento de datos personales referidos al interesado y obtener determinada información relativa al tratamiento, y por otro lado, la obtención de una copia de los datos objeto de tratamiento.
- **El derecho de acceso se despliega sobre datos inferidos, perfiles o fruto de cualquier elaboración o proceso informático o automatizado**.
- **Entre la información que debe prestar el responsable durante el ejercicio de un derecho de acceso cabe destacar por su importancia**: aquella que se refiere a las finalidades del tratamiento, las categorías de datos personales tratados, los destinatarios (o al menos la categoría de destinatarios a los que se comuniquen los datos), la fuente de los datos personales cuando estos no fueron obtenidos del interesado o las garantías que se hubieran establecido en caso de que exista una transferencia internacional de datos personales. Asimismo, el responsable debe informar al interesado de la posibilidad de que este ejerza otros derechos, tales como rectificación, supresión, limitación del tratamiento u oposición. Del mismo modo, el responsable debe informar también acerca de la

existencia de decisiones automatizadas junto con información significativa de la lógica aplicada y sus consecuencias previstas.

- Junto con esta información, cuando se estén realizando tratamientos sobre la base de un interés legítimo, **el responsable aprovechará la comunicación al interesado para informar, de nuevo**, sobre dichos intereses legítimos, los tratamientos basados en ellos y la posibilidad de oponerse a ellos. No debe servir una mención genérica a la existencia de un derecho de oposición desvinculada de la información necesaria para comprender en qué casos concretos se puede ejercer.
- Cuando el tratamiento se refiere a una gran cantidad de información del interesado, el considerando 63 RGPD permite que el responsable pueda accionar la **potestad de solicitar del interesado que especifique sobre qué información o actividades desea ejercer su derecho**. Sin embargo, **el responsable debe hacer un uso limitado** de dicha capacidad. Con carácter general, el responsable debe realizar su mejor esfuerzo por responder a la solicitud de acceso de manera completa. En aquellos casos en los que ejercer dicha potestad esté justificado:
    - **Respecto del derecho del interesado a recibir una copia de sus datos**, el responsable deberá hacer un uso limitado de su petición de que el interesado especifique.
    - **Respecto del derecho del interesado a recibir información sobre el tratamiento**, el responsable únicamente podrá solicitar al interesado que especifique qué información o actividades desea ejercer su derecho en situaciones excepcionales y debidamente motivadas.
- **En su caso, el responsable debe guiar y asistir al interesado cuando necesite que este especifique sobre qué información o actividades desea ejercer su derecho**. Para ello, recaerá sobre el responsable el deber de remitir al interesado aquella información a que se refiere el art. 15. 1 en la medida de lo posible (aquella relativa a los

fines del tratamiento, las categorías de datos tratadas, destinatarios, lógica aplicada en caso de existencia de decisiones automatizadas o posibles consecuencias, etc.), así como cualquier otra información acerca de las actividades del tratamiento que sea significativa y suficiente para que el interesado sea capaz de concretar la petición de acceso de manera efectiva.

- El responsable debe realizar sus mejores esfuerzos para que la información que reciba el interesado conforme al art. 15.1 cumpla con el objetivo del derecho de acceso de obtener control y servir de base para el ejercicio de otros derechos. Por este motivo, la información no debe reiterar el mismo carácter meramente genérico que la información que el interesado ya pudo recibir conforme a los arts. 13 y 14 RGPD. Es decir, en tanto mediante el ejercicio de un derecho se trata de una facultad personal, **la respuesta del responsable ante ello también debe ser personalizada** en la medida de lo posible.
- **El formato en el que el responsable remita la información** al interesado será idealmente aquel que permita que el interesado adquiera conocimiento y control sobre los datos personales y, al mismo tiempo, reutilizable por otro proveedor de servicios al que el interesado quisiera portar sus datos. Por ejemplo, cuando conforme a un derecho de acceso el usuario pueda obtener información sobre su localización durante el tiempo de uso de un dispositivo de medición de actividad física, idealmente esta se transmitirá de modo tal que pueda ser visualizado sobre un mapa (y así, aportar mayor utilidad al interesado), así como en un formato de coordenadas de lectura mecánica (permitiendo así su portabilidad). En caso de que no sea posible, prima el formato que le permita al usuario obtener un control de los datos de modo más sencillo.
- El responsable priorizará también el envío de información en formatos que permitan reutilizar la información (por ejemplo, una tabla) sobre

aquellos otros que no lo permiten (por ejemplo, la imagen de la mista tabla en un documento PDF).

Derecho de portabilidad (art. 20 RGPD)

- El derecho de portabilidad se puede entender como un doble derecho. Por un lado, el derecho a obtener una copia de los datos y, por otro lado, el derecho a que dichos datos sean transferidos al proveedor receptor de la elección del interesado en un formato de lectura mecánica.
- A pesar de que no sea un derecho de obligada atención cuando la base del tratamiento es el interés legítimo, garantizar este derecho aumenta las garantías y la capacidad de control del interesado. **Permitir al interesado ejercitar un derecho de portabilidad** sobre los datos objeto de aquellos tratamientos basados en interés legítimo, aun a pesar de no ser obligatorio será un factor de peso en la evaluación de interés legítimo.
- Los datos susceptibles del derecho deberían incluir, como mínimo, aquellos que son objeto del derecho de portabilidad típico:
    - **Datos aportados directamente por el interesado** (nombre, correo electrónico, fotografías, peso, etc.).
    - **Datos observados** (frecuencias de conexión a una red social, tiempo de respuesta a cuestiones de posibles compradores en una aplicación de venta, kilómetros corridos o velocidad media en una aplicación de monitorización de actividad física, datos de localización durante la utilización del servicio, etc.), en la medida en que hayan sido recogidos y almacenados por el responsable.
- **Como mejor práctica, el responsable debería además garantizar la portabilidad de datos inferidos, aquellos que conforman el perfil** de una persona, patrones de comportamiento y otros datos resultado de un proceso de analítica. La importancia del derecho a obtener y portar este tipo de datos es cada día mayor. Para ello:

- El responsable deberá encontrar un equilibrio entre su interés legítimo a proteger su derecho de propiedad intelectual, secretos comerciales o *know how* y el interés de los usuarios a portar sus datos y hacer a otro proveedor conocedor de su identidad digital.
- Un potencial punto de equilibro podría ser la posibilidad de portar una versión simplificada del perfil de un usuario, sin necesidad de revelar información detallada del modelo algorítmico ni de información extremadamente detallada generada por el responsable. En su caso, el responsable debe atender su obligación de prestar información significativa sobre la lógica aplicada en el proceso de elaboración de perfiles o toma de decisiones automatizadas.
- En todo caso, la denegación de un derecho de portabilidad basada en la necesaria protección de la propiedad intelectual del responsable deberá estar claramente justificada y aplicarse de manera estricta y limitada.

- **El responsable puede implementar medios por los que el interesado ejerza control, acceso, descarga y portabilidad de datos inferidos, así como de sus perfiles**. Para ello, la organización puede crear, por ejemplo, paneles de visualización de las características principales asociadas a cada persona que les permita comprenderlas de modo sencillo y reutilizar dicha información. De este modo, los interesados ven ampliada su capacidad de control sobre la información, así como el beneficio asociado a la utilización de esta. Estos medios de compartir los beneficios del análisis y aplicación de los datos personales pueden ayudar también a inclinar la balanza durante la ponderación de intereses.
- **Los proveedores de servicios digitales deben trabajar en lograr estándares sectoriales de interoperabilidad de sus sistemas**, así como la reutilización de los datos por parte del receptor. Ello se basa en la premisa de que un incorrecto o débil funcionamiento del derecho

de portabilidad en el contexto actual genera consecuencias que trascienden al propio individuo. Las limitaciones al derecho de portabilidad pueden generar deficiencias de mercado por las que los proveedores de un servicio generen o mantengan costes de cambio que dificulten al usuario el movimiento de sus datos a otro proveedor, creando consumidores cautivos.

Derecho a no ser objeto de decisiones automatizadas (art. 22 RGPD)

- El responsable no podrá llevar a cabo tratamientos del art. 22 RGPD basados en el interés legítimo. Para ello, será de relevancia poder definir conceptos como qué se entiende por tratamientos y decisiones únicamente automatizados, qué se entiende por efectos jurídicos o afectación similar significativa para el interesado.
- En su caso, el responsable deberá justificar de modo detallado por qué el tipo de tratamiento en lid no reúne las características del art. 22 y quedan, por tanto, abiertos a la posibilidad de ser basados en un interés legítimo. En concreto, una explicación del alcance de la intervención humana.
- **Si el tratamiento implica el uso de medios automatizados, el responsable debe poder asegurar la capacidad de intervención humana independiente y sustantiva**. De otro modo, la toma de decisiones o las actividades de perfilado que pudieran llegar a cumplir las condiciones del art. 22 RGPD no podrán estar basadas en el interés legítimo.
- Como buena práctica, el responsable que lleve a cabo procesos, que, sin cumplir los requisitos del art. 22, conlleven la de toma de decisiones con un nivel significativo de automatización, incluso cuando estas no sean únicamente automatizadas, o no produzcan efectos significativos o trascendentales para el interesado, deberá también aplicar, como mínimo, las garantías que el RGPD prevé para las decisiones del art. 22, con especial énfasis, en que el interesado exprese su punto de vista sobre la decisión o contestarla.

- En las situaciones a las que se refiere el párrafo anterior, el responsable también deberá informar al interesado de la existencia de dicho tipo de decisiones, aportar información significativa sobre la lógica subyacente al modelo de toma de decisiones, así como las consecuencias previstas y su importancia, todo ello en congruencia con lo exigido en los arts. 13.2.f), 14.2.g) y 15.1.h) RGPD para decisiones del art. 22.
- Mantener las garantías que el RGPD crea para las decisiones automatizadas del art. 22 a aquellas otras decisiones que no cumplan tales requisitos y puedan basar en interés legítimo será un factor de especial peso en la ponderación de intereses. Lo contrario crearía una falta de obligación de informar y proceder que afecta al ejercicio de otros derechos como el de acceso, que provoca que el interesado no sea conocedor de determinados tratamientos que puedan resultarle intrusivos o inesperados. Ello da como resultado un conjunto de incongruencias, lagunas y ambigüedades que pueden terminar por crear graves vacíos o carencias en el sistema de derechos de los interesados. En dicha situación, el ejercicio de ponderación de intereses daría difícilmente un resultado favorable al tratamiento.
- Para hacer la información verdaderamente significativa, el responsable debe adecuar sus comunicaciones, entre otros factores, al momento temporal en que las emite.
    - Conforme a los arts. 13 y 14 RGPD el responsable remite información *ex ante*, y por tanto, de modo más genérico y dirigida a un interesado medio razonable.
    - Cuando el responsable deba proveer información con motivo del ejercicio de un derecho de acceso conforme al art. 15 RGPD, la información, que podrá tener un carácter *ex post*, deberá incluir nuevos conocimientos que no estaban disponibles en momentos anteriores. Ejemplos de ello pueden ser los datos obtenidos por medio de inferencia estadística o un mayor nivel de detalle sobre la lógica del modelo y sus consecuencias presumibles. Asimismo,

deberá referirse y adaptarse en la medida de lo posible al interesado que está ejerciendo su derecho de acceso. Esta información debe ser suficiente para que el interesado pueda accionar las garantías del RGPD tales como expresar su punto de vista sobre la decisión o impugnarla, así como ejercer un derecho de rectificación o iniciar acciones legales, por ejemplo, por discriminación.

