El valor del dato en la economía digital

Mª Mercedes Serrano y Mª Celia Fernández Aller

Documento de Trabajo 21/2020

Mª Mercedes Serrano

Es doctora en Derecho y profesora de Derecho Constitucional de la UCLM. Secretaria Departamento de Ciencia Jurídica y Derecho Público. Coordinadora Máster MUAB- Campus de Albacete. El derecho a la protección de datos de carácter personal constituye una de sus líneas principales de investigación desde la elaboración de sus tesis doctoral sobre el tema. Tiene diversas publicaciones en relación con la protección de datos (libros y artículos). Ha impartido cursos, jornadas, seminarios, participado como ponente en congresos en relación con el tema, del que destaca su estudio como derecho fundamental y sus implicaciones en materia de salud pública e investigación en salud.

Mª Celia Fernández Aller

Doctora en Derecho y profesora de la ETSISI (Escuela Técnica Superior de Ingeniería en Sistemas Informáticos) de la Universidad Politécnica de Madrid (UPM). Su línea de investigación son las interrelaciones entre las TIC y los derechos humanos. Varias publicaciones sobre la materia. Pertenece al grupo de investigación de organizaciones sostenibles (GIOS) en la UPM. Profesora visitante en la UCA de El Salvador y de la Facultad de Derecho de la Universidad de Bristol. Es Secretaria de la Junta Directiva de ONGAWA, Ingeniería para el Desarrollo Humano. Adscrita al ITD UPM, Centro de Innovación en tecnología para el desarrollo humano de la Universidad Politécnica de Madrid. Pertenece a un Consejo Asesor de la Fundación Alternativas.

Impreso en papel ecológico

Maquetación: Clara Román Jiménez
ISBN: 978-84-121118-8-0

RESUMEN EJECUTIVO

La **revolución digital** es una de las seis grandes transformaciones que los expertos consideran claves para la consecución de los Objetivos de Desarrollo Sostenible. En esta revolución, el papel del Big Data resulta esencial. Con dicho término se hace referencia al "conjunto de tecnologías, algoritmos y sistemas empleados para recolectar datos a una escala y variedad no alcanzada hasta ahora y a la extracción de información de valor mediante sistemas analíticos avanzados soportados por computación en paralelo" [1]. Con base en este conocimiento generado se podrán tomar mejores decisiones.

El **Big Data puede suponer un cambio de paradigma en diferentes campos del conocimiento**. Ese cambio de paradigma se centra en el abandono de la causalidad como criterio central y su sustitución por la correlación. Esto puede generar dificultades en la explicabilidad de las decisiones que se tomen basadas en algoritmos de Big Data, que están siendo utilizados para los usos más diversos, como el mejor conocimiento del cliente, del mercado, la personalización de productos o servicios mediante la creación de perfiles, la mejora en la toma de decisiones, la previsión del comportamiento o la monetización.

Centrándonos en el caso del Big Data para la elaboración de perfiles, existen riesgos como la reidentificación (conseguir identificar al sujeto a pesar de la anonimización), las consecuencias discriminatorias (que afectan a individuos) o las correlaciones espurias (conclusiones que, aparentemente están relacionadas, pero que en realidad no tienen ninguna relación, lo cual hace necesario reforzar la explicabilidad de los algoritmos tal y como prevé el artículo 13 del Reglamento Europeo de Protección de Datos).

[1] Para más detalles sobre la tecnología, vid. AGPD, ISMS FORUM. Emilio Aced, M. Rosario Heras, Carlos Alberto Saiz, Código de buenas prácticas en protección de datos para proyectos Big Data, http://www.aepd.es%2Fmedia%2Fguias%2Fguia-codigo-de-buenas-practicas-proyectos-de-big-data.pdf&usg=AOvVaw26Z-N52gvhV_kk3_Xr8kVy

Adicionalmente, el contexto de la **gobernanza de los datos personales** ha sufrido un cambio radical con el desarrollo de las tecnologías Big Data. El impacto inicial se ha producido por la gran cantidad de información generada y que tiene que ser almacenada. Además, hay que tener en cuenta la naturaleza heterogénea de su contenido. Se manejan datos de tipo estructurado tradicionales, pero también información de toda la actividad producida por los usuarios, como audio, video, imágenes, conversaciones, que son muy difíciles de tratar con las herramientas que existían anteriormente. La gobernanza de los datos tiene un peso muy importante en cualquier proyecto de ingeniería, en especial si los datos son personales.

La rapidez con la que se tienen que almacenar unida a esa extensión en su tipología, hace muy difícil que los procesos de verificación y calidad utilizados hasta ahora sean totalmente eficaces, por lo que es necesario crear nuevas metodologías y herramientas adecuadas. Y para esto, es fundamental que toda la organización se involucre en la obtención, análisis y comprensión de los datos y de la información disponible.

El Big Data plantea **retos muy urgentes en el ámbito de la privacidad** cuando los datos que se utilizan son datos personales referidos a personas físicas. La privacidad es uno de los derechos fundamentales claves en nuestro contexto actual, puesto que juega un papel esencial en el ejercicio de otros derechos y libertades en el difícil equilibrio de poder de los Estados y actores privados. Sin privacidad, ni internet ni las tecnologías de tratamiento de información personal pueden funcionar en el marco de nuestras sociedades democráticas.

Cuando el tratamiento de Big Data afecta a datos personales, las normas vigentes sobre protección de datos son aplicables, tratando de hacer compatible la libre circulación y utilización de dicha información con el derecho fundamental a la protección de datos personales. Dos elementos entre los que habrá que encontrar el equilibrio jurídico que permita la cohabitación, sin perjuicio para ninguno de ellos.

El Big Data, por el tratamiento masivo de información que supone, puede representar un riesgo para los derechos de los ciudadanos, debido a la falta de transparencia, las dificultades para solicitar consentimiento en el caso de un tratamiento que no se preveía en el momento de la recogida de los datos, o el desequilibrio en la información entre las empresas o el poder público que tratan datos personales y las personas cuyos datos se tratan.

La transparencia obliga a facilitar información sobre el tratamiento de los datos, "sobre qué información se recolecta, cómo se procesa, con qué propósito serán utilizados y si será transferida a terceros"[2] y acerca del ejercicio de los derechos, esto es, los derechos de acceso, rectificación, cancelación y en especial el derecho de oposición al tratamiento por medio de Big Data, que es el arma jurídica adecuada para quedar fuera de un tratamiento de datos cuando no se ha consentido la utilización posterior de los datos ante la existencia de finalidades compatibles con la primera que permiten el tratamiento.

El papel del consentimiento, como elemento que legitima el tratamiento de datos personales con Big Data, ha de complementarse con la insistencia en las medidas de seguridad previstas en el Reglamento General de Protección de Datos europeo, teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos y gravedad que entraña el tratamiento para los derechos y libertades del sujeto. Algunas medidas propuestas por el legislador europeo son la realización de un análisis de riesgo (que ha de llevar a cabo todo tratamiento de datos) y una Evaluación de Impacto en la Protección de Datos (EIPD).

El Big Data debe prever los riesgos posibles y su gestión. La EIPD pretende minimizar el riesgo para los derechos y libertades de los sujetos (art. 35 RGPD) y actuar frente a él. La referencia a los derechos y libertades de los interesados debe entenderse básicamente a los derechos a la protección de datos y a la intimidad, pero también pueden verse implicados otros derechos fundamentales como "la libertad de expresión, la libertad de pensamiento, la libertad de

[2] 36ª Conferencia Internacional de Autoridades de Protección de Datos.

circulación, la prohibición de discriminación, el derecho a la libertad y la libertad de conciencia y de religión".

Adicionalmente, se debe llevar a cabo un registro de actividades de tratamiento con toda la información que recoge el art. 30 RGPD, así como reforzar, en el caso del Big Data, los principios de Privacidad desde el diseño y por defecto.

Es imprescindible una responsabilidad proactiva, esto es, la implicación en cuanto al cumplimiento de las normas y la protección de los derechos de todos los sujetos interesados en el tratamiento de Big Data, incorporación de mecanismos internos y externos de comprobación de la seguridad de los tratamientos y la posibilidad de demostrar su cumplimiento. El valor de los datos debe ir parejo a la asunción de responsabilidad por parte de quienes los manejan.

Otro requisito es el nombramiento de un Delegado de Protección de Datos (DPD) y el establecimiento de mecanismos internos de solución de quejas o reclamaciones de los interesados, rápido y sencillo. El DPD será nombrado por el responsable del tratamiento y por el encargado (art. 37 RGPD) y deberá participar de forma adecuada en todas las cuestiones relativas a la protección de datos (art. 38.1 RGPD). De entre las funciones del DPD que pueden tener una incidencia mayor en el tratamiento de Big Data destacan:

- Actuar como medio de contacto con los interesados en lo que respecta a las cuestiones relativas al tratamiento de datos personales y al ejercicio de sus derechos. Se puede diseñar un mecanismo interno ante el DPD cuyo objetivo sea resolver las reclamaciones de los sujetos afectados de un modo rápido, sencillo y eficaz;
- informar y asesorar al responsable o al encargado del tratamiento y a los empleados de las obligaciones que derivan del RGPD y de la legislación vigente;

- supervisar el cumplimiento del RGPD, incluida la formación y concienciación del personal que participa en las operaciones de tratamiento;
- En definitiva, la nueva normativa de protección de datos tiene mecanismos para evitar algunos riesgos del Big Data sobre los derechos de las personas. Es necesario, sin embargo, extremar el rigor en la aplicación de los mismos, lo cual conlleva dificultades en la práctica.

Un derecho del titular de los datos que se ha consagrado en la última reforma europea de protección de datos, y que resulta clave en este estudio, es el **derecho a la portabilidad**. Este derecho constituye una parte esencial del objeto del derecho a la protección de datos: permitir el control de los datos personales por parte del sujeto. Con el derecho a la portabilidad se refuerza el control del interesado sobre sus datos de carácter personal que están en manos de un responsable. Pero el derecho a la portabilidad también facilita la libre circulación de los datos en el mercado único digital, pues al permitir el paso de datos de un proveedor a otro mejorará el movimiento de los datos, la competencia, la innovación y la oferta de servicios. Incorpora por tanto un altísimo valor económico y de libre mercado, aunque su regulación normativa, no olvidemos, no persigue ni mejorar la competitividad ni mantenerlo como recurso económico, sino favorecer el control de la persona sobre sus datos, lo que da prioridad a este aspecto frente a cualquier otro.

El derecho a la portabilidad habilita al interesado a recibir los datos personales que previamente haya entregado a un responsable de tratamiento y transmitirlos a otro responsable de tratamiento, o bien, en segundo lugar, a permitir un traspaso directo de datos de responsable a responsable[3]. Los datos se han de entregar en un formato estructurado, de uso común y lectura mecánica. Esta última exigencia obligará a los responsables de los tratamientos de Big Data a desarrollar medios que permitan el ejercicio del derecho a la portabilidad pues, de otro modo se convertiría en una facultad ineficaz para el derecho a la protección de datos.

[3] El WG 29 recomienda la incorporación de herramientas de descarga de datos e interfaces de programación de aplicaciones, Directrices sobre el derecho a la portabilidad de los datos, pág. 3

El derecho a la portabilidad de los datos tiene lugar en tratamientos basados en el consentimiento del sujeto, por tanto, es el consentimiento el que legitima la portabilidad de los datos o bien las obligaciones derivadas de un contrato.

Con la finalidad de facilitar el ejercicio de este derecho se está impulsando el ***Data Transfer Project*** (20 de julio de 2018, creado por Google, Microsoft, Twitter y Facebook, Apple), que así mismo amplía el mercado para las empresas, al permitir "rutas de intercambio de datos"[4]. El DTP tiene como objetivo permitir que las personas puedan transmitir sus datos entre proveedores de servicios en línea a través de un marco común, que incluye protocolos de datos para facilitar la transferencia directa de datos dentro y fuera de los proveedores de servicios en línea participantes, lo cual no está exento de riesgos para los derechos de los sujetos.

Algunas medidas que se plantean para evitar estos riesgos son, entre otras: a) Poner al usuario en el centro e intentar que las herramientas de portabilidad de datos sean fáciles de encontrar e intuitivas de usar; b) Privacidad y seguridad, de forma que los responsables de la transacción de los datos, el responsable que posee los datos y el responsable al que se le transfieren, deben adoptar medidas de seguridad para garantizar la protección de los datos, de manera que se evite el acceso no autorizado, o el desvío de datos a otros proveedores; c) Reciprocidad: el ejercicio de la portabilidad no puede ir en detrimento del derecho a la protección de datos, en el sentido de impedir que el sujeto siga manteniendo el control sobre sus datos de carácter personal y el tratamiento de los datos pueda seguir siendo transparente. El ejercicio del derecho a la portabilidad no es finito y los datos pueden ser portados de nuevo, siempre que para el sujeto se mantengan las garantías en todo momento del proceso; d) centrarse en los datos del sujeto: los datos objeto de la portabilidad son los datos personales que se refieren a la persona, y los datos que ésta haya facilitado a un responsable del tratamiento; e) Respeto entre todos: la portabilidad debe respetar los datos de los demás sujetos y nunca ejercerse de manera que se puede perjudicar a las personas vinculadas con el solicitante del derecho a la portabilidad. Por eso, el cumplimiento del derecho a la

[4] Como lo ha denominado Dans, Enrique, https://www.enriquedans.com/2018/07/data-transfer-project-dtp-que-es-y-para-que-sirve.html

portabilidad no podrá afectar negativamente a los derechos y libertades de otro u otros sujetos.

En definitiva, y dado el valor económico de los datos, el reto será poner a los ciudadanos en el centro de las estrategias de negocio, de forma que no pierdan el control sobre su información personal. Encontrar el equilibrio entre los datos como valor económico y como valor jurídico protegible es uno de los mayores retos que tenemos hoy día.

Los retos que plantea la tecnología del Big Data en nuestra sociedad son enormes, tanto en el ámbito ético, como económico, social, jurídico o tecnológico. Se exponen a continuación recomendaciones que se extraen del estudio:

Con base en las principales conclusiones de este informe, el documento formula algunas **recomendaciones** que debieran ser tenidas en cuenta en la utilización y diseño del Big Data.

- Debido a que los principales riesgos del Big Data para la protección de datos y la privacidad se refieren a la cantidad ingente de información que se recoge y sobre la que se elaboran perfiles, la primera recomendación está relacionada con la inclusión de estas preocupaciones desde la fase de diseño de la tecnología. La adopción del principio de ***e*** es muy relevante. Se recomienda analizar los ejemplos de buenas prácticas que puedan guiar a los diferentes actores (gobiernos, instituciones privadas, etc.) en el logro de estos objetivos. En este sentido, la utilización de Estudios de Impacto en la privacidad son altamente recomendables.

- La **transparencia y la información** son elementos primordiales en el tratamiento de Big Data. Dado que el consentimiento es un principio que se verá modulado en el tratamiento masivo de la información, -pero que nada justifica su desaparición-, tanto por el propio acto de consentir como por su ligazón con el principio de finalidad, es recomendable y

necesario incorporar mecanismos de acceso, de transparencia, de información a través de las páginas web corporativas del centro, del correo electrónico, etc. con el fin de mantener el Big Data en los márgenes de la legalidad y de la ética. Igualmente, para compensar las deficiencias que puede presentar el principio del consentimiento ligado a la finalidad (recuérdese finalidades compatibles con la inicialmente consentida) habrá que contemplar la posibilidad de ejercitar con facilidad y sencillez el derecho de oposición, para el interesado que no desee formar parte de un tratamiento masivo de datos personales.

- Se recomienda **invertir en medidas de seguridad tecnológicas y organizativas** que han de ser permanentemente evaluadas y actualizadas, con el fin de responder a los continuos retos que plantean las TIC. Las medidas de seguridad deben garantizar la confidencialidad, la integridad, la disponibilidad, la transparencia. En este sentido, las normas ISO 27000, como estándares internacionales, pueden ser un buen punto sobre el que empezar a trabajar.

- La **política de educación y formación permanente especializada** debe ser una prioridad, dirigida a todo el personal que trabaja con datos de carácter personal, con el fin de implicar a la empresa, entidad u organización. La formación en principios éticos y jurídicos es esencial. El personal que gestiona y trata los datos para obtener información debe asumir desde el principio de su tarea que maneja elementos propios del contenido de un derecho fundamental y que deben actuar con la debida responsabilidad.

- Ha de asegurarse la existencia y cumplimiento de un **régimen de rendición de cuentas**, que incluya disposiciones de responsabilidad para garantizar que las entidades que recogen, tratan y ceden datos son responsables en caso de abuso, de forma que no sean los usuarios en los que a menudo recaiga dicha responsabilidad. En este sentido, es deseable que se desarrollen más las pólizas de seguros que compensen el

comportamiento responsable de la seguridad y la protección adecuada de los datos personales.

- Es importante que se regulen las cuestiones de privacidad y protección de datos a nivel internacional, con el establecimiento de una **autoridad independiente**. Posiblemente el ámbito de Naciones Unidas sea uno de los que más impacto podrían tener. A pesar de las dificultades del multilateralismo en los últimos años, no hay otro ámbito que goce de más consenso, y capaz de liderar procesos de la importancia de la Agenda 2030.

- Muy relacionado con lo anterior, urge que se aclaren adecuadamente los **roles y las responsabilidades** de aquellos que manejan datos personales en todas y cada una de las fases de utilización de la tecnología. Es importante que las personas con responsabilidad en las organizaciones estén implicadas en los asuntos de *compliance*.

- Se recomienda la elaboración de **códigos de conducta**, tal y como recoge el art. 40 RGPD. El código de conducta es una herramienta que ayuda a la aplicación de los principios y derechos del RGPD (así como de la LOPDGDD) al sector en el que proyecte su actividad el Big Data. El código de conducta además de cumplir con la función de dar transparencia e información del tratamiento de datos al interesado servirá al responsable y al encargado del tratamiento para demostrar que han respetado todas las obligaciones exigidas para la protección de los derechos de los interesados, incluyendo medidas de seguridad, privacidad desde el diseño y por defecto, observancia del principio del consentimiento, finalidad, etc. El DPD es también un elemento que ha de tener un alto valor en el tratamiento en Big Data.

Sin embargo, nunca la existencia de un código de conducta puede sustituir el papel de una legislación jurídicamente exigible que garantice un marco protector de los derechos. El establecimiento de sanciones económicas ha sido siempre un factor que ayuda en el cumplimiento de las normas de convivencia.

La voluntariedad de los códigos de conducta ha de complementarse con la aprobación de normativa suficiente y específica que resuelva los interrogantes que existen hoy día.

- Un asunto clave es la extensión de una **cultura de la protección de datos,** para generar confianza entre los ciudadanos que entregan sus datos de carácter personal. La confianza y la seguridad del sujeto en que sus datos van a ser tratados de forma adecuada y con el respeto a sus derechos facilitará la dación de datos, lo que repercutirá en un tratamiento más extenso de los mismos, esto es, mayor volumen de información, por tanto, de negocio y de valor económico. Para ello es recomendable también dar publicidad a todos los documentos elaborados para garantizar los derechos de los interesados especialmente de la EIPD y del código de conducta.

- Es muy urgente que se ponga suficiente atención a las **políticas de sensibilización** en torno a la importancia de la privacidad y los retos que plantea el Big Data. Si estas cuestiones se convierten en temas importantes para la ciudadanía, ésta presionará suficientemente a los gobiernos para desarrollar propuestas normativas que son necesarias[5].

