La gestión de la información en el paradigma algorítmico: inteligencia artificial y protección de datos

Information management in the algorithmic paradigm: Artificial Intelligence and data protection

Jorge Castellanos Claramunt
jorge.castellanos@uv.es
Universitat de València

Resumen

La gestión de la información en la era digital, en un escenario en el que la inteligencia artificial permite el tratamiento de infinidad de datos personales de los ciudadanos, es un tema sobre el que jurídica y socialmente conviene poner el foco. Además de tener presente la reciente regulación comunitaria y española, también hay que observar la importancia de nuevos derechos derivados de la protección de datos de los ciudadanos con el tratamiento informático de los mismos.

Cuestiones como el derecho al olvido, la incidencia política de estos datos, la automatización de decisiones que nos afectan y el modo en el que se emplean en el ámbito educativo y sanitario los datos y su gestión por la inteligencia artificial, son también de notable actualidad.

Así, la gestión de la información deviene en un derecho digital del que se extraen consecuencias para otros muchos derechos fundamentales, núcleo esencial de cuya reflexión se nutre el presente trabajo, concluyendo en una necesaria conjugación de las cuestiones éticas y jurídicas en el modo de implementar los sistemas de inteligencia artificial en el modo de gestionar los derechos y datos personales de los ciudadanos.

Palabras clave

Protección de datos; inteligencia artificial; RGPD; datos personales; privacidad

Abstract

Information management in the digital age, in a scenario in which artificial intelligence allows the treatment of countless personal data of citizens, is a subject on which it is legally and socially convenient to focus. In addition to taking into account the recent community and Spanish regulations, we must also observe the importance of new rights derived from the protection of citizens' data with their computerized treatment.

Issues such as the right to be forgotten, the political impact of this data, the automation of decisions that affect us and the way in which data and its management by artificial intelligence are used in education and health are also of considerable relevance.

Thus, the management of information becomes a digital right from which consequences are drawn for many other fundamental rights, an essential nucleus of whose reflection this work draws, concluding in a necessary conjugation of ethical and legal issues in the way of implementing artificial intelligence systems in the way of managing the rights and personal data of citizens.

Keywords

Data protection; artificial intelligence; GDPR; big data, privacy

Recibido: 22/12/2020
Aceptado: 29/12/2020
DOI: https://dx.doi.org/10.5557/IIMEI11-N21-059082
Descripción propuesta: Castellanos Claramunt, Jorge 2020. La gestión de la información en el paradigma algorítmico: inteligencia artificial y protección de datos. *Métodos de Información*, **11**(21), 59-82

1. Introducción

Como es sabido, la evolución social y tecnológica va planteando nuevas cuestiones en todas las capilaridades derivadas de la interacción humana. Así, un aspecto que ha ido adquiriendo progresivamente más relevancia es el de los medios y procedimientos que pueden emplearse para la gestión y difusión de información. Asimismo, también se plantean nuevos problemas en relación con los contextos de reciente creación en los que fluye la información, como internet y, en particular, en las redes sociales. Sin ir más lejos, la reciente

Orden PCM/1030/2020 (España 2020) ha generado no poca polémica en relación con la denominada "desinformación".

En este escenario, la irrupción de la inteligencia artificial (en adelante, IA) con el empleo de algoritmos está resultando un hecho diferencial. Y es que la vinculación entre la minería de datos y la IA plantean retos enormemente interesantes que serán objeto de nuevas directrices para preservar la privacidad (Martínez Vázquez 2019). La consecuencia de todo ello es la generación de nuevos derechos, de índole digital (Rallo 2019; Rallo 2020), que abren el camino a un nuevo panorama tanto jurídico como social.

En lo que respecta a la información que puede obtenerse en diversos contextos generados en internet, y la difusión y uso informativo que pueden darse a tales datos, así como los límites que pueden derivarse del derecho a la intimidad y de otros derechos fundamentales, todo ello son cuestiones a desarrollar en un contexto más jurídico que el que aquí nos ocupa. En cualquier caso, Cortina Ramos, incluso, afirma que, teniendo en cuenta el desarrollo de la tecnología y el uso de los datos para interactuar en todos los órdenes, se debería convertir el derecho fundamental a la protección de datos y a la libertad digital en un derecho humano universal (Cortina Ramos 2017). De su "fundamentalidad" da buena cuenta el Tribunal Constitucional (en adelante, TC) en la relevante STC 292/2000 cuando indica que "el contenido del derecho fundamental a la protección de datos consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso. Estos poderes de disposición y control sobre los datos personales, que constituyen parte del contenido del derecho fundamental a la protección de datos se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular. Y ese derecho a consentir el conocimiento y el tratamiento, informático o no, de los datos personales, requiere como complementos indispensables, por un lado, la facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está

sometiendo, y, por otro lado, el poder oponerse a esa posesión y usos" (FJ7) (España 2001).