- El interés legítimo del responsable a ver protegidos sus **derechos de propiedad intelectual, secretos comerciales o *know how* no deberá ser un obstáculo** para que el interesado obtenga información sobre la lógica algorítmica que le resulte significativa o para para crear una falta de transparencia respecto de prácticas poco éticas que se desean mantener opacas.

OTRAS MEDIDAS

- **Nombramiento de un delegado de protección de datos** en aquellas organizaciones que vayan a realizar tratamientos de datos a través de tecnologías de datos masivos, aun cuando por sus circunstancias pudiera no ser obligatorio.
- **Implementación de medios de protección de datos desde el diseño** que facilite al interesado la interacción con el responsable y una mayor sencillez en el ejercicio de sus derechos.
- **Creación de códigos éticos de conducta sectoriales, preferiblemente a nivel comunitario para reducir diferencias de aplicación entre Estados miembros, así como propios de la organización**.[577] Estos deben cubrir con especial énfasis principios éticos y morales que deban guiar los tratamientos de datos, y en concreto, aquellos basados en interés legítimo. Asimismo, serán de

[577] DÍAZ-ROMERAL GÓMEZ, Alberto (2016): "Los códigos de conducta en el reglamento general de protección de datos", en José Luís Piñar Mañas (dir.), *Reglamento general de protección de datos. Hacia un nuevo modelo europeo de privacidad*, Madrid, Reus, pp. 389-412.

gran utilidad directrices que identifiquen con mayor especificidad qué tipo de intereses y riesgos pueden entrar en lid a cada lado de la balanza responsable-interesados.

El proceso de redacción puede contar con mayores garantías y transparencia si se garantiza la consideración de puntos de vista diversos, por ejemplo, haciendo partícipe a las autoridades de control o mediante la apertura de un trámite de audiencia pública. Asimismo, el desarrollo de estas directrices podrá servir el fin del responsable de ayudar a probar responsabilidad proactiva y la realización de esfuerzo y diligencia debidos para conseguir una visión global de todos los factores del tratamiento.

- **Creación de comités éticos dentro de la organización**. En organizaciones grandes, estos pueden tener lugar dentro de la propia organización, mientras que, en otras ocasiones, podrá ser más conveniente la creación de comités sectoriales o incluso intersectoriales.[578]
- **Establecimiento de un sistema de comunicación con la autoridad de control que facilite un medio de autorización previa en los casos que puedan entrañar un alto riesgo** para los derechos e intereses de las personas. En el contexto de tratamientos datos masivos, es probable que así sea.
- **Creación de un sistema de notificación previa para aquellas operaciones de tratamiento de alto riesgo residual**. Cuando, el resultado de una evaluación de impacto en aquellos casos necesarios, o la determinación del riesgo del tratamiento, muestre que el tratamiento puede conllevar un riesgo alto para los derechos y libertades del interesado, y dicho riesgo no pueda ser razonablemente

[578] El Comité Consultivo del Convenio 108 del Consejo de Europa aboga por el uso de comités éticos internos en sus directrices sobre big data. CONSEJO DE EUROPA (2017): *Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data*. Disponible en: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806ebe7a.

mitigado por el responsable, el responsable deberá llevar a cabo una consulta a la autoridad de control previa al inicio del tratamiento. La autoridad de control podrá emitir recomendaciones adecuadas para reducir el riesgo residual del interesado (véase art. 36 RGPD).

- **Las autoridades de control, los responsables y otros agentes deben establecer medios para proveer educación y concienciación** a los interesados sobre la utilización de nuevas tecnologías y el tratamiento de datos personales, sus posibles consecuencias a nivel individual y común.

PROPUESTAS DE FUTURO PARA EL LEGISLADOR

- Sería útil replantear la posibilidad de **permitir la toma de decisiones totalmente automatizadas** o que produzcan efectos trascendentales para los interesados **sobre un interés legítimo** (así como otros tratamientos considerados sensibles o de riesgo), siempre sujeto a debidas garantías.

- Por su parte, también cobraría sentido **vestir a las autoridades de control en materia de protección de datos de la potestad de modificar el comportamiento de los responsables** o de supeditar el inicio o continuación de determinadas actividades de tratamiento a la implementación de acciones requeridas por la autoridad.

  Ello permitiría la creación de un mecanismo de notificación previa en aquellos tratamientos de alto riesgo residual por el que la autoridad de control analice el proyecto y asesore al responsable de modo que este únicamente pueda ponerse en marcha tras la implementación de las garantías y acciones dispuestos por la autoridad. De este modo se aumenta la seguridad jurídica de responsables que deseen llevar a cabo actividades de alta complejidad, como la aplicación del interés legítimo en una operación que conlleve el uso de tecnologías de datos masivos. Al mismo tiempo, la propia autoridad velaría por la protección de los derechos de los interesados. Para ello, será necesario una mayor dotación de medios y personal a las autoridades, hecho que

cobra sentido en atención a la relevancia de su labor en el desarrollo de una fuerte economía comunitaria basada en datos y respetuosa con los derechos de los ciudadanos.

BIBLIOGRAFÍA

ABRAMATIC, Jean-François; et al (2015): “Privacy Bridges, EU and US privacy experts in search of transatlantic privacy solutions”, en 37th International Privacy Conference Amsterdam.

ABRAMS, Martin (2014): “The Origins of Personal Data and Its Implications for Governance”, en OECD Expert Roundtable Discussion `Protecting Privacy in a Data-Driven Economy: Taking Stock of Current Thinking´.

ABRAMS, Martin (2015): “Unified Ethical Frame for Big Data Analysis”, en *The Information Accountability Foundation*.

ABRAMS, Martin; KROPF, John (2014): “Comments on the Article 29 Working Party’s Opinion 06/2014”, en *The Information Accountability Foundation*.

ADSUARA VALERA, Borja (2016): “El consentimiento”, en José Luís Piñar Mañas (dir.), *Reglamento general de protección de datos. Hacia un nuevo modelo europeo de privacidad*, Madrid, Reus.

AGENCIA DE LOS DERECHOS FUNDAMENTALES DE LA UNIÓN EUROPEA Y CONSEJO DE EUROPA (2019): *Manual de legislación europea en materia de protección de datos*, Ed. 2018, Luxemburgo.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (1999): *Memoria anual, 1999*.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (2012): Nota Informativa, El Tribunal de Justicia de la Unión Europea resuelve la cuestión prejudicial planteada por el Tribunal Supremo relativa a la interpretación del artículo 7 f) de la Directiva 95/46/CE.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, GABINETE JURÍDICO (2017): *Informe 195/2017*.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, GABINETE JURÍDICO (2017): *Informe 232/2017*.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, GABINETE JURÍDICO (2018): *Informe 0173/2018*.AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (2019): Análisis de los flujos de información en Android. Herramientas para el cumplimiento de la responsabilidad proactiva.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (2019): Guía práctica para las evaluaciones de impacto en la protección de los datos sujetas al RGPD.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (2020): Resolución Nº: R/00552/2019, de 5 de febrero.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, GABINETE JURÍDICO (2017): *Informe 0195/2017*.

AGENCIA EUROPEA DE LOS DERECHOS FUNDAMENTALES (2012): Understanding and preventing discriminatory ethnic profiling.

ALTMAN, Micah; et al. (2018): "Practical approaches to big data privacy over time", en *International Data Privacy Law*, Vol. 8, No. 1, pp-. 29–51.

ÁLVAREZ CARO, María (2017): *La privacidad en la sociedad de la información: el derecho al olvido en la UE como reto derivado del avance digital*, tesis doctoral.

ÁLVAREZ CARO, María (2016): "El derecho de rectificación, cancelación, limitación del tratamiento, oposición y decisiones individuales automatizadas", en José Luís Piñar Mañas (dir.), *Reglamento general de protección de datos. Hacia un nuevo modelo europeo de privacidad*, Madrid, Reus.

ÁLVAREZ CARO, María (2015): *Derecho al olvido en internet: el nuevo paradigma de la privacidad*, Madrid, Reus.

ÁLVAREZ CARO, María (2014): “Reflexiones sobre la sentencia del TJUE en el asunto "Mario Costeja" (C-131/12) sobre derecho al olvido”, en *Revista española de derecho europeo*, No. 51.

APARICIO SALOM, Javier (2013): *Estudio sobre la protección de datos*, 4ª ed., Navarra, Aranzadi Thomson Reuters.

APARICIO SALOM, Javier (2017): “Big data y entidades financieras”, en *La Revista Análisis Financiero, Instituto Español de Analistas Financieros*.

APARICIO SALOM, Javier (2019): “Derecho de oposición y decisiones individuales automatizadas. Limitaciones (Arts. 21-23 RGPD. Art. 18 LOPDGDD)” en *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD*, 2ª ed. Madrid, Wolters Kluwer.

ARELLANO TOLEDO, Wilma (2019): “El derecho a la transparencia algorítmica en Big Data e inteligencia artificial”, en *Revista General de Derecho Administrativo*, No. 50.

ARENAS RAMIRO, Mónica; et al (2019): “Derechos fundamentales y libertades públicas”, en *Revista española de derecho adminstrativo*, No. 201.

ARTEAGA JUÁREZ, Sor (2014): “Implicaciones legales de la prestación de servicios de cloud computing. Especial referencia a la protección de datos de carácter personal”, en *Revista da AJURIS*, Vol. 41, No. 135.

ASCHER, Marcia; ASCHER, Robert (2013): *Mathematics of the Incas: Code of the Quipu*, Courier Corporation.

ASOCIACIÓN PROFESIONAL ESPAÑOLA DE PRIVACIDAD (APEP) (2015): *Nueva legislación de protección de datos de la UE* [Nota de prensa], de 15 de diciembre.

AUSLOOS, Jeff (2016): “The Interaction between the Rights to Object and to Erasure in the GDPR”, en *KU Leuven Centre for IT & IP law (CiTiP)*.

AUSLOOS, Jeff (2018): *The Right to Erasure in EU Data Protection Law*, Oxford University Press.

BABINIP, Nicolás (2003): “Las antecesoras de la computadora: la era de la tabuladora”, en *Revista de Historia de la Ciencia Saber y Tiempo*, Vol. 4, No. 16.

BAKSHI, Kapil (2012): “Considerations for Big Data: Architecture and Approach”, en *2012 Aerospace Conference,* IEEE.

BALBONI, Paolo; et al. (2013): “Legitimate interest of the data controller New data protection paradigm: legitimacy grounded on appropriate protection” en *International Data Privacy Law*, Vol.3, No.4, pp. 244-261.

BAROCAS, Solon; BRADLEY, Elizabeth; HONAVAR, Vasant; PROVOST, Foster (2017): “Big Data, Data Science, and Civil Rights”, en *Computing Community Consortium*.

BAROCCAS, Solon; NISSEBAUM, Helen (2014): “Big data´s End Run Around Anonymity And Consent”, en *Privacy, big data and the public good. Frameworks for engagement*, Cambridge University Press, p.44-75.

BARRIO ANDRÉS, Moisés (2018): “Robots, inteligencia artificial y persona electrónica”, en Tomás de la Quadra-Salcedo y José Luis Piñar (dirs.), *Sociedad digital y Derecho*, Madrid, BOE-Red.es.