- El **principio de no discriminación** es esencial si se pretende la garantía de los derechos humanos de cualquier persona. Las soluciones de Big Data deben ajustarse a este principio, impidiéndose que las decisiones que se tomen generen brechas digitales que dejen al margen de los avances a minorías y personas vulnerables[6], como personas con discapacidad, mayores, en situación de desventaja económica, infancia, etc.

- Resulta esencial incluir la **perspectiva ética** en cualquier decisión de Big Data. La creación de grupos de trabajo transdisciplinares es clave

[5] "Large-scale societal change is often achieved first in the hearts and minds of the people, and only afterwards accepted in legislation and economic policies", Sachs, J.D, Schimidt-Traub, G, Mazzucato, M, Messner, D, Nakicenovic, N, Rockstrom, J. "Six transformations to achieve the Sustainable Development Goals". *Nature Sustainability.* 2019, p.8

[6] Eusbanks, V. "La automatización de los prejuicios". *Investigación y Ciencia,* 2019.

para conseguir que los valores éticos estén asegurados en las fases de diseño, implementación, uso y evaluación de las tecnologías Big Data.

ÍNDICE

INTRODUCCIÓN: GENERACIÓN DE VALOR EN EL MERCADO A PARTIR DEL TRATAMIENTO DE DATOS PERSONALES, EL NUEVO ECOSISTEMA DIGITAL

La revolución digital es una de las seis grandes transformaciones que los expertos consideran claves para la consecución de los Objetivos de Desarrollo Sostenible[7]. Nos situamos en la cuarta revolución industrial, que incorpora la ubicuidad de la tecnología digital en la vida diaria y la fusión creciente entre los mundos físico, biológico y digital[8]. Los avances tecnológicos clave incluyen el Big Data, la nanotecnología, biotecnología, Internet de las cosas, ingeniería genética, impresoras 3D, informática cuántica[9], 5G, computación en nube, inteligencia artificial (robótica, aprendizaje automático)

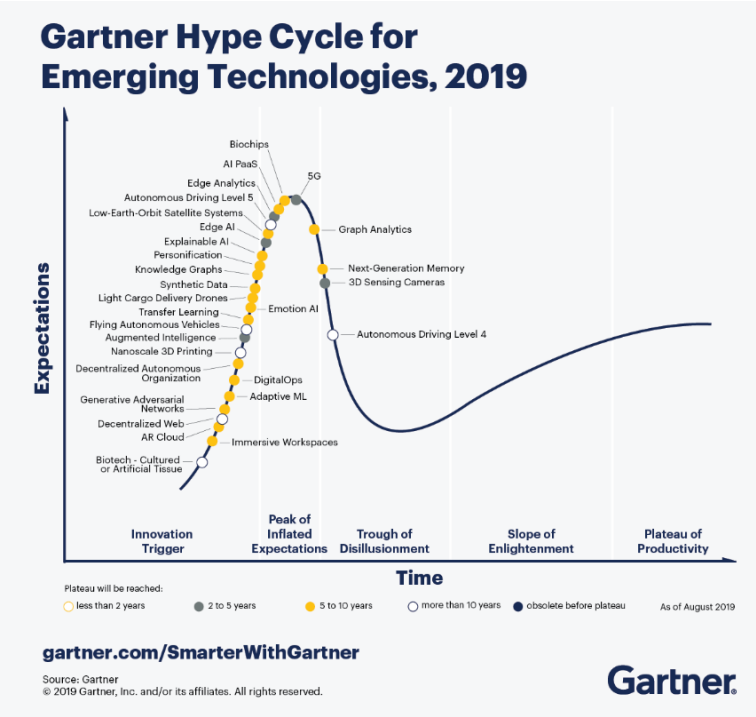
En este contexto, en el que la velocidad del cambio tecnológico es cada vez más vertiginosa, como puede observarse en las previsiones de algunas empresas fiables, merece la pena ahondar en una de las tecnologías, Big Data, para conocer en qué consiste exactamente y las implicaciones éticas, sociales y de impacto en los derechos humanos que trae consigo.

[7] Sachs, J.D, Schimidt-Traub, G, Mazzucato, M, Messner, D, Nakicenovic, N, Rockstrom, J. "Six transformations to achieve the Sustainable Development Goals". *Nature Sustainability.* 2019

[8] El concepto de "digital twin" es un exponente de esta idea, y está utilizándose en la actualidad con mucha frecuencia.

[9] Véase Juskalian, Russ (2017): «TR10: Ordenadores cuánticos funcionales». MIT Technology Review. Disponible el 20/05/2017 en https://www.technologyreview.es/s/6818/tr10- ordenadores-cuanticos- funcionales

FIGURA 1: Ciclo de Tecnologías Emergentes



Fuente: Gartner

Algunos datos que pueden ayudar a entender el contexto son, por ejemplo:

- Un Smartphone tiene más capacidad de procesamiento que la NASA cuando llegó a la luna.
- IoT está aumentando el volumen de datos disponibles desde los dispositivos, y se calcula que en 2020 habrá más de 200.000 millones de objetos conectados.
- El volumen de datos que existe no puede tratarse con el software convencional
- Los datos se procesan a velocidades inimaginables hace años
- Existe una variedad de datos, puesto que provienen de diversas fuentes
- Se aspira a la veracidad de esos datos, extrayendo solamente los de alta calidad
- Se utilizan sólo los datos relevantes para cada uso concreto que puedas rentabilizar: Valor de los datos

- Y además, el significado de los datos cambia frecuentemente y se pueden producir inconsistencias que se deben gestionar de forma adecuada. Es lo que se denomina variabilidad.

Al Big Data frecuentemente se le caracteriza mediante tres 'v': Volumen, Variedad y Velocidad:

- **Volumen** es la característica más obvia y que recoge el propio nombre de Big Data. Se pasa de manejar magnitudes de megabytes, gigabytes, como mucho Terabytes, a manejar Petabytes[10] de forma cada vez más frecuente.

- Su **Variedad** ha crecido exponencialmente, tanto por la tipología de datos como por sus fuentes. Se ha pasado de manejar datos estructurados en bases de datos procedentes, en su mayoría, de fuentes internas de la propia organización, a tratar datos estructurados, semiestructurados y desestructurados[11]; de ser datos cuasi estáticos a datos dinámicos o en continuo cambio; de originarse en un número de fuentes limitadas a proceder de personas, máquinas, sensores, etc. Esta variedad y volumen requieren un tratamiento diferente para poder convertirse en información.

- La **Velocidad** es la tercera 'v'. La captura, movimiento y proceso de los datos se hace a gran velocidad, llegando a ser en tiempo real en algunos casos.

A estas características se han unido también las de **Veracidad**, extrayendo los de alta calidad, y **Valor**, dada la importancia de sacar a la luz los datos relevantes para cada uso concreto que se pueda rentabilizar.

[10] 15 bytes

[11] Los datos estructurados tienen perfectamente definido la longitud, el formato y el tamaño de sus datos. Se almacenan en formato tabla, hojas de cálculo o en bases de datos relacionales. Los datos no estructurados son un conglomerado masivo y desorganizado que no tienen valor hasta que se identifican y almacenan de forma organizada en bases de datos.

El Big Data permite hoy día obtener datos estructurados y no, procesarlos y cargarlos en varias fuentes distribuidas. Cuando están estructurados, el análisis es más rápido. Datos de gran tamaño se distribuyen en varios procesadores. Para analizar los datos, el Big Data utiliza algoritmos, pudiendo emplear diferentes ramas de la IA. Por último, se extrae el valor de los datos en forma de patrones de comportamiento, predicciones de compra o identificación de nuevas oportunidades de negocio.

En síntesis, con dicho término se hace referencia al "conjunto de tecnologías, algoritmos y sistemas empleados para recolectar datos a una escala y variedad no alcanzada hasta ahora y a la extracción de información de valor mediante sistemas analíticos avanzados soportados por computación en paralelo"[12]. Con base en este conocimiento generado se podrán tomar mejores decisiones.

El Big Data puede suponer un cambio de paradigma en diferentes campos del conocimiento. Ese cambio de paradigma se centra en el abandono de la causalidad como criterio central y su sustitución por la correlación (Ricardo Morte Ferrer, 2017). Como consecuencia de ello, se pierde capacidad explicativa, los sesgos se vuelven relevantes y pueden aparecer como consecuencia de los propios datos utilizados en el origen.

Conviene mencionar que hay autores han calificado la época del Big Data como una "época sin razón" y que han comparado el boom en torno al Big Data con el que se produjo desde el Siglo XVII en torno a la estadística (Han, Byung Chul, 2014).

El Big Data aporta valor de diversas formas: por un lado, permite correlaciones inesperadas, basadas en análisis estadísticos de datos históricos. Esto puede aportar información muy relevante y valiosa, por ejemplo, en el ámbito de la Medicina (una correlación inesperada entre dos variables hasta ahora desconocidas puede salvar vidas).

[12] Para más detalles sobre la tecnología, vid. AGPD, ISMS FORUM. Emilio Aced, M. Rosario Heras, Carlos Alberto Sáiz, Código de buenas prácticas en protección de datos para proyectos Big Data, http://www.aepd.es%2Fmedia%2Fguias%2Fguia-codigo-de-buenas-practicas-proyectos-de-big-data.pdf&usg=AOvVaw26Z-N52gvhV_kk3_Xr8kVy

Por otro lado, si nos centramos en el ámbito de los procesos industriales, antes los fenómenos que sucedían se explicaban por leyes físicas. Ahora, sin embargo, las cosas se averiguan de forma más eficiente (pensemos en el ámbito de la monitorización predictiva: se puede contar con información sobre cuándo ha de arreglarse determinado sistema eléctrico con más precisión, rapidez, eficacia...). En este caso, la explicación de por qué ha de hacerse o no un determinado arreglo no puede explicarse fácilmente, simplemente se sabe, como consecuencia de la correlación de información, que es así.

En definitiva, esta tecnología[13] tiene potencial para tratar volúmenes ingentes de datos –muchos de ellos personales- y desarrollar inferencias y correlaciones, teniendo aparejados enormes posibilidades de progreso y a la vez retos importantes para la privacidad y la protección de datos personales a los que hay que hacer frente: por ejemplo, las técnicas de anonimización de datos, la necesidad de realizar una evaluación de impacto de privacidad (PIAS), que es un requisito del RGPD en relación el tratamiento de datos a gran escala; la necesidad de contar con un delegado de protección de datos, en adelante, DPO; los requisitos del profiling y de las decisiones individuales automatizadas.

Se hace imposible tratar los datos con las herramientas de bases de datos y analíticas convencionales. Nuestro entorno genera mucha información diaria (proliferación de páginas web, aplicaciones de imagen y vídeo, redes sociales, dispositivos móviles, apps, sensores del internet de las cosas), se calcula que más de 2.5 quintillones de bytes al día. De hecho, el 90% de los datos a nivel mundial se han creado en los dos últimos años.

Este fenómeno se ha sido descrito como "la revolución que cambiará nuestras vidas" (Mayer Schönberger y Cukier, 2013). Es evidente que uno de los motivos esenciales por los que existe tanta atención, y tanta expectación, en torno al Big Data se debe a su potencial desde el punto de vista económico.

[13] Otro concepto relacionado que se maneja es el de *data lake* o lago de datos, en tanto que no sólo se trata de un almacenamiento de propósito específico de bajo coste y gran volumen, sino que se eleva a una agrupación o conglomerado de datos compartida por toda la organización en la que todo tipo de datos son accesibles simultáneamente por una variedad de motores de análisis sin apenas fricción.

Cuando las aplicaciones de Big Data tienen como objetivo identificar posibles pautas de comportamiento de una persona o grupo de personas, esto puede hacerse de diversos modos: a) Analizar la posibilidad de un comportamiento determinado en relación con diferentes tipos de contratos (*scoring*). b) Acumular datos en principio inconexos con el fin de crear un perfil detallado de una persona o de un grupo de personas (*profiling*). c) Valorar diferentes características de una persona, como pueden ser su estado de salud, sus gustos o su fiabilidad (*personalizing*). d) Seguir a una persona en base al rastro que deja, por ejemplo en Internet (*tracking*).

Parece evidente que estas actividades traen consigo diferentes riesgos, que algunos autores llaman "dictadura *smart*" (Welzer, 2016). Conviene recordar que muchas tecnologías han sido ya implementadas sin que se hayan llevado a cabo estudios previos sobre los posibles peligros para los derechos fundamentales y sin que existan políticas adecuadas de seguridad informática para esas nuevas aplicaciones y productos.

El Big Data se ha convertido en imprescindible para gobiernos y empresas; tiene importantes aplicaciones en el tráfico (comportamiento de conductores), marketing (gustos de consumidores y cómo evolucionan), política (influencia en la tendencia de voto), energía (monitorización predictiva), sistemas financiero, salud (posibilidad de decodificar cadenas de ADN en minutos).

Pero el aumento de la cantidad de datos generados también implica aumentar la capacidad de protección para evitar fugas no deseadas de la información. Para dar una solución a esta nueva problemática, entidades reguladoras y comisiones de privacidad de todo el mundo han elaborado normativas, conscientes de que siempre queda algún ámbito sin proteger. Con la entrada en vigor del Reglamento General de Protección de Datos el pasado 25 de mayo de 2018[14] adelante, RGPD, las organizaciones se enfrentan a sanciones importantes si continúan sin tomar responsabilidad de todos los datos personales, así como de la protección de los mismos.

[14] 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). Unión Europea. «DOUE» núm. 119, de 4 de mayo de 2016. Última modificación: sin modificaciones Referencia: DOUE-L-2016-8980

La cantidad de datos se expandió de 130 exabytes en 2005 a 1.227 en 2010. Si tuviésemos que usar DVDx para mover los datos que existen globalmente en 2010 haría falta una flota de más de 16 millones de jumbo jets[15].

Los expertos del ámbito tecnológico señalan que la gobernanza de los datos supone hoy día hasta un 50% del tiempo que se dedica a los proyectos. Por este motivo, urge que las decisiones se tomen de forma multidisciplinar, incorporando a los equipos de decisión expertos del ámbito ético, jurídico y social, que ayuden a poner en los centros de decisión las preocupaciones en torno a los derechos de las personas.

Por otro lado, tal y como llevan tiempo advirtiendo algunos gurús del ámbito tecnológico como Jaron Lanier, a nivel global se constata una falta de gobernanza: hay instituciones nacionales, y algunas supranacionales, pero se evidencia con demasiada frecuencia la imposibilidad de conseguir que instituciones sólidas que actúen a nivel mundial cuando determinados actores vulneran la privacidad, la libertad de elección política, la dignidad de las personas[16].

"No hay nadie en el mundo que tenga la foto completa de quién está recogiendo datos personales sobre quién" (Jaron Lanier)

El contexto de la gobernanza de la protección de los datos personales, entendida como el conjunto de metodologías, políticas y herramientas que permiten la gestión de los datos personales y de la información para asegurar su calidad, su control y explotación según los objetivos estratégicos definidos dentro de una empresa u organización y el cumplimiento de la normativa sobre esta materia, ha sufrido un cambio radical con el desarrollo de las tecnologías Big Data.

[15] Kuner, Christopher,. Cate, Fred H, Christopher Millard, and Dan Jerker B. Svantesson "The challenge of 'big data' for data protection" *International Data Privacy Law* (2012), Vol. 2, No. 2.

[16] Facebook´s Role in Brexit.
https://www.ted.com/talks/carole_cadwalladr_facebook_s_role_in_brexit_and_the_threat_to_democracy?language=en

El impacto inicial se ha producido por la gran cantidad de información generada y que tiene que ser almacenada. Además, se une a ese gran volumen la naturaleza heterogénea de su contenido. Se manejan datos de tipo estructurado tradicionales, pero también información de toda la actividad producida por los usuarios, como audio, video, imágenes, conversaciones, que son muy difíciles de tratar con las herramientas que existían anteriormente.

La rapidez con la que se tienen que almacenar unida a esa extensión en su tipología, hace muy difícil que los procesos de verificación y calidad utilizados hasta ahora sean totalmente eficaces, por lo que es necesario crear nuevas metodologías y herramientas adecuadas. Y para esto, es fundamental que toda la organización se involucre en la obtención, análisis y comprensión de los datos y de la información disponible.

Estas tareas no pueden quedarse sólo en las áreas de sistemas de información y de inteligencia de negocio. Todos los miembros de la organización deben ver el dato como un valor en sí mismo, y tienen que tener en cuenta, desde los primeros momentos de la definición de un producto, servicio o proceso, cómo conseguir la información adecuada, cómo almacenarla, cómo usarla para mejorar el propio servicio o proceso, y cómo analizarla posteriormente.

1. El concepto de privacidad como necesidad humana versus protección de datos como idea funcional. La importancia de la nueva regulación de protección de datos en el Big Data

Tal y como conceptualizan la privacidad Friedewald y otros autores[17], si se entiende ésta desde una visión simplificada, no figura en el puesto más elevado de la pirámide de necesidades humanas de Maslow. La privacidad se situaría detrás de otras necesidades básicas como el alimento, refugio o seguridad personal. Desde esta perspectiva, sacrificar la privacidad estaría justificado en determinadas ocasiones. Sin embargo, desde una perspectiva

[17] Friedewald, Michael , Johann Cas, Rocco Bellanova J. Peter Burgess, Walter Peissl. *Surveillance, Privacy and Security: Citizens' Perspectives.* Routledge, 2017.

formal de los derechos humanos, estos son universales, irrenunciables e indivisibles, no pudiendo someterse a ninguna jerarquización.

Es cierto que el artículo 8 de la Convención Europea de Derechos Humanos establece algunos motivos de restricción de la privacidad, como la seguridad pública, el interés nacional, la prevención del crimen o la protección de los derechos de terceros. No obstante, las decisiones que justificarían las limitaciones a la privacidad requieren, según los expertos, un análisis individual sobre la adecuación, necesidad y proporcionalidad de las medidas (Bagger , Tranberg, 2011).

La privacidad no sólo es uno de los derechos fundamentales claves en nuestro contexto actual, sino que juega un papel esencial en el ejercicio de otros derechos y libertades y para equilibrar el poder de los estados y actores privados. Sin privacidad, ni internet ni las tecnologías de tratamiento de información personal pueden funcionar en el marco de nuestras sociedades democráticas. En este sentido se entiende la privacidad como idea funcional.

Como ya se ha estudiado, el Big Data aporta ventajas en la reutilización masiva de los datos que ya han sido recabados en un momento anterior, pero existen riesgos para la protección de las personas. La amenaza se cierne sobre el derecho a la protección de datos (a la privacidad) y sobre los derechos de la persona, como la intimidad, el honor, la libertad, etc.

El Big Data puede utilizar datos de carácter personal. La utilización de datos de carácter personal que permitan identificar al sujeto al que se refieren somete el Big Data a las normas vigentes de protección de datos que pretenden proteger a las personas físicas en lo que respecta al tratamiento de sus datos personales y garantizar, al mismo tiempo, la libre circulación y utilización de dicha información. Dos elementos entre los que habrá que encontrar el equilibrio jurídico que permita la cohabitación, sin perjuicio para ninguno de ellos. El Big Data, por el tratamiento masivo de información que supone, puede representar un riesgo para los derechos de los ciudadanos, entre otras cuestiones características del Big Data por la falta de transparencia que puede desprenderse de este último y por el desequilibrio en la información entre las

empresas o el poder público que tratan datos personales y las personas cuyos datos se tratan.

El empleo de datos de carácter personal somete el Big Data a la observancia de las leyes de protección de datos, tanto por la recogida de los datos como por su tratamiento, con el fin de desmontar el desequilibrio señalado por medio del ejercicio de los derechos por parte del sujeto interesado y con la implementación de procesos de transparencia en el tratamiento de los datos. La transparencia nos lleva a insistir en el cumplimiento del derecho a la información acerca de todas las circunstancias recogidas en el art. 13 RGPD, en especial la finalidad del tratamiento, aspecto este último que en el Big Data puede quedar diluido por su propia naturaleza de reutilización de la información. Sobre el derecho a la información insistiremos más adelante.