BARRIO ANDRÉS, Moisés (dir.) (2018): *Derecho de los robots*, Madrid, Wolters Kluwer.

BATTAGLINI Manuela; RASMUSSEN Steen (2019): “Transparency, automated decision-making processes and personal profiling”, en J*ournal of Data Protection & Privacy*, Vol. 2, No. 4, pp. 331-349.

BAUDRILLARD, Jean (1981): *Simulacres et Simulation and Simulation*, Éditions Galilée.

BAUZÁ MARTORELL, Felio José (2017): “Big data y open data en la administración turística: acceso y reutilización de información”, en *Revista Vasca de Administración Pública. Herri-Arduralaritzako Euskal Aldizkaria*, No. 108, pp. 19-41.

BAUZÁ MARTORELL, Felio José (2017): "Big data y open data en la administración turística: acceso y reutilización de información", en *Revista Vasca de Administración Pública. Herri-Arduralaritzako Euskal Aldizkaria*, No. 108, pp. 19-41.

BECERRA, María del Carmen; GÓMEZ, María Claudia; ZARATE, Pedro (2017): "Modelo Genérico para la Gestión de Privacidad de Grandes Datos/Big Data", en *Simposio Argentino sobre Tecnología y Sociedad (STS)*, Córdoba.

BERGIN, Thomas J.; HAIGH, Thomas (2009): "The Commercialization of Database Management Systems, 1969–1983", en *Annals of the History of Computing*, IEEE, Vol. 31, No. 3.

BERRY, Michael J. A.; LINOFF, Gordon S. (2004): Data Mining Techniques: For Marketing, Sales, and Customer Relationship Management, John Wiley & Sons.

BIG BROTHER WATCH (2014): Briefing Note: Why Communications Data (Metadata) Matter.

BODY OF EUROPEAN REGULATORS FOR ELECTRONIC COMMUNICATIONS (2016): *Report on OTT services.*

BOYD, danah; CRAWFORD, Kate (2012): "Critical questions for big data", en *Information, Communication & Society*, Vol. 15, No. 5, pp. 662-679.

BRYSON, Joanna J. (2018): "Patiency is not a virtue: the design of intelligent systems and systems of ethics", en *Ethics and Information Technology*, Vol. 20, No. 1, pp. 15-26.

BUTARELLI, Giovanni (2016): "The EU GDPR as a clarion call for a new global digital gold standar", en *International Data Privacy Law*, Vol 6, No. 2, pp. 77-78.

BUTTARELLI, Giovanni (2019): "Deception by design?" en *ISMS Forum Spain: XXI International Information Security Conference*, Madrid, de 30 de mayo.

BUTTARELLI, Giovanni: “The Commission Proposal for a Regulation on ePrivacy (2017): Why Do We Need a Regulation Dedicated to ePrivacy in the European Union?”, en *European Data Protection Law Review*, Vol. 3, No. 2.

BYGRAVE, Lee A. (2002): Data Protection Law: Approaching Its Rationale, Logic and Limits, Kluwer law international.

CASA BLANCA (2016): “Big Data: A Report on Algorithmic Systems. Opportunity, and Civil Rights”.

CATE, Fred H. y MAYER-SCHÖENBERGER, Viktor (2013): “Notice and consent in a world of Big data”, en *International Data Privacy Law*, Vol. 3, No. 2.

CENTRE FOR INFORMATION POLICY LEADERSHIP (2017): *Comments on the Proposal for an ePrivacy Regulation*, de 11 de septiembre.

CENTRE FOR INFORMATION POLICY LEADERSHIP (2018): “EPR vis-à-vis GDPR, A comparative analysis of the ePrivacy Regulation and the General Data Protection Regulation”.

CENTRE FOR INFORMATION POLICY LEADERSHIP (CIPL) (2018): *Artificial Intelligence and Data Protection: Delivering Sustainable AI Accountability in Practice, First Report: Artificial Intelligence and Data Protection in Tension*.

CENTRE FOR INFORMATION POLICY LEADERSHIP (CIPL) (2018): *The e-Privacy Regulation and the EU Charter of Fundamental Rights*.

CENTRE FOR INTELLECTUAL PROPERTY AND INFORMATION LAW, UNIVERSIDAD DE CAMBRIDGE, *Data Protection Directive, Detailed index of article development*.

CERRILLO I MARTÍNEZ, Agustí (2019): “El impacto de la inteligencia artificial en el derecho administrativo. ¿Nuevos conceptos para nuevas realidades técnicas?”, en *Revista General de Derecho Administrativo*, No. 50.

CERVERA NAVAS, Leonardo (2018): “Data processing beneficial to individuals: the use of legitimate interest”, en *Computers, Privacy and Data Protection Conference*, Bruselas.

CHEN, Daizhuo; FRAIBERGER, Samuel P.; MOAKLER, Robert; PROVOST, Foster (2017): “Enhancing Transparency and Control when Drawing Data-Driven Inferences about Individuals” Big data, Vol. 5, No. 3, pp. 197-212.

CHEN, Hsinchun; CHIANG, Roger HL; STOREY, Veda C. (2012): “Business Intelligence and Analytics: From Big Data to Big Impact”, en *MIS quarterly*, Vol. 36, No 4, p. 1165-1188.

CODD, Edgar F. (1970): “A relational model of data for large shared data banks”, en *Communications of the ACM*, Vol. 13, No. 6, p. 377-387.

COLUMBUS, Louis (2018): “The state of business intelligence 2018”, en *Forbes*.

COMISIÓN EUROPEA (2010): *A comprehensive approach of data protection in Europe* (COM 2010), de 4 de noviembre.

COMISIÓN EUROPEA (2012): Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses.

COMISIÓN EUROPEA (2012): Documento de Trabajo de la Comisión relativo a la evaluación de impacto de su Propuesta de Reglamento General de Protección de Datos (SEC(2012) 72 final), de 25 de enero.

COMISIÓN EUROPEA (2014): *MEMO 14/455 Making the most of the Data-Driven Economy*.

COMISIÓN EUROPEA (2015): *Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, "Una estrategia para el mercado único digital de Europa"*.

COMISIÓN EUROPEA (2017): Ex-post REFIT evaluation of the ePrivacy Directive 2002/58/EC SWD(2017), de 10 de enero.

COMISIÓN EUROPEA (2019): Special Eurobarometer 487ª, The General Data Protection Regulation.

COMISIÓN EUROPEA (2019): *Special Eurobarometer 487ª, The General Data Protection Regulation.*

COMISIÓN EUROPEA, DIRECTORATE-GENERAL FOR RESEARCH AND INNOVATION, EUROPEAN GROUP ON ETHICS IN SCIENCE AND NEW TECHNOLOGIES (2018): *Statement on Artificial Intelligence, Robotics and 'Autonomous' Systems"*.

COMITÉ EUROPEO DE PROTECCIÓN DE DATOS (2018): Statement on the revision of the ePrivacy Regulation and its impact on the protection of individuals with regard to the privacy and confidentiality of their communications.

COMITÉ EUROPEO DE PROTECCIÓN DE DATOS (2019): Declaración 3/2019 sobre el reglamento de privacidad y las comunicaciones electrónicas, de 13 de marzo.

COMITÉ EUROPEO DE PROTECCIÓN DE DATOS (2019): Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, de 8 de octubre.

COMITÉ EUROPEO DE PROTECCIÓN DE DATOS (2019): *Guidelines 4/2019 on Article 25 Data Protection by Design and by Default*, p. 15, de 13 de noviembre.

COMITÉ EUROPEO DE PROTECCIÓN DE DATOS (2020): *Guidelines 05/2020 on consent under Regulation 2016/679*, de 4 de mayo.

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS (2017): Data transfer from WHATSAPP to FACEBOOK: CNIL publicly serves formal notice for lack of legal basis, de 18 de diciembre.

Complete Travaux (English) of the Data Protection Directive.

CONFEDERACIÓN DE ORGANIZACIONES EUROPEAS DE PROTECCIÓN DE DATOS (CEDPO) (2012): *Comparative Analysis of Data Protection Officials Role and Status in the EU and More*.

CONGRESO Y SENADO DE ESTADOS UNIDOS, COMITÉ DE ASUNTOS JURÍDICOS, SUBCOMITÉ DE DERECHOS CONSTITUCIONALES (1969): Privacy, the Census and Federal Questionnaires: Hearings Before the Subcommittee on Constitutional Rights of the Committee on the Judiciary, United States Senate, Ninety-first Congress, First Session, on S. 1791, to Secure Personal Privacy and to Protect the Constitutional Right of Individuals to Ignore Unwarranted Requests for Personal Information, April 24, 25, May 2, and July 1.

CONSEJO DE EUROPA (1973): Explanatory Report to: Council of Europe - Committee of Ministers, Resolution (73) 22 on the Protection of the Privacy of Individuals Vis-à-Vis Electronic Data Banks in the Private Sector.

CONSEJO DE EUROPA (2010): The protection of individuals with regard to automatic processing of personal data in the context of profiling, Recommendation CM/Rec (2010) 13 and explanatory memorandum, de 23 de noviembre.

CONSEJO DE EUROPA (2011): *The protection of individuals with regard to automatic processing of personal data in the context of profiling, Recommendation CM/Rec(2010)13 and explanatory memorandum*.

CONSEJO DE EUROPA (2017): Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data.

CONSEJO DE EUROPA (2017): *Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data*.

CONSEJO DE LA UNIÓN EUROPEA, SECRETARÍA GENERAL (2019): Preparation of the Council position on the evaluation and review of the General Data Protection Regulation (GDPR) - Comments from Member States, de 9 de octubre.

COOLEY, Thomas McIntyre (1888): *A Treatise on the Law of Torts or the Wrongs which Arise Independent of Contract*, 2ª ed., Chicago, Callaghan.

CORAGGIO, Giulio (2018): "Italy: legitimate interest gets complicated", en *DLA Piper's Global Privacy & Data Protection Resource*, de 22 de enero.

CORMACK, Andrew A. (2016): "A Data Protection Framework for Learning Analytics", en *Journal of Learning Analytics*, Vol. 3, No. 1, pp. 91-106.

CORMACK, Andrew Nicholas (2016): "Downstream consent: A Better Legal Framework For Big Data", en *Journal of Information Rights, Policy and Practice*, Vol. 1, No. 1.

COTE PEÑA, Luis Fernando (2015): *Hábeas Data en Colombia, un trasplante normativo para la protección de la dignidad y su correlación con la NTC/ISO/IEC 27001*, en Agencia Española de Protección de Datos y Agencia Estatal Boletín Oficial del Estado.

COTINO HUESO, Lorenzo (2017): "Big data e inteligencia artificial. Una aproximación a su tratamiento jurídico desde los derechos fundamentales" en Dilemata, No. 24.

COTINO HUESO, Lorenzo (2019): "Riesgos e impactos del big data, la inteligencia artificial y la robótica. Enfoques, modelos y principios de la respuesta del derecho". Revista General de Derecho Administrativo, No. 50.

COUNCIL OF EUROPE, EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS (2018): *Handbook on European data protection law"*, Luxemburgo, Publications Office of the EU.

COX, Michael; ELLSWORTH, David (1997): "Application-controlled demand paging for out-of-core visualization", en *Proceedings of the 8th Visualization '97 Conference*, IEEE, p. 235-244.

COX, Michael; ELLSWORTH, David (1997): "Managing Big Data for Scientific Visualization", en *ACM Siggraph*, Vol. 97, p. 21-38.

CULNAN, Mary J.; BRUENING, Paula. (2018): "Privacy Notices Limitations, Challenges, and Opportunities", en Evan Selinger, Rochester Institute of Technology, New York, Jules Polonetsky, Omer Tene (eds.), *The Cambridge Handbook of Consumer Privacy*, Cambridge University Press, pp. 524-545.

CUSTERS, Bart; URŠIČ, Helena (2016): "Big data and Data Reuse. A taxnonomy of data reuse for balancing big data benefits and personal data protection", en *International Data Privacy Law*, Vol. 6, No. 1, pp. 4-15.

CUSTERS, Bart; URSIC, Helena (2016): "Big data and data reuse: a taxonomy of data reuse for balancing big data benefits and personal data protection", en *International Data Privacy Law*.

CUSTERS, Bart; VAN DER HOF, Simone; SCHERMER, Bart (2014): "Privacy Expectations of Social Media Users: The Role of Informed Consent in Privacy Policies", en *Policy Internet* Vol. 6, No. 3, pp. 268-295.

D. WARREN, Samuel; BRANDEIS, Louis D. (1890): "The right to privacy", en *Harvard Law Review*.

DATA PROTECTION COMMISSION (2017): *Informe Anual 2017*.

DATA PROTECTION COMMISSION, (2019): Guidance Note: Legal Bases for Processing Personal Data.

DATA PROTECTION NETWORK (2017): Guidance on the use of Legitimate Interests under the EU General Data Protection Regulation.

DATA PROTECTION NETWORK (2018): Guidance on the use of legitimate interests under the EU General Data Protection Regulation (v.2.0).

DATENSCHUTZSTELLE FÜRSTENTUM LIECHTENSTEIN, Berechtigtes Interesse gem. Art. 6 Abs. 1 Bst. f DSGVO.

DE HERT, Paul, REIDENBERG, Joel, RUBINSTEIN, Ira et al. (2015): "Privacy Bridges, EU and US privacy experts in search of transatlantic privacy solutions", en *37th International Privacy Conference Amsterdam*.

DE HERT, Paul; PAPAKONSTANTINOU, Vagelis (2012): "The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals", en *Computer Law & Security Review*, Vol. 28, No. 2.

DE LA QUADRA-SALCEDO FERNÁNDEZ DEL CASTILLO, Tomás (2018): "Retos, riesgos y oportunidades de la sociedad digital", en Tomás de la Quadra-Salcedo y José Luis Piñar (dirs.), *Sociedad digital y Derecho*, Madrid, BOE-Red.es.

DE MIGUEL, Íñigo; MÉNDEZ GARCÍA, Miriam; ALFONSO FARNÓS, Icíar (2019): "La legitimación para el tratamiento de categorías especiales de datos con finalidades de investigación en el marco del Reglamento (UE) 2016/679 y de la Ley Orgánica 3/2018", en *Revista de Derecho y Genoma Humano*, No. Extraordinario.

DEMCHENKO, Yuri; DE LAAT, Cees; MEMBREY, Peter (2014): "Defining architecture components of the Big Data Ecosystem", en *2014 International Conference on Collaboration Technologies and Systems (CTS),* IEEE.

DIAKOPOULOS, Nicholas (2014): "Algorithmic-Accountability Reporting: on the investigation of Black Boxes", en *Tow Center for Digital Journalism*.

DÍAZ-ROMERAL GÓMEZ, Alberto (2016): "Los códigos de conducta en el reglamento general de protección de datos", en José Luís Piñar Mañas (dir.), *Reglamento general de protección de datos. Hacia un nuevo modelo europeo de privacidad*, Madrid, Reus.

DIGNUM, Virginia (2018): "Ethics in artificial intelligence: introduction to the special issue, en *Ethics and Information Technology*, Vol. 20, No. 1.

DIRECTOR DEL SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS (2018): "Data processing beneficial to individuals: the use of legitimate interest", en *Computers, Privacy and Data Protection Conference*, Bruselas.

DOMINGO MONFORTE, José; et al (2013): "Evolución y socialización del riesgo. Compás legislativo", en *Revista INESE*, No. 7.

DUHIGG, Charles (2012): “How Companies Learn Your Secrets”, en *The New York Times*, de 16 de febrero.

ECKES, Christina (2013): “European Union Legal Methods. Moving away from integration”, en Ulla Neergaard and Ruth Nielsen (eds.), *European Legal method - Towards a New European Legal Realism?*, DJOF Publishing.

EDWARDS, Lilian (2018): “Data Protection and ePrivacy: From Spam and Cookies to Big Data, Machine Learning and Profiling”, en Lilian Edwards (ed.), *Law, Policy and the Internet*, Hart.

ESTELLA DE NORIEGA, Antonio (2019): “Hacia una Teoría del Derecho como Credibilidad”. *Discurso de toma de posesión como Académico Correspondiente de la Real Academia de Doctores de España*.

EVELSON, Boris; NICHOLSON, Norman, (2008): *Topic overview: business intelligence*, Forrester.

FERNÁNDEZ-SAMANIEGO, Javier y FERNÁNDEZ-LONGORIA, Paula (2016): “El derecho a la portabilidad de los datos”, en José Luís Piñar Mañas (dir.), *Reglamento General de Protección de Datos: Hacia un nuevo modelo europeo de privacidad*, Madrid, Reus.

FERNÁNDEZ-SAMANIEGO, Javier; FERNÁNDEZ-LONGORIA, Paula (2019): “El interés legítimo como principio para legitimar el tratamiento de datos”, en Artemi Rallo Lombarte (coord.), *Tratado de protección de datos*, Madrid, Tirant lo Blanch.

FERRETTI, Federico (2012): “A European perspective on data processing consent through the re-conceptualization of European data protection’s looking glass after the Lisbon Treaty: taking rights seriously”, en *European Review of Private Law*, No. 2.

FIALOVÁ, Eva (2014): “Data portability and informational self-determination”, en *Masaryk University Journal of Law and Technology*, Vol. 8, No. 1.

FINCK, Michèle (2017): “Blockchains and Data Protection in the European Union”, en *Max Planck Institute for Innovation and Competition Research Paper Series*, No. 18-01.

FORO ECONÓMICO MUNDIAL (2019): *Why Big Data Keeps Getting Bigger*.

FORO ECONÓMICO MUNDIAL, THE BOSTON CONSULTING GROUP (2012): “Rethinking Personal Data: Strengthening Trust”, en *Proyecto Rethinking Personal Data*.

Freek BOMHOF (2017): “In order to trust big data, transparency is not enough”, en *Datafloq*.

FUTURE FOR PRIVACY FORUM: *What is Do Not Track?*

FUTURE OF PRIVACY FORUM (2017): *Unfairness by algorithm: distilling the harms of automated decision-making*.

GAMBA Julián; et al (2019): “An Analysis of pre-installed android software”, en *41th Symposium on Security and Privacy*, IEEE San Fransisco.

GANDOMI, Amir; HAIDER, Murtaza (2015): “Beyond the hype: Big data concepts, methods, and analytics”, en *International Journal of Information Management*, Vol. 35, No. 2, p. 137-144.

GANTZ, John; REINSEL, David (2011): “Extracting Value from Chaos”, en *IDC Review*, Vol. 1142, p.1-12.

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI (2015): Registro de medidas n. 663. Verificación preliminar. Procesamiento agregado de datos personales en el contexto de una actividad de creación de perfiles compleja y detallada, de 17 de diciembre.

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, Guida all'applicazione del Regolamento europeo in materia di protezione dei dati personali.

GARCÍA, Eddie (2016): “Big data, open data and the need for data transparency (Industry Perspective)”, en *Government Technology*.

GARCÍA MEXÍA, Pablo Luis (2012): *Historias de internet. Casos y cosas de la red de redes*, en Tirant Humanidades, Valencia.

GARCÍA MEXÍA, Pablo Luís (2001): "La ética pública: Perspectivas actuales", en *Revista de Estudios Políticos*, No. 114.

GARRETT, Thomas A. (2003): "Aggregated versus disaggregated data in regression analysis: implications for inference", en *Economics Letters*, Vol. 81, No. 1, p. 61-65.

GELLERT, Raphaël; GUTWIRTH, Serge (2013): "The legal construction of privacy and data protection", en *Compute Law & Security Review*, Vol. 29, No. 5, p- 522-530.

GIL GONZÁLEZ, Elena (2016): Big data, privacidad y protección de datos, en *Agencia Española de Protección de Datos y Agencia Estatal Boletín Oficial del Estado*.

GIL GONZÁLEZ, Elena; De HERT, Paul (2019): "Understanding the legal provisions that allow processing and profiling of personal data—an analysis of GDPR provisions and principles", en *ERA Forum*. Vol. 19. No. 4. Springer Berlin Heidelberg, p. 597-621

GIL GONZÁLEZ, Elena; DE HERT, Paul; PAPAKONSTANTINOU, Vagelis (2020): "The proposed e-Privacy Regulation, The Commission's and the Parliament's drafts at crossroad?", en *Data Protection and Privacy, Data Protection and Democracy*, Hart Publishing, Oxford, 2020.

GILAD, Tamar; GILAD, Benjamin (1986): "SMR Forum, Business Intelligence – The quiet revolution", en *Sloan Management Review*, Vol. 27, No. 4.

GOLD, Sue (2014): "Big data and data protection paper from ICO" en Journal of Direct, Data and Digital Marketing Practice, Vol. 16, No. 2, pp. 135–137.

GONZÁLEZ FUSTER, Gloria (2014): *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, Vol. 16, 1ª ed., Springer International Publishing.

GONZÁLEZ FUSTER, Gloria; GELLERT, Raphaël (2012): “The Fundamental Right of Data Protection in the European Union: In Search of an Uncharted Right”, en *International Review of Law, Computers & Technology*, Vol. 46, p. 73-75.

GOODMAN, Bryce; FLAXMAN, Seth (2017): “European Union regulations on algorithmic decision-making and a "right to explanation"”, en *AI Magazine*, Vol. 38, No. 3.

GORUNESCU, Florin (2011): *Data Mining: Concepts, models and techniques*, Springer Science & Business Media, Vol.12.

GORUNESCU, Florin (2011): *Data Mining: Concepts, models and techniques*, Springer Science & Business Media.

GRAD, Burton; BERGIN, Thomas J. (2009): “History of Database Management Systems”, en *Annals of the History of Computing*, IEEE, Vol. 31, No. 3, p. 3-5.

GRUPO DE TRABAJO DEL ARTÍCULO 29 (2010): Dictamen 1/2010 sobre Dictamen 1/2010 sobre los conceptos de «responsable del tratamiento» y «encargado del tratamiento» (WP 169), de 16 de febrero.

GRUPO DE TRABAJO DEL ARTÍCULO 29 (2010): *Dictamen 3/2010 sobre el principio de responsabilidad* (WP 173), de 13 de julio.

GRUPO DE TRABAJO DEL ARTÍCULO 29 (2011): *Dictamen 15/2011 sobre la definición del consentimiento* (WP 187), de 13 de julio.

GRUPO DE TRABAJO DEL ARTÍCULO 29 (2013): *Opinion 03/2013 on Purpose Limitation* (WP 203), de 2 de abril.

GRUPO DE TRABAJO DEL ARTÍCULO 29 (2013): *Working Party comments to the vote of 21 October 2013 by the European Parliament’s Libe Committee*, Anexo de la Carta a la Presidencia griega, de 11 de diciembre de 2013.