Junto a ello hay que referirse a la aplicación del consentimiento, al principio de finalidad del tratamiento, a la existencia de un plazo de conservación de los datos, a cuestiones relativas a la recogida de la información no directamente del sujeto, a la posibilidad de ejercicio de los derechos por parte del interesado, a la implantación de las medidas de seguridad para evitar y mitigar, en su caso, las amenazas a los derechos de los interesados y la cumplimentación de los documentos necesarios para minimizar y controlar el riesgo que lleva incorporado el tratamiento de la información personal.

El Big Data puede trabajar también con datos seudonimizados[18], lo que no excluye la aplicación de la normativa indicada, pues el riesgo de identificación en estas circunstancias no está absolutamente eliminado[19]. En este caso deberemos aplicar medidas de seguridad que impidan que un tercero pueda, por medio de un acceso a otro tipo de información, proceder a la reidentificación de los sujetos. No obstante, se debe contemplar siempre la posibilidad de que el sujeto se oponga al tratamiento de sus datos, salvo que el interesado alegue

[18] El art. 4.5 RGPD define la seudonimización como "el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable"

[19] El considerando 28 RGPD señala que "La aplicación de la seudonimización a los datos personales puede reducir los riesgos para los interesados afectados y ayudar a los responsables y a los encargados del tratamiento a cumplir sus obligaciones de protección de los datos. Así pues, la introducción explícita de la <<seudonimización>> en el presente Reglamento no pretende excluir ninguna otra medida relativa a la protección de los datos

motivos legítimos imperiosos que prevalezcan sobre los derechos y libertades del interesado, o el mantenimiento de los datos sea necesario para la formulación, el ejercicio o la defensa de reclamaciones (art. 21.1 RGPD).

Un supuesto diferente es la anonimización, que por desvincular de manera total la información personal del titular al que se refieren, constituye una modalidad de tratamiento de datos que deja de estar sometido a la legislación de protección de datos[14]. El WP29 o Comité Europeo de Proteccion de Datos y la propia AEPD tienen recomendaciones al respecto, detallándose técnicas de anonimización.

Se trata de que responsables y encargados de tratamiento tengan una guía sobre cómo abordar procesos de anonimización sobre conjuntos de datos. Tal y como recuerda la Agencia Española de protección de datos, en una realidad en la que fuentes de datos independientes se interconectan y que, por diseño, pueden compartir atributos comunes, cabe la posibilidad de crear un rastro electrónico de los individuos, incluso cuando se hayan suprimido los datos que explícitamente les identifican, pudiendo llegar a establecerse vínculos entre dichas fuentes de información y constituir así una amenaza para la privacidad de los interesados cuyos datos están sujetos a tratamiento. En aplicación del principio de Responsabilidad Proactiva establecido en el Reglamento (UE) 2016/679 General de Protección de Datos, el responsable debe abordar el estudio del riesgo inherente de reidentificación de los sujetos de los datos e implementar las medidas para gestionarlo. El objetivo de dicho análisis es alcanzar un balance correcto entre la necesidad de obtener unos resultados con una determinada fidelidad y el coste que el tratamiento puede tener para los derechos y libertades de los ciudadanos. La AEPD ofrece un procedimiento de k-anonimidad, que evita estas reidentificaciones.

El consentimiento, de acuerdo con el art. 4.11 RGPD, ha de ser un consentimiento voluntario, específico, informado, inequívoco y libre. Por tanto, observar el requisito de la transparencia, así como el de la información resultan esenciales en el momento de recabar el consentimiento. La información debe incluir obviamente la posibilidad de ejercicio de los derechos de la protección de datos. Sobre el consentimiento, la información y la transparencia volveremos

más adelante.

El art. 6 RGPD contempla otras bases jurídicas diferentes del consentimiento para legitimar un tratamiento de datos de carácter personal, lo cual ha generado algunas preocupaciones en el mundo académico y en el de la sociedad civil. Una de estas bases jurídicas es el caso de que el tratamiento esté basado en un contrato o relación negocial, aunque esta circunstancia es poco probable que puede tratarse a través del Big Data, pues precisamente la finalidad del Big Data suele ir más allá desde sus inicios que el cumplimiento de las necesidades derivadas de un contrato o una relación negocial. La base jurídica del cumplimiento de un interés público o en el ejercicio de poderes públicos amparados por el Derecho de la Unión o de los Estados miembros puede tener alguna incidencia mayor en el caso del Big Data, por ejemplo, en el campo de la salud pública, la investigación científica, o la atención sanitaria, valorando la posibilidad, dentro del concepto de interés público, de poder reutilizar los datos para finalidades diferentes de las inicialmente consentidas. Por ejemplo, en el campo de la salud pública poder reutilizar los datos existentes en poder de la Administración sanitaria para atención sanitaria o social, al amparo de un interés público esencial y previsto en el Derecho. Igualmente se puede legitimar un tratamiento de datos al margen de consentimiento para satisfacer intereses legítimos perseguidos por el responsable del tratamiento o un tercero siempre que no prevalezcan los intereses o los derechos y libertades fundamentales del interesado[20]. El WP 29 ha incluido como intereses prevalentes "el derecho a la información y la libertad de expresión, las actividades de marketing o publicidad, prevención del fraude o mal uso de servicios, seguridad, finalidades científicas, estadísticas o de investigación"[21]. El Big Data puede aplicarse también a fines estadísticos, que no son incompatibles con las finalidades iniciales, lo que salva uno de los mayores obstáculos con los que puede encontrarse un tratamiento de datos a través del Big Data. En realidad, los fines estadísticos arrojan como resultado, tras trabajar con datos personales,

[20] El WP 29 (Grupo de Trabajo del Artículo 29 hasta la entrada en vigor del RGPD) en el Dictamen 06/2014 ha establecido un conjunto de criterios con el fin de determinar la prevalencia de un interés sobre otro y que deberían ser incluidos en los documentos de impacto que el responsable lleve a cabo, entre los que destacan: la existencia de un interés legítimo del responsable o del tercero que defienda dicho interés, el impacto que el tratamiento tenga sobre el interesado, la naturaleza de los datos objeto de tratamiento y la forma de dicho tratamiento, el desequilibrio entre el responsable del tratamiento y el interesado

[21] Código de buenas prácticas en protección de datos para proyectos de Big Data, disponible en https://www.aepd.es/media/guias/guia-codigo-de-buenas-practicas-proyectos-de-big-data.pdf, pág. 11.

incluidos los seudonimizados, un conjunto de datos agregados que facilitan la toma de decisiones. Dichas decisiones no podrán fundamentar una decisión que afecte a una persona en concreto, conexión que parece difícil de probar. En general, en relación con las bases jurídicas diferentes del consentimiento habrá que efectuar un análisis caso por caso, pues la propia dinámica del Big Data favorece y permite la reutilización de los datos para finalidades diferentes de las que originariamente justificaron la recogida de los datos, salvo que el Big Data se mantenga siempre en la misma finalidad, por ejemplo, como hemos visto, la satisfacción de un interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento.

Durante todo el proceso de reutilización de los datos a través del Big Data han de tenerse presentes todos los principios relativos al tratamiento (art. 5 RGPD). De entre todos los principios que recoge la norma son especialmente significativos en el tratamiento de Big Data el principio de finalidad, el de minimización de los datos y el principio de conservación. Por supuesto sin dejar de lado los principios de licitud del tratamiento, la exactitud y actualización de los datos y su seguridad.

El principio de finalidad establece que las finalidades han de ser determinadas, explícitas y legítimas. Los datos no serán tratados de manera incompatible con las finalidades iniciales. El respeto al principio de especificación de finalidad es uno de los elementos sobre los que llama la atención la 36a Conferencia de Autoridades de Protección de Datos. La determinación de la finalidad de un tratamiento de datos desde el inicio es un severo inconveniente a respetar en el Big Data, por lo que se ha insistido en la idea de finalidades incompatibles, lo que avala la utilización de los datos a través de Big Data para finalidades diferentes de las iniciales, aunque manteniendo la vinculación a través del concepto de compatibilidad, que ha sido objeto de interpretación por el WG 29 de acuerdo con la regulación del art. 6.4 RGPD sobre los factores a tener en cuenta para determinar la compatibilidad entre la finalidades iniciales y posteriores[22]. En relación con la compatibilidad

[22] El art. 6.4 RGPD señala para tener en cuenta: "a) cualquier relación entre los fines para los cuales se hayan cogido los datos personales y los fines del tratamiento ulterior previsto; b) el contexto en que se hayan recogido los datos personales, en particular por lo que respecta a la relación entre los interesado y el responsable del tratamiento; c) la

de las finalidades puede ser determinante para la protección de los interesados la seudonimización de los datos, pues de esta manera se garantiza mejor la protección de los sujetos. En cualquier caso, el sujeto podrá ejercitar, tras ser informado oportunamente del cambio de finalidad, su derecho de oposición al tratamiento de sus datos para la finalidad que, aun siendo compatible con la primera, no ha sido inicialmente consentida.

Otro de los principios significativos en un contexto de Big Data es el de minimización de los datos, según el cual solamente se recogerán y tratarán los datos que sean adecuados, pertinentes y limitados a lo necesario en relación con los fines del tratamiento[23] La recogida masiva de datos y de diferentes fuentes precisamente facilita todo lo contrario, es decir, una recogida de datos sin filtro y sin limitación, lo que provocaría el incumplimiento de este principio de limitación de datos a lo estrictamente necesario para cumplir la finalidad perseguida. La responsabilidad en la minimización de datos compete al responsable del tratamiento, ya sea una corporación, una organización o una entidad pública la que realiza el tratamiento de Big Data. En este sentido, dichas entidades pueden realizar revisiones periódicas para verificar el cumplimiento del principio de minimización. Por otro lado, la posibilidad legítima de emplear los datos para finalidades compatibles con la primera no justifica el incumplimiento del principio de minimización ni la recogida de datos pensando en las futuras finalidades, pues en caso de admitir la recogida masiva de datos en dicho supuesto estaríamos vaciando de contenido el principio de minimización.

Sustancialmente unido al principio de adecuación y pertinencia se encuentra el principio de conservación de los datos, solamente por el tiempo necesario para la consecución de la finalidad; transcurrido dicho plazo temporal los datos deben ser eliminados. Tanto el principio de minimización como el principio de conservación constituyen garantías para el interesado acerca del tratamiento de

naturaleza de los datos personales, en concreto cuando se traten categorías especiales de datos personales, de conformidad con el artículo 9, o datos personales relativos a condenas e infracciones penales, de conformidad con el artículo 10; d) las posibles consecuencias para los interesados del tratamiento ulterior previsto; e) la existencia de garantías adecuadas, que podrán incluir el cifrado o la seudonimización".

[23] La 36a Conferencia de Autoridades de Protección de Datos lo recoge así: "Limitar la cantidad de información recolectada y almacenada a un nivel que sea necesario para el propósito legítimo que pretende".

sus datos personales en el entorno de Big Data y cuyo cumplimiento descansa en el responsable del tratamiento. El principio de conservación de los datos en el tratamiento a través de Big Data puede concretarse a través de la normativa sectorial de aplicación en el caso concreto, o en supuesto de la existencia de un código de conducta pueden precisarse en este documento los plazos imprescindibles de conservación de datos atendiendo a la finalidad establecida. También pueden fijarse diferentes plazos para distintas categorías de datos.

Por otro lado, las medidas de seguridad constituyen otro de los elementos significativos a adoptar en el Big Data. Se trata de medidas técnicas y organizativas que habrán de incorporarse tras el análisis de riesgo llevado a cabo, la evaluación de impacto, etc., y a las que aludiremos en otro apartado.

Por último, el tratamiento de datos personales en proyectos de Big Data ha de contemplar también -y por tanto de ello se debe informar al interesado- de la posibilidad de ejercer los derechos de acceso, rectificación, supresión, oposición, portabilidad, limitación y a no ser objeto de una decisión basada solamente en tratamientos automatizados, lo que obliga a implementar herramientas e instrumentos adecuados para el ejercicio de los derechos en el Big Data. En este caso, como se trata de un tratamiento continuado y variable en su finalidad habrá que establecer un sistema de información acerca del ejercicio de los derechos fácil y comprensible para el interesado. En caso de utilizar diversas fuentes para la recogida de datos, de cuya circunstancia hay que informar al interesado, se ha de estar también en disposición de comunicar las fuentes de procedencia de los mismos, aspecto contemplado dentro del ejercicio del derecho de acceso (art. 14.1 g) RGPD.

2. Nuevos modelos de negocio: innovación basada en el uno de los datos VS. privacidad

2.1. Transparencia y consentimiento

El Big Data pone en valor la información personal. Por su propia dinámica el Big Data exige la creación de herramientas adecuadas para la protección de las personas. Todos los miembros de la empresa o negocio que tratan la

información personal en proyecto de Big Data deben ver el dato como un valor en sí mismo, es decir, deben tener la capacidad de gestionar adecuadamente la información. La mejor gestión en la empresa o en la Administración pública se consigue para cada producto o servicio logrando recabar la información adecuada, y a continuación resolviendo las cuestiones sobre cómo guardarla, cómo utilizarla y cómo extraer de ella información posteriormente. Este modelo exacto de tratamiento de datos no está contemplado de manera expresa en el RGPD, pero ello no quiere decir que escape del ámbito de aplicación de la norma. Por otro lado, el uso correcto de los datos de todos los sujetos que manejan los datos en cualquier fase del tratamiento exige una labor de formación permanente y actualizada sobre el tratamiento de la información de carácter personal.

La falta de discriminación de los sujetos de la empresa o negocio en el tratamiento de la información dificulta la protección de los sujetos y el cumplimento de la normativa de protección de datos. ¿Cómo actuar entonces para no provocar un desequilibrio entre los poseedores de la información masiva y los interesados de los que se almacena dicha información? El consentimiento de los usuarios y la transparencia sobre cómo se emplean los datos y la finalidad perseguida son fundamentales, pero seguramente no serán suficientes para garantizar los niveles de protección de los derechos de las personas que exige un Estado democrático de Derecho. Junto a ello habrán de adoptarse medidas de seguridad que impidan el acceso a los datos por parte de sujetos no autorizados y a seguir procesos de anonimización o seudonimización eficaces, así como cumplimentar los documentos de impacto y análisis de riesgo con el fin de minimizar las amenazas que el tratamiento entraña para los derechos de los sujetos. Vayamos a ello.

La transparencia obliga a facilitar información sobre el tratamiento de los datos, "sobre qué información se recolecta, cómo se procesa, con qué propósito serán utilizados y si será transferida a terceros"[24] y acerca del ejercicio de los derechos, esto es, los derechos de acceso, rectificación, cancelación y en especial el derecho de oposición al tratamiento por medio de Big Data, que es el

[24] 36a Conferencia Internacional de Autoridades de Protección de Datos

arma jurídica adecuada para quedar fuera de un tratamiento de datos cuando no se ha consentido la utilización posterior de los datos ante la existencia de finalidades compatibles con la primera que permiten el tratamiento. Sobre los derechos habrá que "dar a las personas acceso apropiado a los datos que han sido recolectados sobre ellas y a la información y decisiones que se hayan tomado con esos datos. Las personas deben ser avisadas de la fuente de sus datos personales y, cuando sea apropiado, de su derecho a corregir su información, así como de las herramientas para controlar esta información"[25].
El consentimiento va ligado a una determinada finalidad que es la que persigue el responsable con el tratamiento de los datos personales, aunque ya sabemos de las particularidades en la finalidad en el Big Data. La finalidad explícita, determinada y legítima, de la que además se ha de informar al sujeto, constituye el punto más frágil del Big Data, en la medida en que la finalidad de este último es maleable. De hecho, el Big Data permite una reutilización de datos personales para varios fines que no siempre se pueden determinar desde el principio del tratamiento, lo que además dificulta la transparencia. Para salvaguardar este importante escollo legal, habría que contemplar la posibilidad de utilizar los datos para finalidades no incompatibles con la finalidad que justificó la recogida de los datos, lo que no impide que no se puedan utilizar para finalidades diferentes de la inicial, o bien utilizar con finalidades relacionadas con la primera, es decir, lo esencial es poder establecer una conexión entre las finalidades[26].

Además, persiste el deber informar del cambio de finalidad, si no pudo estar prevista desde el inicio. La compatibilidad de los usos ha sido analizada por el WP 29 señalando un conjunto de criterios que han de valorarse para poder determinar la compatibilidad entre los fines iniciales y los posibles fines posteriores[27].

[25] 36a Conferencia Internacional de Autoridades de Protección de Datos
[26] Por ejemplo, en el ámbito de la investigación en salud pública, la Disposición adicional 17a, de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos vestigación en salud pública, la Disposición adicional 17a, de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, indica que "se considera lícita y compatible la reutilización de datos personales con fines de investigación en materia de salud y biomédica cuando, habiéndose obtenido el consentimiento para una finalidad concreta, se utilicen los datos para finalidades o áreas de investigación relacionadas con el área en la que se integrase científicamente el estudio inicial", lo que no excluye la adopción de otras medidas dirigidas a proteger los derechos de los sujetos
[27] El WP 29 ha señalado los siguientes criterios: Debe existir una relación entre la finalidad original y la finalidad o finalidades ulteriores; el tratamiento ulterior debe encontrarse dentro de las expectativas razonables del interesado; ha de tenerse en cuenta la naturaleza de los datos objeto de tratamiento y la sensibilidad de los mismos; debe considerarse

La transparencia va indisolublemente unida a la información. Información sobre el uso de los datos, el destino, la finalidad, el responsable, las medidas de seguridad, el ejercicio de los derechos. El derecho a la información contempla la comunicación al interesado de todas las circunstancias señaladas en el art. 13 RGPD [28] y tras la información transmitida se podrá consentir de manera informada y consciente. La transparencia en cuanto a la información al sujeto titular de los datos se completa con todos los elementos incluidos en el art. 13.1 y 13.2 RGPD y en el 14.1 y 14.2 RGPD cuando los datos no se hayan obtenido directamente del sujeto. En el tratamiento de Big Data habrá que instaurar un sistema que permita una información permanente y duradera; por ejemplo, a través de la página web del centro corporativo o empresa que utiliza el Big Data o a través del correo electrónico.

Respecto al ejercicio de los derechos, la transparencia y la información demandan al Big Data una especial atención al acceso a los datos por parte del sujeto, así como a las decisiones que se han adoptado en base a esos datos. Por ello se recomienda informar a las personas de las fuentes de donde se han recogido los datos y del acceso, así como del derecho a corregirlos. La transparencia exige igualmente informar de los insumos y de los criterios utilizados para la realización de un perfil. Esta información debe presentarse de forma clara, sencilla y comprensible. La elaboración de perfiles y los algoritmos en que se basen necesitan una valoración continua, esto es, precisan "revisiones regulares para verificar si los resultados de la creación de perfiles son responsables, justos y éticos y si son compatibles y proporcionados con el propósito para el cual los perfiles son usados...Siempre debe estar disponible

---

el impacto que este tratamiento va a tener en los interesados; deben aplicarse medidas de protección por parte del responsable como medidas técnicas organizativas, encriptación, seudonimización, separación funcional, transparencia, oposición al tratamiento, en el Dictamen 03/2013 del GT29 sobre la limitación de la finalidad, 13/EN WP 203, adoptado el 2 de abril de 2013,
http://ec.europa.eu/justice/data-protection/article-29/documentation/opinionrecommendation/files/2013/wp203_en.pdf?wb48617274=39E0E409

[28] La información del art. 13.1 y 13.2 RGPD es una información que se suministra por capas. El responsable del tratamiento le facilitará al sujeto la siguiente información: la identidad y los datos de contacto del responsable o de su representante, los datos de contacto del DPD, los fines del tratamiento y la base jurídica en la que se basa, los intereses legítimos del responsable del tratamiento, los destinatarios o las categorías de destinatarios en su caso, las transferencias internacionales previstas. Además, para que el tratamiento sea transparente se aportará la siguiente información: el plazo de conservación de los datos, la existencia del derecho de acceso, rectificación o supresión, limitación, oposición y portabilidad, si el tratamiento se basa en el consentimiento el derecho a retirarlo en cualquier momento, el derecho a presentar una reclamación ante la autoridad de control, si la comunicación de datos es un requisito legal o contractual, la existencia de decisiones automatizadas, incluida la elaboración de perfiles. Los elementos del art. 14.1 y 14.2 RGPD son similares.

una valoración manual de resultados"[29].