GRUPO DE TRABAJO DEL ARTÍCULO 29 (2014): Dictamen 06/2014 sobre el concepto de interés legítimo del responsable del tratamiento de los

datos en virtud del artículo 7 de la Directiva 95/46/CE (WP 217), de 9 de abril.

GRUPO DE TRABAJO DEL ARTÍCULO 29 (2014): Guidelines on the implementation of the Court of Justice of the European Union judgment on "Google Spain and Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" C-131/12 (WP 225), de 26 de noviembre.

GRUPO DE TRABAJO DEL ARTÍCULO 29 (2014): Statement on the impact of the development of big data on the protection of individuals with regard to the processing of their personal data in the EU (WP 221), de 16 de septiembre.

GRUPO DE TRABAJO DEL ARTÍCULO 29 (2017): *Guidelines on Data Protection Impact Assessment* (DPIA) (WP 248 rev.01), de 13 de octubre. Adoptadas por el Comité Europeo de Protección de Datos.

GRUPO DE TRABAJO DEL ARTÍCULO 29 (2017): *Guidelines on the right to data portability* (WP 242 rev.01), de 5 de abril. Adoptadas por el Comité Europeo de Protección de Datos.

GRUPO DE TRABAJO DEL ARTÍCULO 29 (2018): *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679* (WP 251 rev.01), de 6 de febrero. Adoptadas por el Comité Europeo de Protección de Datos.

GRUPO DE TRABAJO DEL ARTÍCULO 29 (2018): *Guidelines on consent under Regulation 2016/679* (WP 259 rev.01), de 10 de abril.

GRUPO DE TRABAJO DEL ARTÍCULO 29 (2018): *Guidelines on Transparency under Regulation 2016/679* (WP 260 rev.01), de 11 de abril. Adoptadas por el Comité Europeo de Protección de Datos.

GUASCH PORTAS, Vicente; SOLER FUENSANTA, José Ramón (2015): "El interés legítimo en la protección de datos", en *Revista de Derecho UNED*, No. 16.

GUICHOT, Emilio (2019): “El reconocimiento y desarrollo del derecho al olvido en el Derecho europeo y español”, en *Revista de administración pública*, No. 209.

GUICHOT, Emilio (2019): “Nuevos retos de la transparencia”, en *Cuadernos de derecho local*, No. 49.

GUITIÉRREZ DAVID, María Estrella (2017): “Discutiendo la transparencia de las políticas de privacidad en la Era del Big Data. Hacia la Norma Social como una nueva Regla de Derecho”, en *Dilemata,* No. 24, pp. 165-184.

HAIGH, Thomas (2009): “How Data Got its Base: Information Storage Software in the 1950s and 1960s”, en *Annals of the History of Computing*, IEEE, Vol. 31, No. 3, p. 17.

HAMEL, Lutz; HALL, Tyler (2005): “A brief tutorial on Database Queries, Data Mining, and OLAP” en *The Encyclopedia of Data Warehousing and Mining*, Vol. 401, p. 5.

HAND, David J. (2007): “Principles of data mining”, en *Drug Safety*, Vol. 30, No. 7, p. 621.

HEREDERO HIGUERAS, Manuel (2000): “Estudio crítico de la transposición de la Directiva 95/46/CE en el Ordenamiento Jurídico español por la L.O. 15/1999, de 13 de diciembre”, en Conferencia pronunciada en el curso de verano de la Universidad Nacional de Educación a Distancia, 18 de julio.

HERNÁNDEZ LÓPEZ (2013) José Miguel HERNÁNDEZ LÓPEZ (2013), *El derecho a la protección de datos personales en la doctrina del Tribunal Constitucional*, Aranzadi, Cizur Menor.

HILDEBRANDT, Mireille (2016): “The new Imbroglio: living with machine learning algorithms”, en Janssens, L. (ed), *The Art of Ethics in the Information Society, Mind you*, Amsterdam: Amsterdam University Press, pp. 55-60.

HILDEBRANDT, Mireille (2019): “Privacy as protection of the incomputable self: From agnostic to agonistic machine learning”, en *Theoretical Inquiries in Law*, Vol. 20, No. 1, pp. 83-121.

HOEL, Tore; CHEN, Weiqin (2017): “Towards Developing an Educational Maxim for Privacy and Data Protection in Learning Analytics”, en *EC-TEL Workshop on Ethics and Privacy for Learning Analytics*, Tallinn, Estonia, septiembre, Vol. 12.

HOFFMAN, David; MASUCCI, Riccardo (2018): Intel’s AI Privacy Policy White Paper. Protecting individuals’ privacy and data in the artificial intelligence world, en *Intel Corporation*.

HOFFMAN, David; RIMO, Patricia (2017): “It takes data to protect data”, en *SSRN Electronic Journal*, 2973280, pp.1-16.

HONDIUS, Frits (1975): *Emerging Data Protection in Europe*, North-Holland.

HUTCHINSON, Terry; DUNCAN, Nigel James (2012): “Defining and Describing What We Do: Doctrinal Legal Research”, en *Deakin Law Review*, Vol. 17, No. 1.

IAB SPAIN (2018): *Estudio anual sobre redes sociales 2018*.

INFORMATION COMMISSIONER’S OFFICE (2014): *Big data and data protection*.

INFORMATION COMMISSIONER’S OFFICE (2015): *Response to the House of Commons Science and Technology Committee inquiry on “The big data dilemma”*.

INFORMATION COMMISSIONER’S OFFICE (2017): Big data, artificial intelligence, machine learning and data protection (versión 2.2).

INFORMATION COMMISSIONER’S OFFICE (2017): Big data, artificial intelligence, machine learning and data protection.

INFORMATION COMMISSIONER’S OFFICE (2018): *Guide to Privacy and Electronic Communications Regulations*.

INFORMATION COMMISSIONER'S OFFICE (2018): Guide to the General Data Protection Regulation (RGPD).

INFORMATION COMMISSIONER'S OFFICE (2018): *Lawful basis for processing, consent*.

INFORMATION COMMISSIONER'S OFFICE (2019): *Lawful basis guidance*.

INFORMATION COMMISSIONER'S OFFICE (2019): Update report into adtech and real time bidding.

INFORMATION COMMISSIONER'S OFFICE (2019): *Update report into adtech and real time bidding*.

INFORMATION COMMISSIONER'S OFFICE: *Guidance on legitimate interest*.

INTERNATIONAL BIOETHICS COMMITTEE (2017): *Report on big data and health*.

INTERNATIONAL DATA CORPORATION (IDC) (2017): Data Age 2025: The Evolution of Data to Life-Critical, Don't Focus on Big Data; Focus on the Data That's Big.

INTERNATIONAL WORKING GROUP ON DATA PROTECTION IN TELECOMMUNICATIONS (2014): Working Paper on Big Data and Privacy Privacy principles under pressure in the age of Big Data analytics, 55th Meeting, 5 - 6 de mayo, Skopje.

INUKOLLU, Venkata Narasimha; ARSI, Sailaja y RAVURI, Srinivasa Rao (2014): "Security issues associated with Big Data in cloud computing", en *International Journal of Network Security & Its Applications*, Vol. 6, No. 3.

INUKOLLU, Venkata Narasimha; ARSI, Sailaja; RAVURI, Srinivasa Rao (2014): "Security issues associated with big data in cloud computing", en *International Journal of Network Security & Its Applications*, Vol. 6, No. 3.

JELINEK, Andrea (2019): IAPP Global Privacy Summit.

JENSEN, Michael R.; MOLLER, Thomas H.; PEDERSEN, Torben B. (2001): “Specifying OLAP cubes on XML data”, en *Journal of Intelligent Information Systems*, Vol. 17, No. 2-3, p. 256.

JERNIGAN, Carter; MISTREE, Behram FT (2009): "Gaydar: Facebook friendships expose sexual orientation", en *First Monday*, Vol. 14, No. 10.

JONAS, Jeff; CAVOUKIAN, Ann. (2012): “Privacy by Design in the Age of Big data”, en *Privacy by Design (PbD)*.

KALIMO, Harri; MAJCHER, Klaudia (2017): “The Concept of Fairness: Linking EU Competition and Data Protection Law in the Digital Marketplace”, en *European Law Review*, No. 2.

KAMARA, Irene; DE HERT, Paul (2018): “Understanding The Balancing Act Behind The Legitimate Interest Of The Controller Ground: A Pragmatic Approach”, en Evan Selinger, Rochester Institute of Technology, New York, Jules Polonetsky, Omer Tene (eds.), *The Cambridge Handbook of Consumer Privacy*, Cambridge University Press, pp. 321-352.

KAMINSKI, Margot E. (2019): “The right to explanation, explained”, U of Colorado Law Legal Studies Research Paper No. 18-24, en *Berkeley Techology Law Journal*, *V*ol. 34, No. 1, p. 189.

KAYWORTH, Tim; BROCATO, Leslie; WHITTEN, Dwayne (2005): “What is a Chief Privacy Officer? An Analysis Based on Mintzberg's Taxonomy of Managerial Roles”, en *Communications of the Association for Information Systems*, Vol. 16.

KELLER, Benno; et al. (2018): “Big Data and Insurance: Implications for Innovation, Competition and Privacy”, en *The Geneva Association*, pp. 1-48.

KJERSTAD, Kristina (2017): “Building an European data driven economy” conferencia presentada en *CPDP 2017, The age of intelligent machines*.

KOSTA, Eleni (2013): *Consent in European Data Protection Law*, Martinus Nijhoff Publishers

KUNER, Christopher; SVANTESSON, Dan Jerker B.; CATE, Fred H.; LYNSKEY, Orla; MILLARD, Christopher (2017): “Machine learning with personal data: is data protection law smart enough to meet the challenge?”, en *International Data Privacy Law*, Vol 7, No. 1, pp. 1-2.

LANEY, Doug (2001): 3D Data Management: Controlling Data Volume, Velocity and Variety, META Group research note, Vol. 6, No. 70.

LEE; Phil; WEBBER, Mark (2016): “The New EU Data Protection Regulation in under 60 minutes”, en *Conferencia* de 17 de mayo.

LESSIG, Lawrence (2000): “Code is Law”, en *Harvard Magazine*.

LEVY Karen; BAROCAS, Solon (2017): “Designing against discrimination in online markets”, en *Berkerley Technology Law Journal*, Vol. 32.

LLANEZA, Paloma (2019): “La adaptación de los consentimientos tácitos y presuntos: el uso del interés legítimo”, en Javier López Calvo (coord.), *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD*, Wolters Kluwer, Madrid.

López Carballo, Daniel (coord.); et al (2015): *Protección de datos y habeas data: una visión desde Iberoamérica*, en Agencia Española de Protección de Datos y Agencia Estatal Boletín Oficial del Estado.

LOZA CORERA, María (2017): “De los microdatos a los datos masivos. Cuestiones legales”, en *Universitat de València*.

LUCKER, John; HOGAN, Susan K. ; BISCHOF, Trevor (2017): “Predictable inaccurate. The prevalence and perils of bad big data”, en *Deloitte Review*, No. 21.

LUEBKE, David Martin; MILTON, Sybil (1994): “Locating the Victim: An Overview of Census-Taking, Tabulation Technology and Persecution in Nazi Germany”, en *16 Annals of the History of Computing*, IEEE, No. 3.

LUHN, Hans Peter (1958): “A business intelligence system”, en *IBM Journal of research and development*, Vol. 2, No. 4, p. 314-319.

MALGIERI, Gianclaudio; COMANDÉ, Giovanni (2017): "Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation", en *International Data Privacy Law*, Vol. 7, No. 4, pp. 243-265.

MANTELERO, Alessandro (2017): "Privacy or the homo digitals in the era of big data and IoT: purpose limitation or legitimate interest? That is the question" conferencia presentada en *CPDP 2017, The age of intelligent machines*.

MANTELERO, Alessandro (2018): "Ciudadanía y gobernanza digital. Entre política, ética y Derecho" en Tomás de la Quadra-Salcedo y José Luis Piñar (dirs.), *Sociedad digital y Derecho*, Madrid, BOE-Red.es.

MANTELERO, Alessandro(2018): AI and big data: A blueprint for a human rights, social and ethical impact assessment, en *Computer Law & Security Review*, Vol. 4, No. 34.

MARIANI, Marcello; et al, (2018): "Business intelligence and big data in hospitality and tourism: a systematic literature review", en *International Journal of Contemporary Hospitality Management*, Vol. 30, No. 12.

MARTIN, Kirsten E. (2015): "Privacy Notices as Tabula Rasa: An Empirical Investigation into How Complying with a Privacy Notice Is Related to Meeting Privacy Expectations Online", en *Journal of Public Policy and Marketing*, Vol. 34, No.2, p. 210–227.

MARTÍNEZ GUTIÉRREZ, Rubén (2019): "Los retos de la innnovación tecnológica en la jurisdicción contencioso administrativa", en Fernando López Ramón y Julián Valero Torrijos (coords.), *20 años de la Ley de lo Contencioso-administrativo: Actas del XIV Congreso de la Asociación Española de Profesores de Derecho Administrativo*, Murcia, Instituto Nacional de Administración Pública (INAP).

MARTÍNEZ MARTÍNEZ, Ricard (2004): *Una aproximación crítica a la autodeterminación informativa*, Madrid, Civitas.

MARTÍNEZ MARTÍNEZ, Ricard (2017): Cuestiones de ética jurídica al abordar proyectos de Big Data. El contexto del Reglamento general de protección de datos, en *Dilemata*, No. 24.

MARTÍNEZ MARTÍNEZ, Ricard (2020): Privacidad de los empleados. Prevención de riesgos y salud pública en la pandemia, Foro APEP.

MARTÍNEZ, Antonio; VAN ELSEN, Filip; et al. (2016): "The EU General Data Protection Regulation", en *Allen & Overy*.

MAYER-SCHÖENBERGER, Viktor; NEIL CUKIER, Kenneth (2013): *Big Data. La revolución de los datos masivos*, 1ª ed, Turner Publicaciones.

MCCRAE, Robert; JOHN, Oliver P. (1992): "An introduction to the five-factor model and its applications", en *Journal of personality*, Vol. 60, No. 2, pp. 175-215.

MENDIETA, Manuel Villoria (2000): *Ética pública y corrupción: Curso de ética administrativa*, Tecnos-Universitat Pompeu Fabra, Madrid, 2000.

MERINO BADA, Cristina y Ricardo Cañizares Sales (2011). *Implantación de un sistema de gestión de seguridad de la información según ISO 27001*, en FC editorial.

MEYER, David (2017): "Inside the ePrivacy Regulation's furious lobbying war", *IAPP blog*, de 31 de octubre.

MICROSOFT AZURE, What is cloud computing? A beginners guide.

MILLER DEVENS, Richard (1868): *Cyclopaedia of Commercial and Business* Anecdotes, D. Appleton.

MILLS, Steve; et al (2012): "Demystifying Big Data. A Practical Guide To Transforming The Business of Government", en *TechAmerica Foundation's Federal Big Data Commission*.

MISLOVE, Alan; et al. (2010): "You are who you know: inferring user profiles in online social networks", en *Proceedings of the third ACM international conference on Web search and data mining*.

MITJANS SERVETO, Maria (2019): “Exercising GDPR data subjects’ rights Empirical research on the right to explanation of news recommender systems”, Master´s thesis, Universidad Católica de Lovaina.

MOEREL, Lokke; PRINS, Corien (2016): “Privacy for the homo digitalis: Proposal for a new regulatory framework for data protection in the light of Big Data and the internet of things”, en *SSRN Electronic Journal*, 2784123.

MORALES BARCELÓ, Judith (2017): “Big data y protección de datos: especial referencia al consentimiento del afectado”, en *Revista Aranzadi de derecho y nuevas tecnologías*, No. 44.

MURILLO DE LA CUEVA, Pablo Lucas (2018): “Constitución y realidad constitucional. Reforma, integración y mutación del texto de 1978” en *Anales de la Real Academia de Ciencias Morales y Políticas*, Nº. 95.

MURILLO DE LA CUEVA, Pablo Lucas (2008): “El derecho a la autodeterminación informativa y la protección de datos personales” en *Azpilcueta: cuadernos de derecho*, No. 20.

MURILLO DE LA CUEVA, Pablo Lucas (2007): “Perspectivas del derecho a la autodeterminación informativa” en *Revista de Internet, Derecho y Política*, No. 5.

MURILLO DE LA CUEVA, Pablo Lucas (2003): “La primera jurisprudencia sobre el derecho a la autodeterminación informativa”, en *Datospersonales.org: La revista de la Agencia de Protección de Datos de la Comunidad de Madrid*, Nº. 1.

MURILLO DE LA CUEVA, Pablo Lucas (1999): “La construcción del derecho a la autodeterminación informativa”, en Revista de estudios políticos, No. 104.

NEIL CUKIER, Kenneth; MAYER-SCHÖENBERGER, Viktor (2013): “The Rise of Big data. How It’s Changing the Way We Think About the World”, en *Foreign Affairs* Vol. 92, No. 3.

NISSEBAUM, Helen (2018): “Stop thinking about consent: it isn’t possible and it isn’t right”, en *Harvard Business Review*.

O'NEIL, Cathy (2016): Weapons of math destruction. How Big Data Increases Inequality and Threatens Democracy, Crown Books.

OOSTVEEN, Manon (2018): *Protecting individuals against the negative impact of big data. Potential limitations of the privacy and data protection law approach*, Kluwer Law International BV.

ORGANIZACIÓN PARA LA COOPERACIÓN Y EL DESARROLLO ECONÓMICOS (1980): Directrices sobre protección de la privacidad y flujos transfronterizos de datos personales, de 23 de septiembre.

PALAZÓN, Javier (2014): "¿Un ordenador en la Antigua Grecia? El misterioso mecanismo de Anticitera", en *Estratos*, No. 107.

PAREJA, Diego (1986) "Instrumentos prehispánicos de cálculo: el quipu y la yupana", en *Revista Integración*, Vol. 4, No. 1.

PARISER, Eli (2011): The filter bubble: What the Internet is hiding from you, Penguin UK.

PASQUALE, Frank (2015): The black box society: The secret algorithms that control money and information, Cambridge, Londres, Harvard University Press.

PECES-BARBA MARTÍNEZ, Gregorio (1987): *Derechos Fundamentales*.

PÉREZ CAMPILLO, Lorena (2019), "Una aproximación al big data y al blockchain sanitario y su implicación en la protección de datos personales", en *Revista de derecho y genoma humano: genética, biotecnología y medicina avanzada*, No. Extra 1.

PHILIPS, Mark (2017): "Criminalizing re-identification: a misstep for big data science and data protection" conferencia presentada en *Computers, Privacy and Data Protection Conference*, Bruselas.

PICKER, Randal C. (2008): "Competition and privacy in web 2.0 and the cloud", en University of Chicago Law & Economics, Olin Working Paper No. 414.

PILAS, Nicolás (2017): “Data protection and data-driven innovation for health care and biomedical research” conferencia presentada en *CPDP 2017, The age of intelligent machines*.

PIÑAR MAÑAS, José Luís (2018): “Derecho e innovación tecnológica. Retos de presente y futuro”, en *CEU Ediciones*.

PIÑAR MAÑAS, José Luís (2018): “Derecho. Ética e innovación tecnológica”, en *Revista española de derecho administrativo*, No. 195.

PIÑAR MAÑAS, José Luís (2017): “Sociedad, innovación y privacidad, Información Comercial Española”, en *ICE: Revista de economía*, No. 897.

PIÑAR MAÑAS, José Luís (2016), “El objeto del Reglamento”, en José Luís Piñar Mañas (dir.), *Reglamento General de Protección de Datos: Hacia un nuevo modelo europeo de privacidad*, Madrid, Reus.

PIÑAR MAÑAS, José Luís (2011): “Administración electrónica y protección de datos personales”, en *Revista Xuridica da Universidade de Santiago de Compostela*, Nº Extra 1.

PIÑAR MAÑAS, José Luis (2010), “Comentario al artículo 3”, en Antonio TRONCOSO REIGADA (Dir.), *Comentario a la Ley Orgánica de Protección de datos de carácter personal*, Civitas Thomson Reuters , Cizur Menor.

PIÑAR MAÑAS, José Luís (2009): “Seguridad, transparencia y protección de datos: el futuro de un necesario e incierto equilibrio. Documento de trabajo 147/2009”, en *Laboratorio de Alternativas, Centro de Estudios Políticos y Constitucionales*.

PIÑAR MAÑAS, José Luís (2008): “¿Existe la privacidad?”, *en CEU Ediciones*.

PIÑAR MAÑAS, José Luís (2005): “El derecho fundamental a la protección de datos personales. Algunos retos de presente y futuro”, en *Asamblea: revista parlamentaria de la Asamblea de Madrid*, No. 13.

PIÑAR MAÑAS, José Luís; GIL, Álvaro Canales (2011): *Legislación de protección de datos*, 2ª ed., Madrid, Iustel.

PIÑOL TORRENT, Francesca (2016): “De la tradición al diseño textil digital”, en *Primer Simposio de la Fundación Historia del diseño*, Barcelona.

PLAZA PENADÉS, Javier (2018): “El nuevo modelo de protección de datos personales europeo y el modo de obtener un consentimiento lícito”, en *Revista Aranzadi de derecho y nuevas tecnologías*, No. 44.

PLAZA PENADÉS, Javier (2018): “El Proyecto de la nueva Ley Orgánica de Protección de Datos de Carácter Personal”, en *Revista Aranzadi de derecho y nuevas tecnologías*, No. 46.

PLAZA PENADÉS, Javier (2018): “Primeras reflexiones desde el Derecho sobre la Inteligencia Artificial”, en *Revista Aranzadi de derecho y nuevas tecnologías*, No. 47.

PLAZA PENADÉS, Javier (2019): “El consentimiento para la instalación de cookies después de la STJUE de 1 de octubre de 2019”, en *Revista Aranzadi de derecho y nuevas tecnologías*, No. 51.

POWER, Daniel J. (2007): *A brief history of decision Support Systems*, Vol. 4.1, DSS Resources.

PURI, Ritika (2015): “Big data and transparency: Why it matters to you”, en *Insider*.

PUYOL MONTERO, Javier (2014): “Una aproximación a big data”, en *Revista de Derecho de la UNED*, No. 14.

PUYOL MONTERO, Javier (2016): “Los principios del derecho a la protección de datos”, en José Luís Piñar Mañas (dir.), *Reglamento General de Protección de Datos: Hacia un nuevo modelo europeo de privacidad*, Madrid, Reus.