Sin embargo, el consentimiento explícito y la transparencia han de ser reforzados por otros elementos presentes también en la legislación de protección de datos, bajo el riesgo, de no hacerlo, de disminuir la protección debida a los interesados:

- Insistir en las medidas de seguridad desde el diseño y por defecto (art. 25 RGPD) teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos y gravedad que entraña el tratamiento para los derechos y libertades del sujeto. El precepto señalado menciona expresamente la seudonimización, la minimización, plazo de conservación de los datos y la accesibilidad, esto es, "garantizar que los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas".

- Realizar un análisis de riesgo (que ha de llevar a cabo todo tratamiento de datos) y una Evaluación de Impacto en la Protección de Datos (EIPD)[30]. Big Data debe identificar todos los riegos posibles y prever su gestión. La EIPD pretende minimizar el riesgo para los derechos y libertades de los sujetos (art. 35 RGPD) y actuar frente a él. La referencia a los derechos y libertades de los interesados debe entenderse básicamente a los derechos a la protección de datos y a la intimidad, pero también pueden verse implicados otros derechos fundamentales como "la libertad de expresión, la libertad de pensamiento, la libertad de circulación, la prohibición de discriminación, el derecho a la libertad y la libertad de conciencia y de religión"[31].

[29] Recomendaciones de la 36a Conferencia Internacional de Autoridades de Protección de Datos.
[30] Para la elaboración de una EIPD se recomienda seguir las indicaciones de la AEPD, Guía práctica para las evaluaciones de impacto en la protección de los datos sujetas al RGPD, https://www.aepd.es/media/guias/guia-evaluaciones-de-impacto-rgpd.pdf
[31] Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento <<entraña probablemente un alto riesgo>> a efectos del Reglamento (UE) 2016/679, adoptadas el 4 de abril de 2017 y revisadas por última vez y adoptadas el 4 de octubre de 2017, pág. 7, disponible en https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236

- Respecto del desarrollo del Big Data, será necesario, para cumplir con la normativa de protección de datos y reforzar el consentimiento y la transparencia, llevar a cabo un registro de actividades de tratamiento con toda la información que recoge el art. 30 RGPD.

- Accountability (responsabilidad proactiva), esto es, la implicación en cuanto al cumplimiento de las normas y la protección de los derechos a todos los sujetos interesados en el tratamiento de Big Data, incorporación de mecanismos internos y externos de comprobación de la seguridad de los tratamientos y la posibilidad de demostrar su cumplimiento. El valor de los datos debe ir parejo a la asunción de responsabilidad por parte de quienes los manejan.

- Nombramiento de un DPD y establecimiento de mecanismos internos de solución de quejas o reclamaciones de los interesados, rápido y sencillo. Vale la pena detenerse en esta garantía personal que ha incorporado como novedad el RGPD. El DPD será nombrado por el responsable del tratamiento y por el encargado (art. 37 RGPD) y deberá participar de forma adecuada en todas las cuestiones relativas a la protección de datos (art. 38.1 RGPD). Los datos del DPD han de ser publicados, pues se trata de una información que ha de constar en el registro de actividades del tratamiento (art. 30.1 a) RGPD). De entre las funciones del DPD que pueden tener una incidencia mayor en el tratamiento de Big Data destacan:

- Actuar como medio de contacto con los interesados en lo que respecta a las cuestiones relativas al tratamiento de datos personales y al ejercicio de sus derechos. Se puede diseñar un mecanismo interno ante el DPD cuyo objetivo sea resolver las reclamaciones de los sujetos afectados de un modo rápido, sencillo y eficaz;

- Informar y asesorar al responsable o al encargado del tratamiento y a los empleados de las obligaciones que derivan del RGPD y de la legislación vigente;

- Supervisar el cumplimiento del RGPD, incluida la formación y

concienciación del personal que participa en las operaciones de tratamiento;

- Ofrecer asesoramiento en la elaboración de la EIPD (art. 38.1 RGPD).

2.2. Innovación basada en el uso de datos, privacidad y requerimientos del RGPD

Cada persona dentro de la organización deberá participar en la comprensión de la información, desde el perfil más técnico al más ejecutivo. Para conseguir la máxima eficacia y valor del dato, se tienen que crear canales de comunicación y un lenguaje común dentro de la organización para forzar y gestionar adecuadamente esta dinámica. Pero la extensión del valor de los datos a toda la organización conlleva un riesgo en la gestión de información confidencial y personal. El reto principal es cómo conseguir que la información más valiosa sea utilizada por las personas más adecuadas sin comprometer la privacidad y confidencialidad de los datos.

Se deben implantar los sistemas de control de acceso, monitorización y anonimización necesarios, para que el análisis se adecúe a las normativas de protección de datos, unido a la creación de políticas preventivas y mitigadoras de riesgos que puedan cubrir aspectos no contemplados por esos mismos marcos legales. Y asociado a este último punto, destaca la gestión del consentimiento de los usuarios y la transparencia sobre cómo se utiliza su información personal. El usuario debe conocer en todo momento, de forma sencilla, qué información personal se utiliza y para qué se utiliza, así como permitir que pueda o no dar su consentimiento, e incluso posteriormente oponerse al tratamiento.

Las organizaciones en sus tratamientos de Big Data tratan de obtener valor, ya sea económico en las organizaciones con ánimo de lucro u ofrecer un mejor servicio en las que no lo tienen.

Aunque el término se ha puesto de moda en los últimos años, se lleva haciendo desde hace bastante tiempo y se pueden encontrar ejemplos

relevantes en el pasado.

Un ejemplo interesante es cómo Wal-Mart, la gran cadena de supermercados de bajo coste de Estados Unidos, distribuyó con anticipación lo que iban a comprar los ciudadanos al acercarse el huracán Katrina. Esta preparación, en base al análisis de qué compraban sus clientes en estos eventos, le permitió estar preparado y poder satisfacer ese pico de demanda atípica.

La elaboración de perfiles permite que los individuos sean categorizados sobre la base de algunas características observables para así poder inferir otras que no son observables.

La categorización puede ser una herramienta muy útil, pero también entraña riesgos de cometer errores al conectar con una persona determinadas características con ciertos comportamientos. Por su parte, también hay riesgo de que los perfiles basados en características como raza, etnia o religión creen estereotipos poco precisos que causen discriminación.

Normalmente, la creación de perfiles se lleva a cabo en varios pasos. En primer lugar, los datos recogidos se anonimizan. En segundo lugar, se utilizan las técnicas de la minería de datos para conectar los datos y buscar correlaciones que logren crear nuevas categorías de información. Por último, se interpretan los resultados para obtener conclusiones y suposiciones sobre el comportamiento de las personas. Esto se lleva a cabo mediante inferencia, en el sentido en que ya ha sido expuesto al tratar sobre la anonimización. En este punto todavía nos encontramos en la primera fase de desarrollo del *Big Data*, tal y como ha sido definida anteriormente. Es decir, se ha creado un modelo a partir del cual se pueden tomar decisiones sobre las personas. Una vez más, cabe destacar que el problema no es la creación del modelo en sí mismo, sino el uso positivo o negativo que se pueda hacer de él en la segunda fase, una vez que se aplica a individuos concretos para categorizarlos.

El RGPD permite hacer estos perfiles sólo en el caso de que existan un contrato, una ley o el consentimiento del interesado.

En general, hay que recordar cuáles pueden ser los riesgos inherentes al tratamiento de Big Data para la elaboración de perfiles[32]:

1. Reidentificación: A pesar de que entre las medidas recomendadas para el tratamiento masivo de datos es aplicar técnicas de disociación apropiadas, tales datos ya anonimizados pueden ser susceptibles de reidentificación. No estamos hablando, en este caso, de reidentificaciones casuales, debidas a errores o falta de calidad en los métodos de disociación empleados, sino del hecho de que se ha demostrado que, aplicando técnicas, ingenio y esfuerzos adecuados, muchos procesos de disociación `pueden llegar a revertirse.

2. Consecuencias discriminatorias: La finalidad de la mayor parte de los tratamientos masivos de datos persigue la búsqueda de patrones, tendencias o perfiles que permiten sacar conclusiones y tomar decisiones en consecuencia. En ocasiones, estas consecuencias afectan directamente a los individuos que han aportado la información y, si esta contuviese cualquier inexactitud, puede acarrear consecuencias negativas para los afectados, por el hecho de ser signados a perfiles sobre los cuales se tomarán decisiones automáticamente. Pero también pueden llegar a afectar a individuos que ni siquiera han participado en la aportación de datos, por el hecho de pertenecer a colectivos extrapolados a partir de los patrones o perfiles obtenidos.

Pensemos en los residentes en un barrio o zona residencial sobre la que se ha obtenido cualquier tipo de perfil en base a la geolocalización de otros sujetos y que se verán afectados por estereotipos o prejuicios.

Un ejemplo real sucedió en Boston, a raíz de la contratación, por parte de la institución pública, de un sistema informático a IBM, que permitía un control en la concesión de ayudas públicas[33].

[32] V

[33] Vid. Virginia Eubanks, Automating Inequality (2018); Cathy O'Neil, Weapons of Math Destruction (2016) y Khiara Bridges, The Poverty of Privacy Rights (2017).

Por otro lado, en octubre de 2019, en su 74 período de sesiones, el Relator Especial de Naciones Unidas en relación a extrema pobreza y derechos humanos, aprobó un informe en el que advierte de que el Estado social digital es una realidad emergente, en la que los sistemas de protección social se gestionan a través de tecnologías como el Big Data para automatizar, predecir, identificar, supervisar, detectar y castigar. Advierte el Relator de que estas tecnologías se utilizan, en ocasiones, en una "zona 0 derechos humanos"[34].

Una muestra de que estos temas son urgentes y relevantes es la propuesta de Ley en EEUU referida a la transparencia de los algoritmos: "Proposed Algorithmic Accountability Act of US" (que busca la regulación de los sesgos en los sistemas de decisión automáticos). Este texto legal permite flexibilidad a las empresas para auditar sus sistemas de aprendizaje automático en un estudio de impacto.

3. Correlaciones espurias: La naturaleza de los análisis masivos de datos facilitan la introducción de sesgos en las conclusiones debido a la confusión que induce en los conceptos de "correlación" y de "causalidad" [35]: Debido al enorme número de datos analizados, pueden aparecer determinadas correlaciones espurias, es decir, conclusiones que, aparentemente, están relacionados, pero que en realidad no tienen ninguna relación de causalidad, tratándose de correlación casual, sin ninguna causa subyacente o explicación. Los algoritmos utilizados en el análisis masivo de datos no son neutrales y pueden ser la causa de las consecuencias discriminatorias antes apuntadas.

En este sentido, se hace necesario reforzar el concepto de "explicabilidad de los algoritmos", para garantizar el principio de transparencia, tal y como dispone el artículo 13 del RGPD:

[34] https://algorithmwatch.org/en/submission-to-the-report-of-the-united-nations-special-rapporteur-%20on-extreme-poverty-and-human-rights/#casestudygermany

[35] El hecho de confundir causalidad con correlación es uno de los peligros de los que alertan los autores hace tiempo: "Aunque ciertas variables muestren poder predictivo, eso no significa que hayamos encontrado un mecanismo que explica lo sucedido" (Moro, Fundación Ramón Areces).

Artículo 13 **Información que deberá facilitarse cuando los datos personales se obtengan del interesado** 1.Cuando se obtengan de un interesado datos personales relativos a él, el responsable del tratamiento, en el momento en que estos se obtengan, le facilitará toda la información indicada a continuación: a) la identidad y los datos de contacto del responsable y, en su caso, de su representante; b) los datos de contacto del delegado de protección de datos, en su caso; c) los fines del tratamiento a que se destinan los datos personales y la base jurídica del tratamiento; 4.5.2016 L 119/40 Diario Oficial de la Unión Europea ES d) cuando el tratamiento se base en el artículo 6, apartado 1, letra f), los intereses legítimos del responsable o de un tercero; e) los destinatarios o las categorías de destinatarios de los datos personales, en su caso; f) en su caso, la intención del responsable de transferir datos personales a un tercer país u organización internacional y la existencia o ausencia de una decisión de adecuación de la Comisión, o, en el caso de las transferencias indicadas en los artículos 46 o 47 o el artículo 49, apartado 1, párrafo segundo, referencia a las garantías adecuadas o apropiadas y a los medios para obtener una copia de estas o al hecho de que se hayan prestado. 2.Además de la información mencionada en el apartado 1, el responsable del tratamiento facilitará al interesado, en el momento en que se obtengan los datos personales, la siguiente información necesaria para garantizar un tratamiento de datos leal y transparente: a) el plazo durante el cual se conservarán los datos personales o, cuando no sea posible, los criterios utilizados para determinar este plazo; b) la existencia del derecho a solicitar al responsable del tratamiento el acceso a los datos personales relativos al interesado, y su rectificación o supresión, o la limitación de su tratamiento, o a oponerse al tratamiento, así como el derecho a la portabilidad de los datos; c) cuando el tratamiento esté basado en el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), la existencia del derecho a retirar el consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a su retirada; d) el derecho a presentar una reclamación ante una autoridad de control; e) si la comunicación de datos personales es un requisito legal o contractual, o un requisito necesario para suscribir un contrato, y si el interesado está obligado a facilitar los datos personales y está informado de las posibles consecuencias de que no facilitar tales datos; f) la existencia de decisiones automatizas, 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. 3.Cuando el responsable del tratamiento proyecte el tratamiento ulterior de datos personales para un fin que no sea aquel para el que se recogieron, proporcionará al interesado, con anterioridad a dicho tratamiento ulterior, información sobre ese otro fin y cualquier información adicional pertinente a tenor del apartado 2. 4.Las disposiciones de los apartados 1, 2 y 3 no serán aplicables cuando y en la medida en que el interesado ya disponga de la información.

Ejemplo de esta obligación de transparencia en relación a los algoritmos es la *Fair Credit Reporting Act* de EEUU, que obliga, por ejemplo, a que, si un banco niega un crédito, se proporcione al solicitante las razones específicas por las cuáles fue rechazado. En este sentido, el caso de la Apple Card de APPLE[36] es un asunto que ha suscitado mucha preocupación recientemente, y que está

[36] https://www.bbc.com/mundo/noticias-50375172

pendiente de resolver por parte de las autoridades competentes. Esta tarjeta de crédito incorpora, presuntamente, sesgos discriminatorios hacia la mujer en la concesión de crédito.

De hecho, la Corte Suprema de Justicia de ese país ya estableció en 2015 que los demandantes solo necesitan demostrar que una política tiene efecto discriminatorio en una clase protegida, y no que la discriminación fue intencional (*Texas Department of Housing and Community Affairs vs. Inclusive Communities Project)*.

Frente a los riesgos expuestos en relación al tratamiento de datos a través de Big Data, la legislación vigente obliga a adoptar un enfoque preventivo y proactivo que analice los datos que se tratan, las finalidades que se persiguen y el tipo de operaciones que se llevan a cabo.

Todo tratamiento de datos, también el Big Data, debe comenzar con un análisis de riesgo. De la valoración acerca del riesgo que el tratamiento de Big Data pueda implicar para los derechos y libertades del interesado dependerán las medidas a adoptar. Si el riesgo que se prevé es elevado, "un alto riesgo", refiere el RGPD, será necesario realizar una EIPD.

En el caso de los tratamientos en proyectos de Big Data resultará coherente elaborar una EIPD, al tratarse de tratamientos que afectarán a un elevado número de sujetos, que previsiblemente realizarán una gran variedad y cantidad de tratamientos, y que realizarán perfiles que servirán para la toma de decisiones (art. 35.3 RGPD). Ante la duda de si es necesario realizar una EIPD para un determinado tratamiento en base al concepto de "alto riesgo", el WP 29 recomienda su elaboración, por la ayuda que este documento representa para el cumplimiento de la legislación de protección de datos[37]. El WP 29 ha analizado los elementos que han de tenerse en cuenta para valorar si el tratamiento entraña un alto riesgo para los derechos y libertades del interesado y en lo que atañe a tratamiento a gran escala del art. 35.3 RGPD, el documento señala un conjunto de criterios a tener en cuenta para determinar si el tratamiento se realiza a gran escala: "a. el número de interesado afectados, bien como cifra

[37] Directrices sobre la evaluación de impacto relativa..., ob. cit., pág. 9

concreta o como proporción de la población correspondiente; b. el volumen de datos o la variedad de elementos de datos que se procesan; c. la duración, o permanencia, de la actividad de tratamiento de datos; d. el alcance geográfico de la actividad del tratamiento"[38]

La EIPD es una "herramienta de carácter preventivo que debe realizar el responsable del tratamiento para poder identificar, evaluar y gestionar los riesgos a los que están expuestos sus actividades de tratamiento al objeto de garantizar los derechos y libertades de las personas físicas"[39]. Para el WP 29 una EIPD[40] "es un proceso concebido para describir el tratamiento, evaluar su necesidad y proporcionalidad y ayudar a gestionar los riesgos para los derechos y libertades de las personas físicas derivados del tratamiento de datos personales evaluándolos y determinando las medidas para abordarlos". El responsable debe prever una adecuada gestión de riesgos y a partir de esa valoración confeccionar la EIPD. Por tanto, la EIPD es previa al inicio del tratamiento de datos, lo que no impide que sea necesario actualizarla durante la vida activa de los datos.

¿Qué elementos debe incluir como mínimo la EIPD? Según el art. 35.7 RGPD, la EIPD ha de incluir, al menos, en primer lugar, una descripción sistemática de las operaciones de tratamiento previstas y de los fines, lo que sabemos que en el Big Data entraña serias dificultades de precisar al inicio del mismo y la base jurídica legítima del tratamiento de los datos. En segundo lugar, una evaluación, es decir, una justificación de la necesidad y proporcionalidad de las operaciones de tratamiento de acuerdo con la finalidad perseguida, esto es, se ha de realizar un juicio de proporcionalidad/ponderación, al que hemos aludido en páginas atrás, para calibrar la constitucionalidad de la medida en relación con el fin previsto. En tercer lugar, una evaluación de los riesgos para los

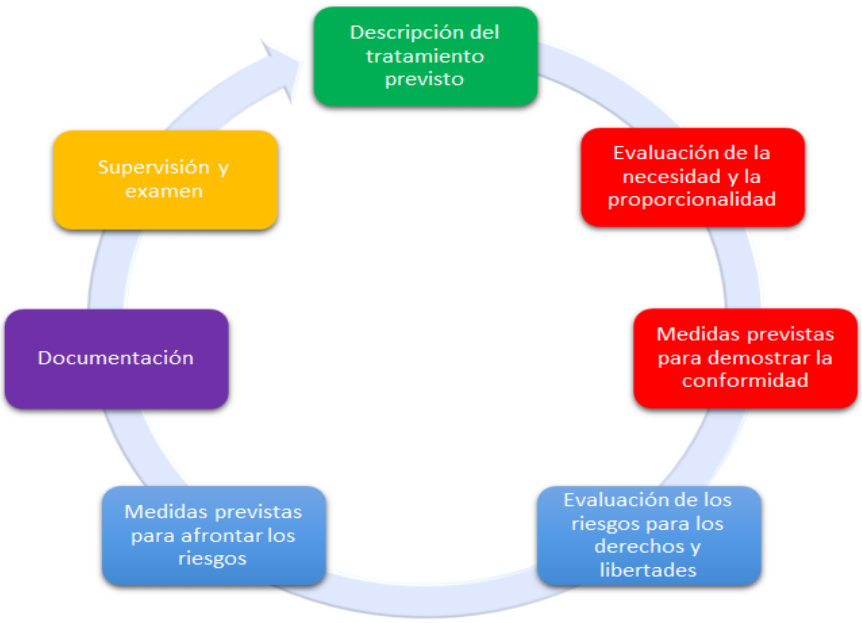
[38] El documento enumera también otros criterios que han de valorarse para concluir cuándo un tratamiento u operaciones de tratamiento de datos "probablemente" entrañan un alto riesgo para los derechos y libertades del interesado, entre los que se encuentran: evaluación o puntuación, incluida la elaboración de perfiles, toma de decisiones automatizadas con efectos jurídico o similar, observación sistemática, datos sensibles o datos muy personales, asociación o combinación de conjunto de datos, datos, datos relativos a interesado vulnerables, uso innovador o aplicación de nuevas soluciones tecnológicas u organizativas, cuando el tratamiento impida a los interesados ejercer un derecho o utilizar un servicio o ejecutar un contrato". El documento señala que se puede valorar que un tratamiento que cumpla dos criterios requerirá la elaboración de una EIPD. El criterio del WP 29 es que cuantos más criterios se cumplan más probable es que el tratamiento represente un alto riesgo para los derechos de los interesados. También es posible que un responsable de tratamiento estime que un tratamiento que cumpla solo uno de los criterios señalado requiere una EIPD, Documento sobre la evaluación de impacto relativa..., ob. cit., págs. 10 y 11.

[39] https://www.aepd.es/media/guias/guia-evaluaciones-de-impacto-rgpd.pdf, pág. 4. Esta guía asesora sobre la forma de elaborar una EIPD

[40] Directrices sobre la evaluación de impacto relativa..., ob. cit., pág. 4

derechos y libertades de las personas físicas, es decir, un análisis de riesgo para tener presentes las amenazas que dicho tratamiento puede acarrear. En cuarto y último lugar, las medidas previstas para hacer frente a los riesgos, las medidas de seguridad, y los mecanismos que garanticen la protección de datos personales, teniendo en cuenta, dice el art. 35.7 d) RGPD, "los derechos e intereses legítimos de los interesados y de otras personas afectadas". Todo ello en un lenguaje sencillo y asequible, que pueda ser comprendido por los sujetos que recurrirán a la EIPD para poder garantizar el respeto a los derechos de los interesados.

FIGURA 2: Gráfico del proceso creativo de una EIPD [41]



Fuente: Manual de buenas prácticas de ISms y la AEPD

La EIPD es un documento vivo, "un proceso utilizado para reforzar y demostrar el cumplimiento del RGPD"[37] que hay que revisar y actualizar cuando se produzca una modificación en el riesgo, pues debido a esta variación podría quedar inservible a los efectos de proteger los derechos de los interesados, o bien cuando se produzca un cambio en aspectos relevantes de las actividades de tratamiento. Es decir, tras la modificación del riesgo podría derivarse un alto riesgo para los derechos de los interesados que habría que mitigar y que antes

[41] Directrices sobre la evaluación de impacto relativa..., ob. cit., pág. 18.

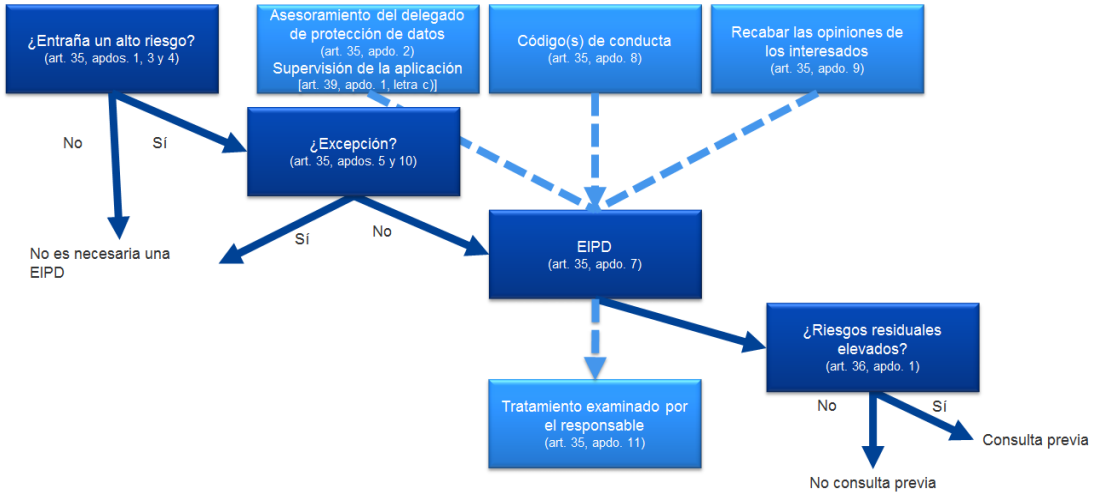
de dicha variación no se había presentado.

La responsabilidad de la realización de la EIPD corresponde al responsable del tratamiento, y debe ser asistido en dicha tarea por el DPD y por el encargado del tratamiento. Las EIPD cumplen una doble misión en sus relaciones con el responsable pues "son instrumentos importantes para la rendición de cuentas", ya que, además de ayudar a los responsables a cumplir los requisitos del RGPD, resultan esenciales para demostrar que este ha adoptado las medidas adecuadas para garantizar el cumplimiento del Reglamento. En todo caso, las autoridades de control deberán elaborar y comunicar al Comité Europeo de Protección de Datos una lista de las operaciones de tratamiento que requieran una EIPD.

Tras la elaboración de la EIPD se ha de concluir con una respuesta favorable o desfavorable respecto de la gestión de riesgos en el tratamiento concreto. Si la respuesta no es favorable se deberán incluir medidas de control adicionales a las establecidas que, resulta obvio, no son suficiente para la protección de los derechos, lo que ocurre cuando se concluye que el riesgo es elevado. Si no es posible mejorar las garantías estudiadas, el tratamiento no se puede iniciar y habrá que plantear una consulta previa ante la AEPD que finalmente resolverá la cuestión. La AEPD dará la solución a través de una resolución favorable que puede incluir recomendaciones para añadir medidas de refuerzo que aseguren la protección de los derechos de los sujetos, o bien con una resolución desfavorable, en cuyo caso el tratamiento de Big Data no podrá iniciarse.

Por otro lado, la adhesión del responsable a un código de conducta (art. 40 RGPD) puede resultar un elemento adecuado para la mejor realización y gestión de la EIPD.

FIGURA 3: Ilustración de la relación de la EIPD con el RGPD y la forma de concebir el documento[42]



Fuente: Manual de buenas prácticas de ISms y la AEPD

La EIPD ha de incluir como contenido mínimo (art. 35.7 d) RGPD) las medidas de seguridad que garanticen la protección de datos personales. Las medidas de seguridad del tratamiento a que alude el art. 32.1 RGPD se adoptarán teniendo en cuenta el estado de la técnica, los costes de aplicación y la naturaleza, el alcance, el contexto y los fines del tratamiento y los riesgos variables para los derechos de los interesados. Las medidas de seguridad serán adecuadas al riesgo detectado tras el análisis realizado y como mínimo han de incluir (art. 32.1 RGPD):

- la seudonimización y el cifrado de los datos, lo que garantiza que el tratamiento de datos personales ya no puede atribuirse a una persona sin utilizar información adicional. Esta información adicional está guardada de forma separada y cuyo acceso está impedido por medidas técnicas que no permitan su atribución a una persona física identificada o identificable.

- La capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanente de los sistemas y servicios de tratamiento. La confidencialidad, la integridad y la disponibilidad han de evitar el tratamiento no autorizado, los accesos no legítimos y han

[42] Directrices sobre la evaluación de impacto relativa..., ob. cit., pág. 8.

de velar por la protección física del dato, esto es, se ha impedir o minimizar el daño, la destrucción, la pérdida o la modificación del dato como elemento objetivo que incorpora información. La modificación o alteración de datos personales puede ser no intencionada al igual que su pérdida o borrado. Cualquier alteración que afecte a la integridad de los datos ha de ser objeto de una rápida respuesta por parte del propio sistema que ha de manifestar una permanente capacidad de resiliencia ante estas eventualidades. Por ejemplo, medidas concretas de control en el sentido indicado pueden ser copias de seguridad que mitiguen la pérdida o borrado accidental del dato o el almacenamiento en ubicaciones distintas; para asegurar la confidencialidad se pueden establecer mecanismos de control de accesos.

- La capacidad de restaurar la disponibilidad y el acceso a los datos personales en caso de incidente físico o técnico, lo que pone de manifiesto de nuevo la resiliencia del sistema.

- Procesos de verificación, evaluación y valoración regular de las medidas técnicas y organizativas.

De nuevo, al igual que en el caso de la elaboración de una EIPD, la adhesión a un código de conducta, de acuerdo con el art. 40 RGPD (o a un mecanismo de certificación aprobado según el art. 42) podrán servir como elementos para demostrar el cumplimiento de los requisitos sobre la seguridad del tratamiento que se acaban de mencionar (art. 32.3 RGPD). Por otro lado, las medidas técnicas y organizativas de seguridad que hemos detallado han de quedar reflejadas en el registro de actividades de tratamiento[43]

Ahora bien, las medidas técnicas y organizativas apropiadas, según la política proactiva incorporada por el RGPD, deben ser consideradas desde el diseño, con la finalidad de incorporar desde el inicio del tratamiento las garantías para la

[43] El registro de actividades de tratamiento del art. 30.1 RGPD establece que "cada responsable y, en su caso, su representante llevarán un registro de las actividades de tratamiento efectuadas bajo su responsabilidad. Dicho registro deberá contener toda la información indicada a continuación: a) el nombre y los datos de contacto del responsable y, en su caso, del corresponsable, del representante del responsable, y del delegado de protección de datos; b) los fines del tratamiento; c) una descripción de las categorías de interesados

protección de los datos y de los derechos de los interesados. Esta previsión de protección desde el comienzo es especialmente aconsejable en los proyectos de Big Data y su previsión convierte la adopción de dichas medidas en un elemento esencial de la protección de datos. El art. 25 RGPD alude a la protección de datos desde el diseño y por defecto, que consiste en incorporar, desde las primeras fases del proyecto de tratamiento de datos y durante el desarrollo del mismo, las medidas necesarias para proteger los derechos y libertades del interesado y cumplir los requisitos del RGPD. Para desarrollar la privacy by design and default se han establecido una serie de principios fundamentales[44]:

- Proactivo y preventivo. Las medidas que se adoptan son proactivas, no reactivas. Se trata de mantener una anticipación a la eventualidad que puede agredir los derechos de los interesados antes de que está pueda realmente acontecer.

- La protección de datos desde el diseño y por defecto opera sin necesidad de interactuación del sujeto interesado. La protección es automática al estar integrada en el propio sistema, de manera que la protección de datos está prevista como parte esencial del propio sistema o tratamiento. No constituye una parte del sistema, sino que es el sistema mismo.

- Funcionalidad completa en el sentido de asegurar que se cumplen todas las necesidades y exigencias de todos los sujetos implicados.

- Protección completa, que abarca toda la vida activa de los datos, desde su recolección hasta su desaparición. La protección completa implica que la seguridad cubre todo el ciclo de vida de los datos.

- Viabilidad y transparencia, elementos que aseguran el cumplimiento de la normativa, de los principios y finalidades establecidos, que además se puede verificar de forma independiente.

- Respecto a la privacidad del usuario, máxima cuyo significado implica que por encima de todo se encuentra la protección de la persona, fin

[44] Código de buenas prácticas en protección de datos…, ob. cit., pág. 20.
[41] Código de buenas prácticas en protección de datos…, ob. cit., pág. 21.

al que van dirigidas las medidas de seguridad desde el diseño y por defecto.

"Si en todo proyecto de Big Data se tuviesen en consideración estos principios, y muy en particular los asociados a la Limitación en la Recogida y la Minimización de Datos, se reduciría considerablemente el riesgo para la privacidad[45].

Como estrategias para asegurar la privacidad que se pueden adoptar desde el diseño se han propuesto las siguientes[46]: minimización de datos, agregar los datos lo máximo posible y con el mínimo detalle, ocultar los datos para los usuarios, separar, esto es procesar los datos en entornos diferentes, información y transparencia a los usuarios de cómo y cuándo se va a llevar a cabo el tratamiento de sus datos, control por parte de los interesados, lo que equivale a ejercitar sus derechos y conocer qué se va a hacer con sus datos personales, demostrar que se cumple la política de privacidad y la normativa en vigor.

Las estrategias de privacidad se pueden implementar con mayor o menor intensidad según la fase del tratamiento de Bi Data en la que nos encontremos[47]:

[45] Código de buenas prácticas en protección de datos..., ob. cit., pág. 21
[46] Privacy by design in big data. An overview of privacy enhancing technologies in the era of big data analytics, disponible en https://www.enisa.europa.eu, pág. 22.
[47] Código de buenas prácticas en protección de datos..., ob. cit., pág. 29

FIGURA 4: Código de Buenas Prácticas en Protección de datos

FASE BIG DATA	ESTRATEGIA	IMPLEMENTACIÓN
Adquisición y recolección	Minimizar	• Seleccionar antes de adquirir • EIPD
	Agregar	• Anonimización en la fuente origen
	Ocultar	• Herramientas de cifrado • Herramientas de enmascaramiento de datos
	Informar	• Transparencia - Comunicación al interesado
	Controlar	• Mecanismos para recabar consentimiento
Análisis y validación	Agregar	• Técnicas de anonimización
	Ocultar	• Herramientas de cifrado
Almacenamiento	Ocultar	• Herramientas de cifrado • Mecanismos de autenticación y control de acceso
	Separar	• Almacenamiento distribuido / descentralizado
Explotación	Agregar	• Técnicas de anonimización
Todas las fase	Cumplir / Demostrar	• Definición de políticas • Trazabilidad de las acciones • Herramientas de cumplimiento

Fuente: Manual de buenas prácticas de ISms y la AEPD

La sensibilidad hacia la asunción de un papel fundamental por parte de los responsables de tratamiento, las empresas y entidades que tratan datos personales, en el tratamiento de la información personal es fundamental para garantizar la cohabitación racional entre la tecnología y la persona en términos de respeto hacia sus derechos y beneficio para ambas partes. Esa sensibilidad tiene reflejo en la concepción de la accountability, concebida como la mentalidad que cumple la normativa y las obligaciones de la protección de datos por convencimiento y que puede demostrarlo. Por ello, esta mentalidad conjuga los intereses de las organizaciones y los ciudadanos y la propia sociedad para "identificar, comprender y responder" acerca de los temas que preocupan y poder garantizar de forma adecuada la sostenibilidad jurídica y social de los tratamientos de datos[48].

[48] Código de buenas prácticas en protección de datos..., ob. cit., pág. 21.

En esta labor de concienciación, las autoridades de control han de liderar el proceso con la elaboración de guías, documentos, redacción de Informes, establecimiento de cauces de contacto para solventar dudas y mantener una fluida colaboración; y las empresas asumir con responsabilidad su papel de responsables de tratamiento de datos. El principio de accountability alude, como señala la AEPD "a la responsabilidad de las compañías en la implantación de medidas, en el seno de sus organizaciones, de garantía y cumplimiento de los principios y obligaciones en materia de protección de datos, así como el establecimiento de mecanismos internos y externos para evaluar su fiabilidad y demostrar su efectividad cuando se solicite por las autoridades de control"[49].

En esta actitud de compromiso hacia la observancia de todos los elementos y principios necesarios para la protección de los derechos de los interesados es necesario destacar la formación adecuada, permanente y actualizada que hay que ofertar a todo el personal que participe en cualquiera de las fases del tratamiento de datos. Se deben dedicar recursos humanos y económicos suficientes para proveer la formación necesaria para poder resolver con garantías todos los aspectos del tratamiento de la información personal.

Por otro lado, el RGPD promueve la elaboración de códigos de conducta, "destinados a contribuir a la correcta aplicación del Reglamento teniendo en cuenta las características específicas de los distintos sectores de tratamiento y las necesidades específicas de las microempresas y las pequeñas y medianas empresas" (art. 40.1 RGPD). En el tratamiento de datos en proyectos de Big Data los códigos de conducta pueden convertirse en una útil herramienta para dar transparencia al tratamiento y recabar así la confianza de los interesados.

2.3 La privacidad como valor ético esencial del siglo XXI

Expertos en privacidad alertan de que, en cierto sentido, mi valor como persona está hoy día representado por mi vida digital (cómo me ven los demás,

[49] Código de buenas prácticas en protección de datos..., ob. cit., Ibidem

cuántos seguidores tengo en redes sociales, qué dicen los bancos sobre mi solvencia, qué coberturas merezco frente a las aseguradoras, etc.).

Se comienza a aceptar una nueva disciplina, la Ciberética, como ciencia aplicada que se sitúa entre las Ciencias de la Computación y la Ética. Un ámbito clave en la Ciberética es precisamente el objeto de este estudio: la compatibilidad entre la privacidad, el Big Data y la Inteligencia artificial.

Es necesario devolver la confianza en el uso que se está haciendo de los datos personales. Urge desarrollar tecnologías robustas (que sitúen los asuntos de seguridad[50]entre los más prioritarios) y con propósito ético.

Para ello, puede ser muy valioso extrapolar al Big Data las DIRECTRICES ÉTICAS para una IA FIABLE (**UE, 2019** Grupo de expertos de alto nivel sobre inteligencia artificial):

- Desarrollar, desplegar y utilizar los sistemas respetando los principios éticos de: ***respeto de la autonomía humana***, ***prevención del daño***, ***equidad y explicabilidad***. Reconocer y abordar las tensiones que pueden surgir entre estos principios. - Prestar una atención especial a las situaciones que afecten a **los grupos más vulnerables**, como los niños, las personas con discapacidad y otras que se hayan visto históricamente desfavorecidas o que se encuentren en riesgo de exclusión, así como a las situaciones caracterizadas por **asimetrías de poder o de información** - Reconocer y tener presente que, pese a que **aportan beneficios** sustanciales a las personas y a la sociedad, los sistemas de IA también **entrañan determinados riesgos** y pueden tener efectos negativos, algunos de los cuales pueden resultar difíciles de prever, identificar o medir (por ejemplo, sobre la democracia, el estado de Derecho y la justicia distributiva, o sobre la propia mente humana).