RAAB, Charles D.; WRIGHT, David (2012): “Surveillance: Extending the Limits of Privacy Impact Assessment”, en David Wright y Paul de Hert (eds.), *Privacy Impact Assessments*, Dordrecht, Springer;

RAHWAN, Iyad (2018): “Society-in-the-loop: programming the algorithmic social contract”, en *Ethics and Information Technology*, Vol. 20, No. 1.

RALLO LOMBARTE, Artemi (2020): “Una nueva generación de derechos digitales”, en *Revista de estudios políticos*, No. 187.

RALLO LOMBARTE, Artemi (2029): “El nuevo derecho a la protección de datos”, en Revista española de derecho constitucional, No. 116.

RALLO LOMBARTE, Artemi (2017): “El Tribunal de Justicia de la Unión Europea como juez garante de la privacidad en internet”, en Teoría y realidad constitucional, No. 39.

RALLO LOMBARTE, Artemi (2012): “hacia un nuevo sistema europeo de protección de datos: las claves de la reforma”, en Revista de Derecho Político, N.º 85, p. 13-56.

RAVAT, Franck; TESTE, Olivier; TOURNIER, Ronan (2007): “OLAP aggregation function for textual data warehouse”, en *ICEIS*, Vol. 1.

RECIO GAYO, Miguel (2016): *Protección de datos personales e innovación: ¿(In)compatibles?*, Reus, Madrid.

RECIO GAYO, Miguel (2017): “Big data: hacia la protección de datos personales basada en una transparencia y responsabilidad aumentadas”, en *Revista de Derecho, Comunicaciones y Nuevas Tecnologías, Universidad de Los Andes (Colombia)*, No. 17.

REDING, Viviane (2012): “Protección de la privacidad en un mundo conectado. Un marco europeo de protección de datos para el siglo XXI”, en Jorge Pérez y Enrique Badía (coords), *El debate de la privacidad y seguridad en la red: regulación y mercados*, Madrid, Ariel/Telefónica.

REIDENBERG, Joel R., et al (2014): “Privacy Harms and the Effectiveness of the Notice and Choice Framework”, en *I/S: A Journal of Law and Policy for the Information Society*, Vol. 1, No. 2.

RODOTÀ, Stefano (2016): “Internet and Privacy: There Is a Judge in Europe Who Curbs the United States”, en *The Federalist Debate*, No. 1

RODOTÀ, Stefano (2014): *El derecho a tener derechos*, Madrid, Trotta.

RODOTÀ, Stefano (2010): *La vida y las reglas. Entre el Derecho y el no Derecho*, Madrid, Trotta.

RODOTÀ, Stefano (2005): Quale diritto per il nuovo mondo, en *Estudios de derecho civil. Obligaciones y contratos. Libro Homenaje a Fernando Hinestrosa*, No. 3.

RODOTÀ, Stefano (1999): *Repertorio di fine secolo*, 2.ª ed., Editori Laterza, Roma-Bari.

RODOTÀ, Stefano (1997): *Tecnopolítica: La democracia y las nuevas tecnologías de la comunicación*, Roma, Laterza.

RONALD, Koorn; et al (2015): "Big Data Analytics & Privacy: How To Resolve This Paradox".

RUBÍ NAVARRETE, Jesús (2012): "Tratamiento de datos personales. Satisfacción del interés legítimo. Ley de protección de datos. Sentencia Tribunal Supremo, de 8 de febrero de 2012. Sentencia TJUE, de 24 de noviembre de 2011", en *Comunicaciones en Propiedad Industrial y Derecho de la Competencia*, No.66.

RUBINSTEIN, Ira; PETKOVA, Bilyana (2018): "The International Impact of the General Data Protection Regulation", en Marc Cole & Franziska Boehm (eds.), *Commentary on the General Data Protection Regulation*, Edward Elgar.

RUSITSCHKA, Sebnem; RAMÍREZ, Alejandro (2014): "Big Data Technologies and Infrastructures", en *Proyecto Big data roadmap and cross-disciplinary community for addressing societal externalities*, Deliverable D1.4, 2014.

Ryan, CALO (2017): "Artificial Intelligence Policy: A Primer Roadmap" en *UCDL Review*. Vol. 51.

SANCHO LÓPEZ, Marina (2017): "Nuevas amenazas para la protección de datos en el contexto del Big Data*", en Revista Aranzadi de derecho y nuevas tecnologías*, No. 43.

SCHERMER, Bart W.; CUSTERS, Bart; VAN DER HOF, Simone (2014): "The Crisis of Consent: How Stronger Legal Protection May Lead to Weaker Consent in Data Protection", en *Ethics and Information Technology*, Vol. 16, No. 2.

SCHNEIER, Bruce (2015): Data and Goliath: The Hidden Battles to Capture Your Data and Control Your World, WW Norton & Company.

SCHWARTZ, Richard L. (1992), "Internal and external method in the study of law", en *Law and Philosophy*, No.11.

SECUROSIS, L.L.C. (2012): *Securing Big Data: Security recommendations for Hadoop and NoSQL environments*.

SELBST, Andrew D.; POWLES, Julia (2017): "Meaningful Information and the Right to Explanation", en *International Data Privacy Law*, Vol. 7, No. 4.

SENOR, Monica (2018): "La reticenza italiana sul legittimo interesse del titolare quale base giuridica del trattamento di dati personali", en *Blog Medialaws*, 2 de mayo de 2018.

SHARMA, Priya P.; NAVDETI, Chandrakant P. (2014): "Securing Big Data Hadoop: A Review of Security Issues, Threats and Solution", en *International Journal of Computer Science and Information Technologies*, Vol. 5, No. 2.

SIEMS, Mathias M. (2007): *Legal Originality*, Oxford Journal of Legal Studies, Vol. 28.

SOLOVE, Daniel (2006): "A Taxonomy of Privacy", en *University of Pennsylvania Law Review*, Vol. 154.

SOLOVE, Daniel J (2013): "Privacy Self-Management and the Consent Paradox", en *Harvard Law Review*, Vol. 126, No. 7.

SOTO, Yasmina (2017): "Datos masivos con privacidad y no contra privacidad", en *Revista de bioética y derecho*, No. 40.

SRIVASTAVA, Jaideep; DESIKAN, Prasanna; KUMAR, Vipin (2002): *Web mining: Accomplishments and future directions*, National Science Foundation Workshop on Next Generation Data Mining (NGDM'02).

STALLA-BOURDILLON, Sophie; PAPADAKI, Evangelia; CHOWN, Tim. (2015): "Metadata, traffic data, communications data, service use information…What is the difference? Does the difference matter? An interdisciplinary view from the UK", Serge Gutwirth & Ronald Leenes (eds.), *Data Protection on the Move*, Springer.

SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS (2005): *Position paper on the role of Data Protection Officers in ensuring effective compliance with Regulation (EC) 45/2001*, de 28 de noviembre de 2005.

SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS (2011): Dictamen sobre la Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones — Un enfoque global de la protección de los datos personales en la Unión Europea (2011/C 181/01), de 22 de junio.

SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS (2015): Opinion 7/2015, Meeting the challenges of big data, A call for transparency, user control, data protection by design and accountability, de 19 de noviembre.

SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS (2016): Developing a toolkit for assessing the necessity of measures that interfere with fundamental rights.

SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS (2016): Opinion 5/2016, Preliminary EDPS Opinion on the review of the ePrivacy Directive (2002/58/EC), de 22 de julio.

SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS (2016): *What you should know about the Data Protection Officer (DPO)*, de 7 de julio.

SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS (2017): Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit.

TALEB, Nassim Nicholas (2007): The black swan: *The impact of the highly improbable*, Vol. 2, Penguin Random house.

TELEFÓNICA: *Smart steps project*.

THE FUTURE OF PRIVACY FORUM Y NYMITY (2018): Processing Personal Data on the Basis of Legitimate Interests under the GDPR: practical cases.

THE INFORMATION ACCOUNTABILITY FOUNDATION (2017): *Legitimate Interests and Integrated Risk and Benefits Assessment: A Framework for Determining if Processing as Permitted by Legitimate Interests is Legal, Fair and Just*.

TRENTO LAW AND TECHNOLOGY RESEARCH GROUP (2016): *Big Data: Privacy and Intellectual Property in a Comparative Perspective*.

TROIANO, Guglielmo (2015): *General Data Protection Regulation, a complete link collection*.

TRONCOSO REIGADA, Antonio (2019): "La Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales", en *Derecom*, No. 26.

TRONCOSO REIGADA, Antonio (2016): "Autoridades de control independientes", en José Luís Piñar Mañas (dir.), *Reglamento General de Protección de Datos: Hacia un nuevo modelo europeo de privacidad*, Madrid, Reus.

TRONCOSO REIGADA, Antonio (2010*): La protección de datos personales: en busca del equilibrio*, Valencia, Tirant lo Blanch.

TRONCOSO REIGADA, Antonio (2010): "La protección de datos personales. Una reflexión crítica de la jurisprudencia constitucional", en *Cuadernos de Derecho Público*, No. 19-20.UNESCO, WORLD COMMISSION ON THE ETHICS OF SCIENTIFIC KNOWLEDGE AND TECHONOLOGY (COMEST) (2017): *Report on robotics*.

VALERO TORRIJOS, Julián (2013): *Derecho, innovación y Administración electrónica*, Sevilla, Global Law Press.

VALERO TORRIJOS, Julián (2015): "Ciudades inteligentes y datos abiertos: implicaciones jurídicas para la protección de los datos de carácter personal", en I*stituzioni del federalismo rivista di studi giuridici e politici*, No. 4.

VALERO TORRIJOS, Julián (2019): "Las garantías jurídicas de la inteligencia artificial en la actividad administrativa desde la perspectiva de la buena administración", en *Revista catalana de dret públic* No. 58.

VAN DER SLOOT, Bart.: (2016) "International and comparative legal study on Big Data", en *WRR*.

VAN DER SLOOT, Bart; VAN SCHENDEL, Sascha. (2016): "Ten Questions for Future Regulation of Big Data: A Comparative and Empirical Legal Study", en *JIPITEC – Journal of Intellectual Property, Information Technology and E-Commerce Law*, Vol. 7.

VEALE, Michael; EDWARDS, Lilian (2018): "Clarity, Surprises, and Further Questions in the Article 29 Working Party Draft Guidance on Automated Decision-Making and Profiling", en *Computer Law & Sexurity Review*, Vol. 34, No. 2.

VEDDER, Anton (1999): "KDD: The challenge to individualism", en *Ethics and Information Technology*, Vol. 1, No. 4.

VEDDER, Anton (1999): "KDD: The challenge to individualism", en *Ethics and Information Technology*, Vol. 1, No. 4.

VIDA FERNÁNDEZ, José (2018): "Los retos de la regulación de la inteligencia artificial: algunas aportaciones desde la perspectiva europea" en Tomás de la Quadra-Salcedo y José Luis Piñar (dirs.), *Sociedad digital y Derecho*, Madrid, BOE-Red.es.

WACHTER, Sandra (2018): "The GDPR and the Internet of Things: a three-step transparency model" *Law, Innovation and Technology*, Vol. 10, No. 2.

WACHTER, Sandra (2018): “The GDPR and the Internet of Things: a three-step transparency model”, en *Law, Innovation and Technology*, Vol. 10, No. 2.

WACHTER, Sandra; MITTELSTADT, Brent; FLORIDI, Luciano (2016): “Why a right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation”, en *International Data Privacy*, Vol 7, No. 2.