[50] Vid. The Cloud Security Alliance (CSA) Big Data Working Group (BIG DATAWG) has come up with 100 best practices to enhance the security and privacy of Big Data:
https://docs.google.com/document/d/1FqeHlA53sliNS3sd3ECy2hwyJu0UJDZT71zUs-02nX4/edit
The top 10 best practice concerning security are: 1. Authorize access to files by predefined security policy

- Garantizar que el desarrollo, despliegue y utilización de los sistemas cumplan los requisitos para una IA fiable:
  - 1) acción y supervisión humanas,
  - 2) solidez técnica y seguridad,
  - 3) gestión de la privacidad y de los datos,
  - 4) transparencia,
  - 5) diversidad, no discriminación y equidad,
  - 6) bienestar ambiental y social, y
  - 7) rendición de cuentas.

- Para garantizar el cumplimiento de estos requisitos, se deberá estudiar la posibilidad de emplear tanto métodos técnicos como no técnicos.

- Impulsar la investigación y la innovación.

- Comunicar información a las partes interesadas, de un modo claro y proactivo, sobre las capacidades y limitaciones de los sistemas, posibilitando el establecimiento de expectativas realistas, así como sobre el modo en que se cumplen los requisitos. Ser transparentes acerca del hecho de que se está trabajando con un sistema.

- Facilitar la trazabilidad y la auditabilidad de los sistemas, especialmente en contextos o situaciones críticos.

- Adoptar una evaluación de la fiabilidad al desarrollar, desplegar o utilizar sistemas, y adaptarla al caso de uso específico en el que se aplique dicho sistema.

- Tener presente que este tipo de listas de evaluación nunca pueden ser exhaustivas. Garantizar la fiabilidad no consiste en marcar casillas de verificación, sino en identificar y aplicar constantemente requisitos, evaluar soluciones y asegurar mejores resultados a lo largo de todo el ciclo de vida del sistema de IA, implicando a las partes interesadas en el proceso.

Para conseguir estos retos, no pueden perderse de vista los peligros de los que alerta Floridi (2019):

— *Ethics shopping*, que supone que una organización elija, entre las muchas iniciativas que hay de códigos éticos muy dispersos, el que mejor se adapte a su forma de hacer, justificando así sus intenciones, poco coherentes con la ética en ocasiones.

— *Ethics dumping,* que consiste en la conducta de exportar prácticas no éticas a países donde hay más laxitud o diferencia de criterios.

— *Ethics lobbying,* o la práctica de algunos actores privados de usar autorregulación en temas como la ética de la Inteligencia Artificial para hacer lobby en contra de la introducción de normas con fuerza jurídica, sometidas estas últimas a mecanismos más exigentes en caso de incumplimiento.

— *Bluewashing,* como concepto proveniente de la ética de la Ecología –*greenwashing*- (Delmas and Burbano 2011), que es la mala práctica de una organización pública o privada que busca aparecer socialmente como más verde, sostenible y comprometida de lo que en realidad es.

3. El valor del dato personal en la nueva economía digital. El papel de la portabilidad

3.1. La portabilidad y sus impactos en el libre accedo a la información

El derecho a la portabilidad se consagra en el artículo 20 del RGPD:

> "*Artículo 20.* **Derecho a la portabilidad de los datos** 1.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, cuando: a) el tratamiento esté basado en el consentimiento con arreglo al artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), o en un contrato con arreglo al artículo 6, apartado 1, letra b), y b) el tratamiento se efectúe por medios automatizados. 2. Al ejercer su derecho a la portabilidad de los datos de acuerdo con el apartado 1, el interesado tendrá derecho a que los datos personales se transmitan directamente de responsable a responsable cuando sea técnicamente posible. 3.El ejercicio del derecho mencionado en el apartado 1 del presente artículo se entenderá sin perjuicio del artículo 17. Tal derecho no se aplicará al tratamiento que sea necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento. 4.El derecho mencionado en el apartado 1 no afectará negativamente a los derechos y libertades de otros.

La portabilidad de los datos se concibe como un derecho para el interesado, lógicamente, pues constituye una parte esencial del objeto del derecho a la protección de datos: permitir el control de los datos personales por parte del sujeto. Con el derecho a la portabilidad se refuerza el control del interesado sobre sus datos de carácter personal que están en manos de un responsable. Pero el derecho a la portabilidad también facilita la libre circulación de los datos en el mercado único digital, pues al permitir el paso de datos de un proveedor a otro mejorará el movimiento de los datos, la competencia, la innovación y la oferta de servicios. Incorpora por tanto un altísimo valor económico y de libre mercado, aunque su regulación normativa, no olvidemos,

no persigue ni mejorar la competitividad ni mantenerlo como recurso económico, sino favorecer el control de la persona sobre sus datos, lo que da prioridad a este aspecto frente a cualquier otro.

El derecho a la portabilidad habilita al interesado a recibir los datos personales que previamente haya entregado a un responsable de tratamiento y transmitirlos a otro responsable de tratamiento, o bien, en segundo lugar, a permitir un traspaso directo de datos de responsable a responsable[51]. Los datos se han de entregar en un formato estructurado, de uso común y lectura mecánica. Esta última exigencia obligará a los responsables de los tratamientos de Big Data a desarrollar medios que permitan el ejercicio del derecho a la portabilidad pues, de otro modo se convertiría en una facultad ineficaz para el derecho a la protección de datos.

El derecho a la portabilidad de los datos tiene lugar en tratamientos basados en el consentimiento del sujeto, por tanto, es el consentimiento el que legitima la portabilidad de los datos o bien las obligaciones derivadas de un contrato.

Con la finalidad de facilitar el ejercicio de este derecho se está impulsando el *Data Transfer Project* (20 de julio de 2018, creado por Google, Microsoft, Twitter y Facebook, al que se han unido Apple en julio de 2019), que así mismo amplía el mercado para las empresas, al permitir "rutas de intercambio de datos" [52]. El DTP tiene como objetivo permitir que las personas puedan transmitir sus datos entre proveedores de servicios en línea a través de un marco común, que incluye protocolos de datos para facilitar la transferencia directa de datos dentro y fuera de los proveedores de servicios en línea participantes, lo cual no está exento de riesgos para los derechos de los sujetos. El DTP recoge un conjunto de principios con el fin de someter a los responsables de las grandes empresas a pautas de actuación en el ejercicio a la portabilidad[53]:

[51] El WG 29 recomienda la incorporación de herramientas de descarga de datos e interfaces de programación de aplicaciones, Directrices sobre el derecho a la portabilidad de los datos, pág. 3

[52] Como lo ha denominado Dans, Enrique, https://www.enriquedans.com/2018/07/data-transfer- project-dtp-que-es-y-para-que-sirve.html

[53] DTP pretende hacer más fácil nuestra vida digital facilitando de manera segura la comunicación de nuestros datos entre proveedores de servicio en internet. Algunos ejemplos que pueden ayudar a entender el alcance son: a) La posibilidad de mover nuestros datos, perfil, comentarios y fotos de una red social a otra; b) La facilidad de imprimir fotos

- Construir para usuarios y facilitar la portabilidad, para lo que las herramientas de portabilidad de datos deben ser fáciles de encontrar e intuitivas de usar. La facilidad y la disponibilidad constituyen también, a nuestro modo de ver, una proyección de la transparencia en el contexto de la portabilidad. Los instrumentos para ejercer la portabilidad deben ser abiertos e interoperables, lo que refuerza la facilidad de uso entre los usuarios (transferirlos o descargarlos para los fines del sujeto).

- Privacidad y seguridad. Los responsables de la transacción de los datos, el responsable que posee los datos y el responsable al que se le transfieren, deben adoptar medidas de seguridad para garantizar la protección de los datos, de manera que se evite el acceso no autorizado, o el desvío de datos a otros proveedores. Se propone la minimización de datos, así como la transparencia en la operación de transferencia de datos entre los proveedores. Los sujetos que ejercitan el derecho a la portabilidad deben ser informados de manera clara, sencilla y concisa de todos los elementos de la transferencia de datos. Esta información garantiza la privacidad y la seguridad de la transferencia.

- Reciprocidad: el ejercicio de la portabilidad no puede ir en detrimento del derecho a la protección de datos, en el sentido de impedir que el sujeto siga manteniendo el control sobre sus datos de carácter personal y el tratamiento de los datos pueda seguir siendo transparente. El ejercicio del derecho a la portabilidad no es finito y los datos pueden ser portados de nuevo, siempre que para el sujeto se mantengan las garantías en todo momento del proceso. Como señala el DTP "proporcionar transparencia alrededor de la portabilidad llevará a los usuarios a preferir proveedores comprometidos con la reciprocidad de la protección frente a los que no lo son", lo que previsiblemente obligará a los proveedores a

que tenemos en una red social, a través de un proveedor de internet, al poder pasar la información de un lugar a otro; c) La agilidad en el cambio de nuestro proveedor de música sin perder las listas o preferencias que hayamos creado; d) El hecho de compartir nuestro historial de compra de una cadena de supermercado online a otra, con el ahorro de tiempo y energía que eso supone.

cumplir la normativa en materia de protección de datos y a poder demostrarlo.

Centrarse en los datos del sujeto: los datos objeto de la portabilidad son los datos personales que se refieren a la persona, y los datos que esta hay facilitado a un responsable del tratamiento[54]. Se excluyen por tanto los datos anónimos o que no conciernan al individuo, pero sí se incluirían los datos seudonimizados. En cuanto a datos facilitados por el interesado, según el WP 29 se incluyen también "los datos personales que se observan a partir de las actividades de los usuarios, tales como datos en bruto procesados por un contador inteligente u otros tipos de objetos conectados, registros de actividad, historial de usos de sitios web o actividades de búsqueda", (pero no se incluyen los datos creados por el responsable del tratamiento, sobre los datos facilitados por el usuario, que por tanto no serán objeto de portabilidad). La expresión datos facilitados por el usuario se debe entender en sentido amplio, pero sin incluir los "datos inferidos" y los "datos deducidos" [55] . La expresión "datos que incumben al interesado" no puede comprenderse solamente como datos que se refieran estrictamente al sujeto, por ejemplo, si es el historial de abonado del sujeto inevitablemente se incluirán también los datos relativos a las llamadas entrantes y salientes de otras personas. La limitación al empleo de estos datos recaerá en el responsable que recibe los datos que no podrá tratarlos sin consentimiento y por supuesto con perjuicio para los derechos y libertades de un tercero.

- Respeto entre todos: la portabilidad debe respetar los datos de los demás sujetos y nunca ejercerse de manera que se puede perjudicar

[54] Por ejemplo, datos facilitados por el interesado incluye las siguientes categorías: "datos facilitados de forma activa y consciente por el interesado (por ejemplo, dirección postal, nombre de usuario, edad, etc.); datos observados facilitados por el interesado en virtud del uso del servicio o dispositivo. Estos pueden incluir, por ejemplo, el historial de búsqueda, lo datos de tráfico y los datos de ubicación de una persona. Pueden incluir asimismo otros datos en bruto tales como el ritmo cardiaco registrado por un dispositivo ponible", Directrices de portabilidad..., ob., cit., pág. 12.

[55] El derecho a la portabilidad tal y como se establece en el RGPD y en la LOPDGDD supone un derecho más reducido que el que inicialmente figuraba en los primeros proyectos de RGPD. De hecho, el derecho a la portabilidad se puede ejercitar respecto a datos obtenidos por el responsable con el consentimiento del interesado, quedando fuera de este derecho cualquier otro dato obtenido posteriormente por parte del responsable y deducido de un tratamiento de big data, por ejemplo. Sobre esta cuestión, vid. Paul De Hert a,b, Vagelis Papakonstantinou a, Gianclaudio Malgieri a, Laurent Beslay c, Ignacio Sanchez (2017) "The right to data portability in the GDPR: Towards user-centric interoperability of digital services" *Computer law & s e c u r i t y review*.

> a las personas vinculadas con el solicitante del derecho a la portabilidad. Por eso, el cumplimiento del derecho a la portabilidad no podrá afectar negativamente a los derechos y libertades de otro u otros sujetos. Por tanto, el ejercicio del derecho a la portabilidad no puede incluir la recuperación y transmisión de los datos que contienen información personal de otros sujetos. El art. 20.4 RGPD alude a la imposibilidad de afectar negativamente a los derechos y libertades de los otros interesados.

El efecto negativo se produciría si la transmisión de datos de un responsable a otro impidiese que un tercero pudiera ejercitar los derechos que le corresponden o bien si se destinarán los datos de los terceros a otros fines. Como ejemplos de esta situación: los datos de la cuenta bancaria de un sujeto incorporan datos de otros sujetos con los que ha realizado las transacciones. Si el titular de la cuenta ejercita el derecho a la portabilidad de los datos, los derechos y libertades de los otros sujetos que aparecen en su cuenta no se verán lesionados si solo se utilizan para el mismo fin, por ejemplo, para ver el historial de la cuenta del interesado. Por el contrario, se verían perjudicados si sus datos se utilizaran para otros fines como pueden ser fines de mercadotecnia. ¿Cómo se propone la protección de los derechos de los terceros involucrados en el ejercicio del derecho a la portabilidad de un sujeto? Una solución podría ser que el tratamiento de los datos personales de los sujetos cuyos datos se ven afectados por el derecho a la portabilidad de otra persona se permita solamente para cuestiones puramente personales o domésticas, bajo el control y la responsabilidad del sujeto que recibe los datos portados. El responsable que recibe los datos nunca podrá usarlos para sus propios fines, esto es, no podrá extraer información de los terceros afectados y crear perfiles sobre ellos, salvo que cuente para ello con el consentimiento[56]. En caso contrario, el tratamiento de datos sería ilícito, pues no cuenta con el consentimiento explícito del sujeto para ello.

Se plantea también, como una solución añadida, la utilización de herramientas por parte de los responsables emisores y receptores que permitan

[56] Así lo recomienda la 36a Conferencia Internacional de Autoridades de Protección de Datos, al señalar que se debe "obtener cuando sea apropiado el consentimiento válido del titular de los datos en relación con el uso de información personal para fines de análisis y de creación de perfiles".

al sujeto que ejerce la portabilidad seleccionar los datos de otras personas que desea transmitir y los que desea excluir, medida que reduce el riesgo para los terceros. Junto a ello, los responsables pueden emplear instrumentos que permitan recabar el consentimiento de los terceros, con el fin de facilitar la transmisión de datos relacionados con un sujeto que ejerce la portabilidad.

Respecto del receptor de los datos, la transparencia es un principio de nuevo esencial, pues habrá de quedar claro, antes del ejercicio del derecho a la portabilidad, la finalidad del nuevo tratamiento de datos; y si el receptor de los datos opta por iniciar un nuevo tratamiento, habrá de dar cumplimiento a todos los principios del art. 5 RGPD, tales como la minimización de datos, la exactitud, la lealtad, la licitud, la limitación del tiempo de conservación, etc. Así pues, los datos personales que no sean necesarios para el nuevo tratamiento habrán de ser eliminados.

¿Cómo actuar cuando el derecho a la portabilidad colisione con el derecho a la libertad de información? Cuando se trate del ejercicio del derecho al libre acceso a la información en colisión con el derecho a la protección de datos, la respuesta no puede consistir en una solución general, válida para todos los casos que puedan presentarse, pues habrá que atender a las circunstancias de caso concreto. En todo caso, existen reglas que permiten iniciar un procedimiento pautado que ofrezca una solución racional y ajustada al Derecho, pues en el choque entre derechos fundamentales habrá que someter la respuesta al juicio de proporcionalidad. El juicio de proporcionalidad ya presupone la existencia de la disminución de uno de los derechos en conflicto frente a la expansión o prevalencia del otro. La medida que justifique la limitación de uno de los derechos frente a la restricción del otro ha de ser idónea, necesaria y proporcional. La medida será idónea si es susceptible de conseguir el fin propuesto. Comprobada la idoneidad, la medida será necesaria, a continuación, si no existe otra medida menos lesiva para el derecho fundamental limitado que permita conseguir el mismo objetivo. Finalmente, la medida será proporcionada si se desprende de ella más beneficios para el interés general que perjuicios para la persona que ve reducido su derecho. Por supuesto el fin perseguido ha de ser constitucional y tener previsión legal.

En definitiva, será necesario en estos casos tener en cuenta cómo se han utilizado los datos, las expectativas razonables sobre su utilización, las relaciones entre responsable y afectado y las posibles salvaguardas adicionales que puedan ser aplicadas por el responsable[57].

¿Cómo asegurar por parte del responsable del tratamiento que los datos se entregan a la persona adecuada? El responsable del tratamiento es quien debe adoptar todas las medidas de seguridad necesarias para garantizar que los datos personales se transmiten de manera segura (mediante el uso de seguridad de extremo a extremo o encriptado de datos) al destinatario correcto y también para continuar con la protección de los datos personales que quedan en sus sistemas. Se han de abordar procedimientos transparentes para hacer frente a las posibles violaciones de la seguridad de los datos.

3.2. La competencia en el acceso a los datos

Las normas de privacidad actuales parten de la base de que compartir datos puede perjudicar al individuo. Por ello se hacía necesario gestionar mecanismos como la notificación y el consentimiento para la recolección y tratamiento de los datos. Sin embargo, existen muchos nuevos servicios actuales (tales como Twitter, Facebook, Instagram) que ponen de manifiesto que los individuos sí quieren compartir datos personales.

Para crear valor, los datos necesitan moverse, y para moverse, se necesita confianza entre todos los agentes que participan en la cadena de valor (individuos, empresas, organizaciones, gobiernos, reguladores, etc.). Y más aún, al contrario que con la mayoría de los bienes físicos, el valor de los datos crece con su uso: conectar dos datos crea un nuevo dato que a su vez puede servir para nuevas aplicaciones y para seguir creando valor.

[57] Paul De Hert a,b, Vagelis Papakonstantinou a, Gianclaudio Malgieri a,Laurent Beslay c, Ignacio Sanchez (2017) "The right to data portability in the GDPR: Towards user-centric interoperability of digital services" *Computer Law & S e c u r i t y Review ,* p. 6.

La falta de confianza en los modelos actuales de consentimiento y anonimización han propiciado una corriente basada en los derechos de acceso y cancelación de los datos de los individuos de las bases de datos, así como de los sistemas *opt-in*. Por ejemplo, el RGPD introduce el denominado «derecho al olvido» que faculta a los ciudadanos europeos a pedir el borrado de sus datos bajo determinados requisitos, e introduce la obligación de que el consentimiento sea a través de una clara acción afirmativa no siendo válido el consentimiento tácito y, en determinados casos, requiriendo un consentimiento explícito como en relación con lo datos sensibles del art.9 RGPD.

Si bien estos derechos no deben eliminarse, deben regirse con flexibilidad. Se podrían poner en peligro algunas ventajas del acceso abierto. Estos datos comunes son aquellos datos que han sido agregados, anonimizados y hechos públicos para favorecer el conocimiento y la innovación. Esto se perjudicaría si los individuos encuentran incentivo para borrar sus datos si aprecian un riesgo de que los sistemas de anonimización fallen y puedan ser reidentificados, sin importar cuán pequeño sea este riesgo.

Una vez más, (aparte de la evidente solución técnica), una solución complementaria puede verse en que los agentes compartan derechos y obligaciones. Efectivamente, el hecho de que un investigador, una empresa, o una agencia gubernamental tengan la capacidad técnica de reidentificar a los sujetos, no quiere decir que deba hacerlo, ni que tenga derecho a ello.

Para generar la confianza que el entorno necesita, las normas y las leyes no son suficientes por sí solas. Una de las soluciones que se ha propuesto es un modelo de co- regulación en la que las responsabilidades y los derechos sean compartidos entre todos los agentes, y que se base en la creación de los llamados «puertos seguros» en el uso de los datos. Y por supuesto, todo sistema debe ir acompañado de las mayores medidas de ciberseguridad disponibles en cada momento.