WACHTER, Sandra; MITTELSTADT, Brent; RUSSELL, Chris (2018): “Counterfactual Explanations Without Opening the Black Box: Automated Decisions and the GDPR”, en *Harvard Journal of Law & Technology*.

WARREN Samuel D.; D. BRANDEIS, Louis (1890): “Right to privacy”, en *Harvard Law Review*, Vol. 4, No. 5.

WISE, Alyssa Friend; SHAFFER, David Williamson (2015): **“***Why Theory Matters More than Ever in the Age of Big Data*”, en *Journal of Learning Analytics*, Vol. 2, No. 2.

WRIGHT, David; RAAB, Charles D.: “Constructing a surveillance impact assessment”, en *Computer Law & Security Review*, Vol. 28, No. 6.

ZANFIR, Gabriela (2012): “The Right to Data Portability in the Context of the EU Data Protection Reform”, en *International Data Privacy Law*, Vol. 2, No. 3.

ZANFIR, Gabriela (2014): “Forgetting about consent. Why the focus should be on “suitable safeguards” in data protection law”, en *Reloading Data Protection*, Dordrecht, Springer.

ZANFIR, Gabriela (2019): “10 reasons why the RGPD is the opposite of a ‘notice and consent’ type of law”, en *Medium Blog*.

ZARSKY, Tal (2016): “The Trouble with Algorithmic Decisions: An Analytic Road Map to Examine Efficiency and Fairness in Automated and Opaque Decision Making”, en Scie*nce, Technology & Human Values*, Vol. 41, No. 1.

ZARSKY, Tal (2017): “Incompatible: The GDPR in the Age of Big Data”, en *Seton Hall Law Review*, Vol. 47, No. 2.

ZHENG, Jack G (2018): Business intelligence and analytics: a comprehensive overview.

ZUBOFF, Shoshana (2015): “Big Other: Surveillance Capitalism and the Prospects of an Information Civilization”, en *Journal of Information Technology*, Vol. 30, No.1.

ZUBOFF, Shoshana (2018): The Age of Surveillance Capitalism. The Fight for a Human Future at the New Frontier of Power, Londres, Profile Books.

ZUBOFF, Shoshana (2019): *The age of surveillance capitalism: The fight for a human future at the new frontier of power*, Londres, Profile Books.

ZUIDERVEEN BORGESIUS, Frederik J. (2015): “Personal Data Processing for Behavioural Targeting: Which Legal Basis?”, en *International Data Privacy Law*, Vol. 5, No 3.

ZUIDERVEEN BORGESIUS, Frederik J. (2015): *Improving Privacy Protection in the Area of Behavioural Targeting*, Kluwer Law International BV.

ZUIDERVEEN BORGESIUS, Frederik J.; et al. (2017): “Tracking Walls, Take-It-Or-Leave-It Choices, the GDPR, and the ePrivacy Regulation”, en *European Data Protection Law Review*, Vol. 3, No. 3.

ZUIDERVEEN BORGESIUS, Frederik; et al. (2017): “An assessment of the Commission’s Proposal on Privacy and Electronic Communications”, en *Directorate-General for Internal Policies, Policy Department C: Citizen's Rights and Constitutional Affairs*.

ZWENNE, Gerrit-Jan; KROES Quinten; VAN EYMEREN, Joost (2018): “EPR vis-à-vis GDPR A comparative analysis of the ePrivacy Regulation and the General Data Protection Regulation”, en *Centre for Information Policy Leadership*, de 19 de julio.

Tabla de normas y legislación

AUDIENCIA NACIONAL (2012): Sentencia de 11 de abril. ECLI: ES:AN:2012:1702.

Carta de los Derechos Fundamentales de la Unión Europea, de 18 de diciembre de 2000 (2000/C 364/01).

COMISIÓN EUROPEA (1990): *Proposal for a Council Directive concerning the protection of individuals in relation to the processing of personal data* COM(90) 314 final – SYN 283, (90/C 277/03), de 27 de julio.

COMISIÓN EUROPEA (1990): Proposal for a Council Directive concerning the protection of individuals in relation to the processing of data (COM(90) 314 final), de 27 de julio.

COMISIÓN EUROPEA (2012): *Commission Staff Working Paper. Impact Assessment Accompanying the document Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) and Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data* COM(2012) 10 final, de 25 de enero.

COMISIÓN EUROPEA (2012): *Propuesta de Reglamento del Parlamento Europeo y del Consejo 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)* COM (2012) 11 final – 2012/0011 (COD), de 25 de enero.

Conclusiones del Abogado General presentadas el 26 de enero, Asunto C-13/16, Rïgas. ECLI:EU:C:2017:43.

Conclusiones del Abogado General Sr. Niilo Jääskinen presentadas el 10 de julio de 2014, Asunto C-212/13, Ryneš, ECLI:EU:C:2014:2072.

Conclusiones del Abogado General Sra. Eleanor Sharpston presentadas el 27 de septiembre de 2018, C-345/17, Sergejs Buivids vs Datu valsts inspekcija. ECLI:EU:C:2018:780.

CONSEJO DE EUROPA (1981): Convenio 108, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal.

CONSEJO DE EUROPA (2018): *"Convenio 108" modernizado de 17 de 2018 para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal*.

CONSEJO DE EUROPA (2018): *Modernisation of the Data Protection "Convention 108"*.

CONSEJO DE LA UNIÓN EUROPEA (1992): *Amended proposal for a Council Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data* COM(92) 422 final - SYN 287, de 15 de octubre.

CONSEJO DE LA UNIÓN EUROPEA (2015): *Propuesta de Reglamento del Parlamento Europeo y del Consejo 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) - Preparación de un planteamiento general*, 2012/0011 (COD) 9565/15, de 11 de junio.

CONSEJO DE LA UNIÓN EUROPEA (2018): *Legislative Acts and Other Instruments: Corrigendum/Rectificatif of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*, 19 de abril.

COUNCIL OF EUROPE, COMMITTEE OF MINISTERS (2010): *Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic*

processing of personal data in the context of profiling (Profiling Recommendation), de 23 de noviembre.

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

Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas).

Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006 sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE.

Directiva 2009/136/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009 por la que se modifican la Directiva 2002/22/CE relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas, la Directiva 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas y el Reglamento (CE) No. 2006/2004 sobre la cooperación en materia de protección de los consumidores.

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.

Explicaciones sobre la Carta de los Derechos Fundamentales, de 14 de diciembre de 2007 (2007/C 303/02).

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

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

Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal (LORTAD).

ORGANIZACIÓN PARA LA COOPERACIÓN Y EL DESARROLLO ECONÓMICOS (2002): *Resumen sobre las Directrices de la OCDE sobre protección de la privacidad y flujos transfronterizos de datos personales*.

PARLAMENTO EUROPEO (1992): *Proposal for a Council directive concerning the protection of individuals in relation to the processing of personal data* COM(90) 314 final – SYN 287, (C 94/173), de 11 de marzo.

PARLAMENTO EUROPEO (2014): *Resolución legislativa del Parlamento Europeo, de 12 de marzo de 2014, sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo 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)* (COM(2012)0011 — C7-0025/2012 — 2012/0011(COD)), de 12 de marzo.

Propuesta de Reglamento del Parlamento Europeo y del Consejo, de 10 de enero de 2017 sobre el respeto de la vida privada y la protección de los datos personales en el sector de las comunicaciones electrónicas y por el que se deroga la Directiva 2002/58/CE (Reglamento sobre la privacidad y las comunicaciones electrónicas.

Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

Reglamento (CE) 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos.

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

Reglamento (UE) 2018/1807 del Parlamento Europeo y del Consejo, de 14 de noviembre de 2018, relativo a un marco para la libre circulación de datos no personales en la Unión Europea.

Reglamento 2018/1725, de 23 de octubre de 2018, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos, y por el que se derogan el Reglamento (CE) No. 45/2001 y la Decisión No. 1247/2002/CE.

TJUE, asuntos acumulados C-203/15 y C-698/15 *Tele2 Sverige AB y Secretario de Estado del Ministerio del Interior,* ECLI:EU:C:2016:970.

Tribunal Constitucional Federal de Alemania, Sentencia de 15 de diciembre de 1983.

TRIBUNAL CONSTITUCIONAL, Sentencia 290/2000 de 30 de noviembre.

TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA (2008): Asunto C-524/06, Huber, de 16 de diciembre. ECLI:EU:C:2008:724.

TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA (2010): Asuntos acumulados C-92/09 y C-93/09, Volker und Markus Schecke y Eifert, de 9 de noviembre. ECLI:EU:C:2010:662.

TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA (2010): Asuntos acumulados C-92/09 y C-93/09 Volker und Markus Schecke and Eifert, de 9 de noviembre. ECLI:EU:C:2010:662.

TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA (2011): Asuntos acumulados C-468/10 y 469/10 ASNEF y FECEMD, de 24 de noviembre. ECLI:EU:C:2011:777.

TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA (2014) Digital Rights Ireland Ltd, asuntos C-293/12 y C-594/12.

TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA (2014): Asunto C-131/12, Google Spain SL, Google Inc v Agencia Española de Protección de Datos (AEPD), Mario Costeja González, de 13 de mayo.

TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA (2014): asunto C-212/13, Ryneš, de 11 de diciembre. ECLI:EU:C:2014:2428.

TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA (2015): Asunto C-362/14, Maximillian Schrems v Data Protection Commissioner, de 6 de octubre.

TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA (2016): Asunto C-582/14 Patrick Breyer v Germany, de 19 de octubre. ECLI:EU:C:2016:779.

TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA (2017): Asunto C-13/16, Rīgas, de 4 de mayo. ECLI:EU:C:2017:336.

TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA (2017): Asunto C-131/12, Google Spain y Google, de 13 de mayo. ECLI:EU:C:2014:317.

TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA (2017): Asunto C-398/15, Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce vs Salvatore Manni, 9 de marzo. ECLI:EU:C:2017:197.

TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA (2017): Asunto C-434/16, Peter Nowak vs Data Protection Commissioner, de 20 de diciembre. ECLI:EU:C:2017:994.

TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA (2018): Asunto C-210/16, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein vs Wirtschaftsakademie Schleswig-Holstein GmbH, de 5 de junio ECLI:EU:C:2018:388.

TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA (2018): Asunto C–25/17, Tietosuojavaltuutettu vs Jehovan todistajat, de 10 de julio. ECLI:EU:C:2018:551

TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA (2019): Asunto C-345/17, Sergejs Buivids vs Datu valsts inspekcija, de 14 de febrero. ECLI:EU:C:2019:122.

TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA (2019): Asunto C-40/17, Fashion ID GmbH & Co. KG vs Verbraucherzentrale, de 29 de julio. ECLI:EU:C:2019:629.

TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA (2019): Asunto C-673/17, Planet49 GmbH, de 1 de octubre. ECLI:EU:C:2019:801.

TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA (2019): Asunto C-708/18, TK vs Asociaţia de Proprietari bloc M5A-ScaraA, de 19 de diciembre. ECLI:EU:C:2019:1064.

TRIBUNAL EUROPEO DE DERECHOS HUMANOS (1983): Sentencia 5947/72, Silver y otros v Reino Unido, de 25 de marzo.

TRIBUNAL SUPREMO (1943): Sentencia de 10 de julio.

CEU
Escuela Internacional
de Doctorado

TESIS DOCTORAL

ELENA GIL

GONZÁLEZ

2020