Por otro lado, en el ámbito de la Union Europea, la Estrategia de Datos y el Libro Blanco sobre Inteligencia Artificial son los primeros pilares de la nueva

estrategia digital de la Comisión. Todos ellos se centran en la necesidad de poner a las personas en primer lugar en el desarrollo de la tecnología, así como en la necesidad de defender y promover los valores y derechos europeos en la forma en que diseñamos, hacemos y desplegamos la tecnología en la economía real. La estrategia europea en materia de datos tiene por objeto crear un mercado único de datos que garantice la competitividad global y la soberanía de Europa en materia de datos. Los espacios comunes europeos de datos garantizarán que haya más datos disponibles para su uso en la economía y la sociedad, manteniendo al mismo tiempo el control de las empresas y las personas que generan los datos.

Los datos son un recurso esencial para el crecimiento económico, la competitividad, la innovación, la creación de empleo y el progreso de la sociedad en general. Las aplicaciones impulsadas por los datos beneficiarán a los ciudadanos y las empresas de muchas maneras: mejorando la atención sanitaria, creando sistemas de transporte más seguros y limpios, generando nuevos productos y servicios, reduciendo los costes de los servicios públicos, mejorando la sostenibilidad y la eficiencia energética.

Las empresas tendrán más datos disponibles para innovar. Para ello, se pondrán en marcha normas prácticas, justas y claras sobre el acceso y el uso de los datos, que cumplan los valores y las normas europeas, como la protección de los datos personales. Para garantizar el liderazgo de la UE en la economía mundial de los datos, esta estrategia europea para los datos pretende: Adoptar medidas legislativas sobre la gobernanza, el acceso y la reutilización de los datos, por ejemplo, para el intercambio de datos entre empresas y gobiernos en aras del interés público; dar mayor difusión a los datos abriendo los conjuntos de datos de alto valor en poder del público en toda la UE y permitiendo su reutilización de forma gratuita. Para ello la Unión pretende comenzar un proyecto europeo para desarrollar infraestructuras de procesamiento de datos, instrumentos de intercambio de datos, arquitecturas y mecanismos de gobernanza para un próspero intercambio de datos y para federar infraestructuras de nube fiables y eficientes desde el punto de vista energético y servicios conexos; de esta forma, se permitirá el acceso a servicios de nubes

seguros, justos y competitivos facilitando la creación de un mercado de contratación de servicios de procesamiento de datos y creando claridad sobre el marco reglamentario aplicable en materia de nubes de normas sobre nubes; Además, se facultará a los usuarios para que mantengan el control de sus datos e invertir en el fomento de la capacidad de las pequeñas y medianas empresas y de las aptitudes digitales.

En definitiva, se trata de fomentar el despliegue de espacios comunes europeos de datos en sectores cruciales como la fabricación industrial, el acuerdo ecológico, la movilidad o la salud.

Como parte de la estrategia de datos, la Comisión Europea ha publicado un informe sobre el intercambio de datos entre empresas y gobiernos (B2G). El informe contiene un conjunto de recomendaciones políticas, jurídicas y de financiación que contribuirán a que el intercambio de datos B2G en el interés público sea una práctica escalable, responsable y sostenible en la UE.

Los datos no deben ser vistos sólo en términos de privacidad cuando se trata de datos personales.

Los datos que se generan en el mundo digital son un recurso esencial hoy día para el crecimiento económico, la competitividad, la innovación, la creación de empleo y el progreso de la sociedad en general. El valor económico de estos datos ha ido creciendo en la Unión Europea, pudiendo llegar a incrementarse desde 285 billones de euros en 2015, más del 1.94% del PIB, hasta 739 billones en 2020, lo que supondría un 4% del PIB de toda la UE.

Los métodos de análisis de datos se usan de formas muy diversas: tanto para predecir elecciones de los consumidores o la probabilidad de padecer determinada enfermedad; para detectar extremismo político en medios de comunicación y redes sociales, como para gestionar mejor las redes de comunicación.

El tratamiento de los datos a partir del Big Data ofrece infinitas posibilidades en muchos ámbitos de la actividad económica[58].

Como recuerdan algunos autores (Villatoro, 2014), las empresas persiguen la creación de una relación emocional con sus clientes. No obstante, la única y principal diferencia entre un mundo que vende productos y el que vende servicios es que el propietario del servicio es el prestador del mismo. Esto significa que los clientes y las empresas comienzan una relación que, como todas las relaciones, necesita de actualizaciones constantes porque las preferencias cambian con el tiempo y se mueven constantemente, y esos movimientos exigen cambios, adaptaciones y reconfiguraciones. Además, las

[58] • Mejor conocimiento del cliente: la información permite ofrecer un mejor servicio y atención al cliente.
• Mejor conocimiento del mercado para la captación de nuevos clientes.
• Personalización de productos y servicios: la información permite personalizar el servicio ofreciendo una mejor experiencia de cliente, incrementando la fidelización y satisfacción.
• Mejora y rapidez en la toma de decisiones: la información permite a las organizaciones públicas y privadas tomar mejores decisiones, optimizando la gestión de procesos y, por tanto, reduciendo costes aumentando la competitividad.
• Previsión del comportamiento: un análisis adecuado permite obtener una mejor visión de qué puede pasar, ampliar la visión estratégica y de negocio, crear nuevos servicios y productos, y obtener nuevos ingresos.
• Monetización: la propia información puede ser monetizada, por ejemplo, a través de una mejor publicidad o compartiendo estos datos con otras compañías (eso sí, asegurando el cumplimiento del marco legal).
Prácticamente en todos los sectores de actividad se pueden encontrar ejemplos de uso del Big data. Aunque solo se llegan a conocer los casos de éxito, hay que estar preparado para que en cualquier uso de Big data se produzcan resultados erróneos y poder evitar que su aparición cause efectos dañinos. En muchos casos, esos "errores" pueden ser inocuos (pensemos, por ejemplo, en la presentación de una publicidad ligeramente errónea donde el perjuicio es que la probabilidad de venta es cero) comparado con el uso para la toma de decisiones que puedan causar perjuicios a personas o colectivos específicos.
Algunos usos del big data por sectores de actividad serían los siguientes:
• Venta por Internet: es el más obvio y uno de los pioneros. Todo aquel que compra por Internet puede observar cómo la publicidad que recibe es cada vez más atinada al contenido de las búsquedas que realiza o la información que consulta, incluso aunque aparentemente no se haya identificado. Asimismo, en el proceso de compra, rara es la tienda que no ofrecerá productos y servicios complementarios en base a la experiencia de otros clientes.
• Venta presencial: análisis de los patrones de compra dentro de la tienda y por cliente. En el caso del cliente, el uso de las tarjetas de fidelización es clave. Toda esa información ayuda a colocar los productos para maximizar su venta, ofrecer descuentos y productos a los clientes apropiados, identificar compras correlacionadas, etc. Cuanto más conozcan cómo compramos, más se puede adaptar la tienda para maximizar su venta. Sector bancario: uso en el análisis de riesgos en general y en la concesión de préstamos en particular, lucha contra el fraude, personalización de ofertas para clientes, captación de clientes externos ayudándoles a utilizar su información financiera o a crear servicios de valor añadido, etc. Al tratar el Big data en el sector financiero, además de las normas de protección de datos hay que tener en cuenta la Directiva PSD2, que supone muchos cambios con múltiples implicaciones, como puede ser la apertura de los bancos de sus servicios de pagos a terceras empresas. Esto permitirá el acceso de terceros a las cuentas de los clientes, pero también hará que se refuerce la seguridad de estas entidades.
• Industria petrolífera: ha sido una de las industrias pioneras en el uso del Big data, el apropiado análisis de la información sísmica y otros datos geológicos permite perforar en los lugares más productivos. Una vez en producción, la monitorización continua mediante múltiples sensores permite maximizar el tiempo de funcionamiento y mejorar la seguridad de trabajadores y del entorno.
• Políticas públicas: Soporte para toma de decisiones en el desarrollo de políticas públicas en diferentes ámbitos como el educativo, sanitario, servicios de emergencia, turismo, transporte, seguridad ciudadana, empleo.
• Ayuda al desarrollo y situaciones de emergencia: Herramienta para la gestión de situaciones de catástrofes, políticas de desarrollo humano y social.
• En el ámbito de la salud, cantidades enormes de datos de salud y genéticos complejos aumentan cada vez más. Se extrae información de las historias clínicas electrónicas, de datos administrativos, de seguimiento de los pacientes, entre otros. La investigación médica está transformándose cada vez más en una actividad muy intensiva en el uso de datos, entre ellos datos relativos a la salud, genéticos o biométricos, que se recogen, reutilizan e interconectan a gran escala

empresas tienen que conseguir que esta interacción mutua o este mutuo compromiso con el cliente esté automatizado.

Con el fin de embarcarse en este nuevo paradigma de relaciones individuales y automatizadas, las empresas tienen que aprender a escuchar y conseguir que el cliente se suba a bordo. Tienen que escuchar porque necesitan automatizar la relación entre el cliente y el servicio con tecnología informática y crear muchos datos que necesitan ser ajustados constantemente. Además, tienen que involucrar a los clientes para que ellos mismos hagan el trabajo: ellos compran el teléfono en la tienda online, lo actualizan y descargan las aplicaciones.

En el ámbito del marketing, a partir del análisis a gran velocidad de los datos ya almacenados de lo que ocurrió en el pasado y de lo que está pasando ahora se pueden predecir los comportamientos de los clientes en el futuro. "Por ejemplo, es muy útil para realizar un seguimiento en tiempo real de una campaña publicitaria, para comprobar si está funcionando y modificarla sobre la marcha. Sin embargo, intentar predecir algo en *Big Data* sin contar con científicos de datos es como tener el mejor avión sin piloto".

Las redes sociales, que aportan un flujo incesante de datos que ofrece enormes oportunidades de negocio, tanto en términos de conocimiento de los clientes como de apertura de nuevos canales de mercado. El Big Data es una herramienta esencial en el ámbito de la Inteligencia de Negocio.

3.3. Propiedad de los datos

Según el estudio "Analytics: The realworld use of Big Data", del IBM Institute for Business Value y la Said Business School de la Universidad de Oxford, el 100% de los retailers disponen en sus Big Data de información derivada de sus transacciones de back-office; un 67%, de los registros que permiten la trazabilidad completa de su actividad comercial; un 57%, de la información generada por sus terminales punto de venta, escáneres y RFID; un 43%, de los datos capturados en las redes sociales; un 40%, de los datos obtenidos a través

de sensores y el mismo porcentaje de ellos, de los correos electrónicos y de datos provenientes de fuentes externas (climatología, estadísticas ofi ciales, etc.). Según describe el estudio citado, cabe destacar que un 25% de los retailers ya disponen de información geoespacial, de audio y de vídeo incorporada a sus Big Data.

Resolver la propiedad de la información que se está utilizando en la nueva economía digital es otro gran reto. Por la rapidez con la que se genera a través del Big Data y el potencial de la Inteligencia artificial, los conflictos sobre la propiedad de los datos van en aumento. En el caso de que se generalizase la propuesta de monetización de la información con pago a usuarios, habrá que delimitar muchos aspectos en relación a cómo se genera el valor del dato, qué criterios se tienen en cuenta para calcularlo, etc.

3.4. La compensación económica a los usuarios por el uso de los datos personales

Algunas voces venimos proponiendo la viabilidad/compatibilidad de nuestro modelo de protección de datos con la posible monetización de los datos personales[59]. De esta forma, las organizaciones que utilizan Big Data podrían compartir con los consumidores el valor de sus datos. Este valor podría materializarse mejorando los productos y servicios digitales, haciéndolos mejores y más sencillos de comprender. Este enfoque también incluye buscar formas más eficaces de concienciar al público acerca de la generación y empleo de datos. La transparencia es un prerrequisito para este control, puesto que permite una comprensión de las opciones disponibles. No es posible tener una elección sustantiva sin transparencia.

Los individuos también deben contar con la posibilidad de utilizar sus datos para generar valor para terceras partes. Empresas como Telefónica están

[59] Lanier, Jaron "New conceptions of privacy" *Investigación y Ciencia,* 2014; López Garrido, Diego, (coord.), Serrano Pérez, Ma Mercedes, Fernández Aller, Ma Celia, *Derechos y obligaciones de los ciudadanos en el entorno digital*. Fundación Alternativas, 2018, p. 74; Telefónica, *Manifiesto por un New Digital Deal*, 2018, p. 55.

desarrollando una amplia gama de colaboraciones para permitir a nuestros usuarios utilizar sus datos en su propio beneficio.

Este asunto se complicará aún más si llega a generalizarse la propuesta de utilización de Blockchain para responder al reto del cuello de botella en las experiencias digitales por parte de las plataformas tecnológicas globales.

Esta tecnología es esencialmente descentralizada y puede contribuir a una justa distribución del valor generado en la nueva economía digital. Se podrían crear organizaciones autónomas descentralizadas, que permitirían compartir valor entre individuos y comunidades sin intervención de intermediarios (las plataformas digitales actuales).

Otra aplicación relevante en el tema que nos ocupa sería la posibilidad de que las personas pudiesen compartir potencia de cómputo para actividades de minería de datos. En lugar de utilizar anuncios on line, las web enviarían códigos de minería que las máquinas de los usuarios podrían ejecutar. De esta forma, el modelo de negocio cambiaría sustancialmente.

CONCLUSIONES

Los retos que plantea la tecnología del Big Data en nuestra sociedad son enormes, tanto en el ámbito ético, como económico, social, jurídico, tecnológico. Se exponen a continuación las principales conclusiones de este estudio, junto a algunas recomendaciones.

PRIMERO

El Big Data permite el almacenamiento, tratamiento y comunicación de ingentes cantidades de información personal. Cualquier tratamiento de Big Data ha de hacerse en un marco de protección de los derechos que permita a estas personas saber en todo momento quién tiene sus datos personales, con qué finalidad se tratan y si van a comunicarse a terceros. De lo contrario, el titular de los datos perderá el control sobre lo que se sabe de él, y qué tipo de decisiones que le afectan se tomarán sin su control (concesión de una hipoteca, aumento de la prima de un seguro, admisión en nuevo puesto de trabajo, por ej.).

Si hay algo que caracteriza a esta tecnología es que, a priori, antes de comenzar el tratamiento de los datos personales, no se conoce la información o conclusiones que se derivarán. Por este motivo, es difícil solicitar el consentimiento antes de comenzar el tratamiento cumpliendo los requisitos legalmente previstos: que este se preste de forma libre, específica e informada. Esto supone un reto grande en un momento en que en Europa estrenamos legislación de protección de datos, siendo nuestro sistema el más protector y garantista de los que existe. El consentimiento para el tratamiento de los datos debe verse acompañado de procesos transparentes e informados, con el fin de alcanzar y respetar el mayor equilibrio posible entre tratamiento de la información a través de Big Data y derechos de los ciudadanos.

A nivel global, las mayores preocupaciones surgen cuando el Big Data se dirige a hacer correlaciones entre datos de salud, datos financieros, datos demográficos y datos de localización; así mismo, cuando se hace seguimiento de

la actividad comercial del cliente y se comparte con terceras partes; también saltan las alertas cuando los resultados de los tratamientos de Big Data se almacenan en una nube que abarque diferentes ámbitos geográficos. Finalmente, hay un reto con la falta de transparencia: quién tiene acceso a los datos, qué información se recoge y para qué finalidad. Por tanto, este trabajo se enmarca en los ámbitos en los que el Big Data suponen mayores riesgos para la protección de datos. La accountability como filosofía y forma de actuación de todos los implicados en el tratamiento de datos personales debe ser una prioridad en la formación de estos sujetos. La accountability como responsabilidad, como actitud diligente, proactiva y como capacidad de demostrar que se cumple con lo establecido.

SEGUNDO

Con respecto a las soluciones de Big Data y explotaciones de este, es necesario recordar que, si bien se están haciendo avances, no vemos más que la punta del iceberg de las posibilidades que existen. Como la cantidad de datos que generamos está aumentando a cifras inmanejables, es necesario mantener los estándares de protección de datos más altos posibles.
El Big Data está más presente en nuestras vidas de lo que imaginamos. Desde las decisiones que tomamos basadas en la experiencia, que incluyen descartar un sitio porque no lo pasaste bien, hasta las decisiones del futuro o aquellas otras más esporádicas, estamos usando el 'Big Data' sin darnos cuenta. Generamos tal cantidad de datos que no somos conscientes de lo vulnerables y accesibles que estamos en Internet.

Es urgente que el ciudadano sea consciente de hasta qué punto son importantes los datos personales porque, aunque existan normativas que nos ayuden, sin sensibilidad de cada persona para velar por su privacidad, las vulneraciones seguirán produciéndose. La cultura de la protección de datos todavía debe extenderse mucho más. Las autoridades de control deben desempeñar un papel educativo y formativo significativo en este sentido.

TERCERO

No hay que olvidar la potencialidad del enfoque preventivo, sin el cual no será posible conseguir el respeto a la privacidad. Para ello hay que llevar a cabo una adecuada gestión de riesgos, incorporar el principio de 'privacy by design', resiliencia y transparencia. Sin duda, la privacidad será el valor ético esencial en el siglo XXI. La responsabilidad proactiva del responsable y del encargado obliga a pensar en términos de protección de datos para desde el inicio del tratamiento y a aplicar las medidas necesarias para garantizar los derechos de los interesados, así como mantenerlas durante toda la vida de los datos, sin necesidad de actuación del sujeto del que se recaba la información, es decir, a iniciativa y bajo la responsabilidad proactiva y diligente del responsable del tratamiento. Además, el responsable ha de poder demostrar que actúa de modo correcto y cumpliendo la normativa en vigor. La adhesión a un código de conducta facilita tanto dicho cumplimiento como su verificación.

CUARTO

El Big Data supone una revolución tecnológica muy importante, que presenta indudables ventajas en cuanto a la eficiencia, los impactos de los nuevos usos de la información, la reducción de costes, entre otros. Sin duda, puede contribuir a la generación de crecimiento económico y a la creación de valor. No obstante, como siempre sucede con la introducción de nuevas tecnologías, puede traer consigo riesgos relacionados con las violaciones a la privacidad, la discriminación y los sesgos, la falta de seguridad, entre otros. En este sentido, un análisis desde la Ética es esencial, por cuanto soluciones jurídicas o técnicas exclusivamente no están consiguiendo proteger los derechos del interesado. La mirada desde la ética ha de coordinarse siempre con las otras miradas desde el ámbito legal, político, social, etc.

Los códigos éticos de las asociaciones de Ingeniería recogen principios que debieran guiar los desarrollos tecnológicos del Big Data. Sin embargo, existen demasiadas propuestas de principios éticos de aplicación en el campo tecnológico, descoordinadas entre sí. Association for Computing Machinery

(ACM), Institute of Electrical and Electronics Engineers (IEEE), Principios de Asilomar para la Inteligencia Artificial[60], el Contrato de la web de la WWW Foundation, Naciones Unidas, a través de su Relator sobre el derecho a la privacidad[61], Unión Europea, Telefónica, Internet Society, Global Network Initiative[62] (GNI), Ranking Digital Rights (RDR), por citar algunas.
La privacidad es uno de los asuntos que más preocupan a los expertos en ética en los últimos tiempos.

QUINTO

Aunque las legislaciones de protección de datos pueden ayudar a garantizar la privacidad, también pueden afectar la innovación y la creación de nuevos modelos de negocio al evitar la reutilización y combinación de diferentes tipos de información. El RGPD y la LOPDGDD limitan la recopilación de datos personales al cumplimiento de propósitos específicos predefinidos. También requiere la destrucción de datos una vez que se logra el propósito para el que se han recopilado. Esta disposición evita la acumulación de datos, que es una condición necesaria para los grandes datos. Por otro lado, se exige que responsables y encargados mantengan los datos personales actualizados. Esta disposición puede ayudar a aumentar la calidad de los datos, lo que a su vez puede mejorar la precisión de la estimación y el análisis de Big Data.

Existe una evidente necesidad de adaptar la legislación de protección de datos a la tecnología Big Data. En general, esta se desarrolla ofreciendo potencialidades que no tienen un marco de protección adecuado.

Hay varias visiones en torno a las características que habría de tener un sistema de regulación de la privacidad en relación al Big Data:

1. La privacidad es un derecho fundamental y no puede verse limitado por intereses de ningún tipo que pongan en peligro la capacidad de las personas de controlar el uso que se haga de la información que les concierna.

[60] https://futureoflife.org/ai-principles/
[61] https://www.ohchr.org/EN/Issues/Privacy/SR/Pages/SRPrivacyIndex.aspx
[62] https://globalnetworkinitiative.org/about-gni/

2. b) La otra visión, más extendida entre el sector industrial, prefiere extender el "motivo de interés legítimo" al tratamiento de todas las categorías de datos y a todas las fases del ciclo de vida de los datos. Esta visión considera que el "consentimiento informado" y la "minimización de datos" son contrarios a la realidad de los grandes datos.

En este segundo caso, los datos personales pueden recogerse, utilizarse (lo que incluye la elaboración de perfiles), fusionarse, transferirse y destruirse si existe un "interés legítimo del responsable del tratamiento que no supere los derechos de privacidad de las personas". Por ejemplo, mediante la inclusión de un panel de configuración de perfil en un sitio web de medios sociales donde se muestran las características relevantes del perfil y que puede ser adaptado por el individuo.

"El principio de responsabilidad debería extenderse explícitamente a todas las fases del ciclo de vida de los datos. Los controladores deben ser responsables de la implementación de un programa interno de cumplimiento de la protección de datos que garantice que las decisiones tomadas se implementen realmente en las prácticas de la empresa. Por consiguiente, no deben imponerse requisitos prescritos en materia de documentación y de consulta y autorización ex ante.

Parte de la obligación de rendición de cuentas consiste en realizar una evaluación de impacto de la protección de datos cuando se lleven a cabo nuevas operaciones de tratamiento de datos. Proponen ampliar esta obligación a la realización de una evaluación de impacto tecnológico más amplia" (Lokke Moerel).

SEXTO

La seguridad es uno de los retos legales más importantes de los grandes datos. Si los datos personales no se procesan teniendo en cuenta la seguridad, la protección de datos no es posible y las personas pueden verse afectadas. Un reciente proyecto de investigación de la Open University del Reino Unido afirma

que "las empresas que extraen valor de los datos personales estarían más dispuestas a invertir en seguridad de la información y protección de datos que en lo contrario. Las empresas que tratan los datos como un activo clave y son conscientes de los posibles riesgos económicos y de reputación generados por la pérdida o la divulgación no autorizada de datos pueden dedicar más recursos a la protección de datos que las organizaciones que tienen que tratar datos personales, pero no ven ningún valor en los datos. Estas organizaciones podrían subestimar la importancia de asignar recursos a los programas de protección de datos y, por lo tanto, podrían poner en peligro la privacidad de las personas".

Algunos tipos de usos de grandes datos son los que más preocupan a las políticas públicas. Son principalmente los siguientes:

a) Correlación de datos dispares, tales como datos sanitarios, financieros, demográficos y de localización.
b) Seguimiento del comportamiento de los consumidores para facilitarlos a terceros sin la debida autorización para la selección y otros fines.
c) Almacenamiento de grandes cantidades de datos en la nube a través de múltiples fronteras geográficas.
d) Falta de transparencia (quién tiene acceso a qué datos, qué datos se recopilan y por qué razón).

En general, todos los criterios relacionados con la seguridad está puestos en entredicho con la utilización del Big Data. En el caso de la disponibilidad, puesto que es muy difícil de conseguir si los tratamientos se realizan en tiempo real. Así mismo, la integridad, puesto que, dependiendo de cuál sea la fuente en la que se hayan obtenido los datos, por ejemplo en Internet, puede suponer un problema. En cuanto a la confidencialidad, solo se podría alcanzar este objetivo de protección mediante una anonimización absoluta de los datos. Pero hay que recordar que es muy difícil alcanzar una anonimización absoluta de los datos, ya que nuevas tecnologías podrían hacer posible una reidentificación de estos.

En cuanto a la transparencia, en este ámbito las empresas activas en el campo del Big Data suelen excusarse haciendo referencia al secreto industrial[59]. Desde el punto de vista del sujeto afectado es evidente que no es alcanzable ya

que, a diferencia de lo que sucede en los tratamientos “tradicionales”, él no es consciente de la existencia del tratamiento.

SÉPTIMO

La normativa no se encuentra adaptada al nuevo entorno tecnológico. El principio de «minimización de datos» no se cumple en la práctica. Este principio implica que los datos recopilados no deben ser excesivos, sino que debe recopilarse solo la cantidad mínima necesaria para el fin para el que se recogen. Pues bien, en muy pocas ocasiones las autoridades de protección de datos obligan de forma efectiva a las empresas a rediseñar sus procesos para minimizar los datos recabados.

Es más, el principio de minimización de datos se contrapone contra la misma lógica del Big Data. Los nuevos modelos analíticos se basan precisamente en el estudio de cantidades masivas de datos sin los cuales no podría extraerse el conocimiento que nos permite el Big Data. La minimización ha de ser una máxima asumida y respetada por el responsable del tratamiento.

Un modelo de protección de datos basado exclusivamente en el consentimiento del titular para recopilar y tratar sus datos de carácter personal trae consigo muchos problemas. La experiencia dice que la gran mayoría de los individuos no lee las políticas de privacidad antes de prestar su consentimiento; y aquellos que lo hacen no las comprenden.

La anonimización ha demostrado tener limitaciones. Si bien se presentaba como la mejor solución para tratar los datos protegiendo la privacidad de los sujetos, se produce a menudo la reidentificación de bases de datos que habían sido anonimizadas, o lo que es lo mismo, no se anonimiza de forma irreversible. Cada vez se hace más sencillo reidentificar a los sujetos, ya no solo a través del análisis de distintas fuentes que contienen datos personales parciales de una persona, sino a través de datos no personales. Esto supone un debilitamiento de la anonimización como medida para asegurar la privacidad durante el tratamiento de datos.

El Big Data aumenta el riesgo relacionado con la toma de decisiones de forma automática. Esto hace que decisiones trascendentales para nuestra vida, tales como calcular nuestro riesgo crediticio, queden sujetas a algoritmos ejecutados de forma automática. El problema surge cuando los datos que son analizados por medio de los algoritmos no son precisos o veraces, pero los individuos no tienen incentivos para corregirlos porque no son conscientes de que están siendo utilizados para tomar decisiones que les afectan.

OCTAVO

En general, se observa una falta de transparencia, ligada al celo que las organizaciones ponen cada vez más en cómo procesan la información y qué utilidad puede tener el resultado de ese procesamiento para la propia organización. Este celo en no revelar los tratamientos de la información que llevan a cabo puede conducir a que los ciudadanos no sepan realmente qué ocurre con sus datos una vez los facilitan. Y esto es así porque, en ocasiones, quizás ni las propias empresas son del todo conscientes de hasta dónde llegarán tales tratamientos de información. En este sentido, es muy relevante que los interesados sean conocedores de los impactos que los diferentes tratamientos pueden tener sobre su privacidad. La pérdida de la posibilidad de realizar el control sobre los datos personales del sujeto en manos ajenas implica una vulneración del derecho a la protección de datos de carácter personal.

La transparencia de un tratamiento de datos en su conjunto y de las partes implicadas puede permitir que especialmente los sujetos afectados y las autoridades de control puedan detectar posibles fallos y exigir que se lleven a cabo las modificaciones necesarias para suprimirlos. En general, existe un desequilibrio en la información entre las personas y las empresas que tratan sus datos personales; desequilibrio que es muy probable que aumente con el avance de sistemas Big Data. Un ejemplo relevante de esta posible situación es la modificación de precios de un producto en función de lo que esté dispuesto a pagar cada consumidor.

NOVENO

Como punto positivo, el *Big Data*, analizado con los métodos adecuados, va a proporcionarnos una gran oportunidad de avanzar nuestro conocimiento. Por un lado, pone a nuestra disposición datos con una precisión y grado de detalle y desagregación que nunca han existido en la historia. Por otro, las necesidades de análisis con datos masivos van a requerir un enfoque más interdisciplinario, con la Estadística en una posición central, pero con aportaciones fundamentales de las Ciencias de la Computación y del Aprendizaje Máquina. Además, cualquier análisis debe enmarcarse en el conocimiento ya adquirido y contrastado de la disciplina concreta que estudia en cada caso los datos analizados. En esta tarea, la creación de institutos de investigación interdisciplinarios sobre *Big Data* y *Data Science* facilitará la cooperación de estos científicos y que las herramientas más eficaces desarrolladas en unos campos de aplicación se trasladen a otros. Es importante no caer en particularismos y defensas gremiales para asegurar la unidad del método científico, que ha sido la mejor garantía de los avances pasados y lo será, indudablemente, de los futuros.

RECOMENDACIONES

- Debido a que los principales riesgos del Big Data para la protección de datos y la privacidad se refieren a la cantidad ingente de información que se recoge y sobre la que se elaboran perfiles, la primera recomendación está relacionada con la **inclusión de estas preocupaciones desde la fase de diseño** de la tecnología. La adopción del principio de *privacy by design* es muy relevante. Se recomienda analizar los ejemplos de buenas prácticas que puedan guiar a los diferentes actores (gobiernos, instituciones privadas, etc.) en el logro de estos objetivos. En este sentido, la utilización de Estudios de Impacto en la privacidad son altamente recomendables.

- La **transparencia y la información** son elementos primordiales en el tratamiento de Big Data. Dado que el consentimiento es un principio que se verá modulado en el tratamiento masivo de la información, -pero que

nada justifica su desaparición-, tanto por el propio acto de consentir como por su ligazón con el principio de finalidad, es recomendable y necesario incorporar mecanismos de acceso, de transparencia, de información a través de las páginas web corporativas del centro, del correo electrónico, etc. con el fin de mantener el Big Data en los márgenes de la legalidad y de la ética. Igualmente, para compensar las deficiencias que puede presentar el principio del consentimiento ligado a la finalidad (recuérdese finalidades compatibles con la inicialmente consentida) habrá que contemplar la posibilidad de ejercitar con facilidad y sencillez el derecho de oposición, para el interesado que no desee formar parte de un tratamiento masivo de datos personales.

Se recomienda **invertir en medidas de seguridad tecnológicas y organizativas** que han de ser permanentemente evaluadas y actualizadas, con el fin de responder a los continuos retos que plantean las TIC. Las medidas de seguridad deben garantizar la confidencialidad, la integridad, la disponibilidad, la transparencia. En este sentido, las normas ISO 27000, como estándares internacionales, pueden ser un buen punto sobre el que empezar a trabajar.

La **política de educación y formación permanente especializada** debe ser una prioridad, dirigida a todo el personal que trabaja con datos de carácter personal, con el fin de implicar a la empresa, entidad u organización. La formación en principios éticos y jurídicos es esencial. El personal que gestiona y trata los datos para obtener información debe asumir desde el principio de su tarea que maneja elementos propios del contenido de un derecho fundamental y que deben actuar con la debida responsabilidad.

- Ha de asegurarse la existencia y cumplimiento de un **régimen de rendición de cuentas**, que incluya disposiciones de responsabilidad para garantizar que las entidades que recogen, tratan y ceden datos son responsables en caso de abuso, de forma que no sean los usuarios en los que a menudo recaiga dicha responsabilidad. En este sentido, es deseable que se desarrollen más las pólizas de seguros que compensen el

comportamiento responsable de la seguridad y la protección adecuada de los datos personales.

Es importante que se regulen las cuestiones de privacidad y protección de datos a nivel internacional, con el establecimiento de una autoridad independiente. Posiblemente el ámbito de Naciones Unidas sea uno de los que más impacto podrían tener. A pesar de las dificultades del multilateralismo en los últimos años, no hay otro ámbito que goce de más consenso, y capaz de liderar procesos de la importancia de la Agenda 2030.

Muy relacionado con lo anterior, urge que se aclaren adecuadamente los **roles y las responsabilidades** de aquellos que manejan datos personales en todas y cada una de las fases de utilización de la tecnología. Es importante que las personas con responsabilidad en las organizaciones estén implicadas en los asuntos de *compliance*.

Se recomienda la elaboración de **códigos de conducta**, tal y como recoge el art. 40 RGPD. El código de conducta es una herramienta que ayuda a la aplicación de los principios y derechos del RGPD (así como de la LOPDGDD) al sector en el que proyecte su actividad el Big Data. El código de conducta además de cumplir con la función de dar transparencia e información del tratamiento de datos al interesado servirá al responsable y al encargado del tratamiento para demostrar que han respetado todas las obligaciones exigidas para la protección de los derechos de los interesados, incluyendo medidas de seguridad, privacidad desde el diseño y por defecto, observancia del principio del consentimiento, finalidad, etc. El DPD es también un elemento que ha de tener un alto valor en el tratamiento en Big Data.

Sin embargo, nunca la existencia de un código de conducta puede sustituir el papel de una legislación jurídicamente exigible que garantice un marco protector de los derechos. El establecimiento de sanciones económicas ha sido siempre un factor que ayuda en el cumplimiento de las normas de convivencia. La voluntariedad de los códigos de conducta

ha de complementarse con la aprobación de normativa suficiente y específica que resuelva los interrogantes que existen hoy día.

- Un asunto clave es la extensión de una **cultura de la protección de datos,** para generar confianza entre los ciudadanos que entregan sus datos de carácter personal. La confianza y la seguridad del sujeto en que sus datos van a ser tratados de forma adecuada y con el respeto a sus derechos facilitará la dación de datos, lo que repercutirá en un tratamiento más extenso de los mismos, esto es, mayor volumen de información, por tanto, de negocio y de valor económico. Para ello es recomendable también dar publicidad a todos los documentos elaborados para garantizar los derechos de los interesados especialmente de la EIPD y del código de conducta.

- Es muy urgente que se ponga suficiente atención a las **políticas de sensibilización** en torno a la importancia de la privacidad y los retos que plantea el Big Data. Si estas cuestiones se convierten en temas importantes para la ciudadanía, ésta presionará suficientemente a los gobiernos para desarrollar propuestas normativas que son necesarias[63].

- El **principio de no discriminación** es esencial si se pretende la garantía de los derechos humanos de cualquier persona. Las soluciones de Big Data deben ajustarse a este principio, impidiéndose que las decisiones que se tomen generen brechas digitales que dejen al margen de los avances a minorías y personas vulnerables[61], como personas con discapacidad, mayores, en situación de desventaja económica, infancia, etc.

  Resulta esencial incluir la **perspectiva ética** en cualquier decisión de Big Data. La creación de grupos de trabajo transdisciplinares es clave para conseguir que los valores éticos estén asegurados en las fases de diseño, implementación, uso y evaluación de las tecnologías Big Data.

[63] Eusbanks, V. "La automatización de los prejuicios". *Investigación y Ciencia,* 2019.

BIBLIOGRAFÍA

ACED, Emilio, Heras, Ma Rosario, Sáiz, Carlos Alberto, AEPD, ISMS FORUM, Código de buenas prácticas en protección de datos para proyectos Big Data, https://www.aepd.es/media/guias/guia-codigo-de-buenas-practicas-proyectos-de-big- data.pdf

AEPD, Guía práctica para las evaluación de impacto en la protección de los datos sujetas al RGPD, https://www.aepd.es/media/guias/guia-evaluaciones-de-impacto-rgpd.pdf.

BAGGER TRANBERG, C. (2011) 'Proportionality and Data Protection in the Case Law of the European Court of Justice', International Data Privacy Law, 1: 239–248.

BYUNG CHUL, Han, 2014

Council of Europe, Unboxing Artificial Intelligence: 10 steps to protect Human Rights, 2019

DANS, Enrique, https://www.enriquedans.com/2018/07/data-transfer-project-dtp- que-es-y-para-que-sirve.html

DELMAS, Burbano "The drivers of Greenwashing". California Management Review. 2011.

De Hert, Paul, Vagelis Papakonstantinou, Gianclaudio Malgieri, Laurent Beslay, Ignacio Sanchez (2017) "The right to data portability in the GDPR: Towards user-centric interoperability of digital services" Computer law & S e c u r i t y review.

Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento <<entraña probablemente un alto riesgo>> a efectos del Reglamento (UE) 2016/679, adoptadas el 4 de abril de 2017 y revisadas por última vez y adoptadas el 4 de octubre de 2017, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236

EDPS, Opinion 9/2016 on Personal Information Management Systems -Towards more user empowerment in managing and processing personal data, 20 October 2016, 65 Article 29 WP, Guidelines, rev01, p. 5.

Floridi, Luciano, "Translating Principles into Practices of Digital Ethics: Five Risks of Being Unethical". Springer Nature, 2019.

Fundación Ramón Areces. Big Data. Impulsando el conocimiento, 2015.

Gil, Elena, Big Data, privacidad y protección de datos, Agencia de Protección de Datos, 2015.

González, Pedro Alberto. “Ética de datos, sociedad y ciudadanía”. DILEMATA, año 9 (2017), no 24, 115-129 ISSN 1989-7022 124

Guidelines on the right to data portability, Article 29 WP, 16/EN, WP 2042, rev01, as last revised and adopted on 5 April 2017, p.6. See also, European Commission, Building a New Data Economy. Communication (January 2017), https://ec.europa.eu/digital-single-market/en/policies/building-european-data-economy

Kuner, Christopher,. Cate, Fred H, Christopher Millard, and Dan Jerker B. Svantesson “The challenge of ‘big data’ for data protection” International Data Privacy Law (2012), Vol. 2, No. 2.

Lanier, Jaron “New conceptions of privacy” Investigación y Ciencia (2014).

López Garrido, Diego, (coord.), Serrano Pérez, Ma Mercedes, Fernández Aller, Ma Celia, Derechos y obligaciones de los ciudadanos en el entorno digital. Fundación Alternativas, 2018.

Mayer-Schönberger, V., & Cukier, K. (2013). Big data: A revolution that will transform how we live, work, and think. Houghton Mifflin Harcourt.

Privacy by design in big data. An overview of privacy enhancing technologies in the era of big data analytics, disponible en https://www.enisa.europa.eu

Ricardo Morte Ferrer (2017), ¿Protección de datos/privacidad en la época del Big Data, IoT, wearables...? Sí, ...Etica de datos, sociedad y ciudadanía, ISSN 1989-7022 DILEMATA, año 9 (2017), no 24, 219-233 229

Russ, Juskalian (2017): «TR10: Ordenadores cuánticos funcionales». MIT Technology Review. Disponible el 20/05/2017 en https://www.technologyreview.es/s/6818/tr10- ordenadores-cuanticos-funcionales

Sachs, J.D, Schimidt-Traub, G, Mazzucato, M, Messner, D, Nakicenovic, N, Rockstrom, J. “Six transformations to achieve the Sustainable Development Goals”. Nature Sustainability. 2019.

Telefónica, Manifiesto por un New Digital Deal, 2018.

Villatoro, Daniel, Big Data: de la investigación científica a la gestión empresarial, 2014.

Weltzer, H. Die smarte Diktatur. 2016

Don Ramón de la Cruz, 39 – 1º izda (28001) Madrid
Tel. 91 319 98 60 – Fax 91 319 22 98
www.fundaciónalternativas.org