El tema de la protección de datos y la necesaria protección jurídica de los mismos es una cuestión de creciente interés. Así, sin duda, en el ámbito de la información, en su concurrencia con las nuevas tecnologías, se ha producido un avance exponencial en los últimos años, debiendo, en consecuencia, considerar especialmente la mediatización del acceso a la información (Castellanos 2020). Y es que el derecho a la información constituye uno de los pilares de la democracia moderna (Arellano 2007). Samano y Arellano apuntaban ya, de hecho, que la aparición de las tecnologías de la información y la comunicación había supuesto diversos cambios en todas las esferas y aspectos de la vida individual y colectiva, siendo el ejercicio del derecho a la información no solo no una excepción, sino que se concebía como uno de los derechos fundamentales más positivamente influenciados por su aparición (Samano y Arellano 2010, 338).

Por ello, resulta fundamental tener una visión clara de lo relativo a la protección de datos en relación a esa información, por lo que desde el prisma jurídico conviene, inicialmente, mostrar una somera revisión relativa a su regulación.

2. Aproximación jurídica a la protección de datos

En lo que respecta a la protección de datos personales, aunque parezca que se trata de una cuestión novedosa y cuya evolución va apareciendo paulatinamente en medios de comunicación y obras académicas (Rebollo y Serrano 2019), lo cierto es que es una materia tenida en cuenta desde hace tiempo más allá de su consideración constitucional, comprendida en el artículo 18.4 CE: "La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos". Como muestra inicial de la materia que se atisbaba podemos hacer referencia al Convenio Europeo de Derechos Humanos (en adelante, CEDH) en cuyo artículo 8 se dispone lo siguiente:

Artículo 8 CEDH. Derecho al respeto a la vida privada y familiar.

> 1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia.
>
> 2. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención de las infracciones penales, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás.

Destacamos a continuación el Convenio 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, hecho en Estrasburgo el 28 de enero de 1981. Fue ratificado por España el 27 de enero de 1984 (entró en vigor de forma general el 1 de octubre de 1985, de conformidad con lo establecido en el artículo 22.2 del mismo). De este Convenio destacamos su artículo 1 en el que fija como sus fines "garantizar, en el territorio de cada Parte, a cualquier persona física sean cuales fueren su nacionalidad o su residencia, el respeto de sus derechos y libertades fundamentales, concretamente su derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona ("protección de datos")".

También es destacable la labor de pedagogía que pretende al tratar de definir los conceptos sobre los que va a gravitar el Convenio. Así, "datos de carácter personal" significa cualquier información relativa a una persona física identificada o identificable ("persona concernida"); "fichero automatizado" significa cualquier conjunto de informaciones que sea objeto de un tratamiento automatizado; por "tratamiento automatizado" se entiende las operaciones que a continuación se indican efectuadas en su totalidad o en parte con ayuda de procedimientos automatizados: Registro de datos, aplicación a esos datos de operaciones lógicas aritméticas, su modificación, borrado, extracción o difusión; autoridad "controladora del fichero" significa la persona física o jurídica, la autoridad pública, el servicio o cualquier otro organismo que sea competente con arreglo a la ley nacional para decidir cuál será la finalidad del fichero automatizado, cuáles categorías de datos de carácter personal deberán registrarse y cuáles operaciones se les aplicarán.

Además de lo indicado, el Acuerdo de Schengen de 14 de junio de 1985 también tiene una incidencia en la cuestión de la protección de datos. Si bien no se trata de un documento específico en esta materia, sí que es destacable lo referido a sus artículos 7 y 9 para la coordinación a efectos de "facilitar datos que puedan ser de interés para las otras partes en la lucha contra la criminalidad" (artículo 9).

El Sistema de Información de Schengen (en adelante, SIS) es un sistema de información a gran escala que facilita la cooperación entre las autoridades nacionales de control de fronteras, aduanas y policía en el denominado "Area Schengen".

Como complemento al sistema de información SIS se encuentra el sistema de información de visados (en adelante, VIS) que permite a las autoridades competentes la implementación de la política común de visas sobre los visados de corta duración (hasta 90 días).

La normativa que regula el sistema VIS reconoce el derecho de los ciudadanos afectados al ejercicio de los derechos de acceso, rectificación y supresión, así como determinadas limitaciones a los mismos.

La Carta de Derechos Fundamentales de la Unión Europea (en adelante, CDFUE), por su parte, concreta en mayor medida la cuestión, también en su artículo 8:

> Artículo 8. Protección de datos de carácter personal. CDFUE.
>
> 1. Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan.
>
> 2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación.
>
> 3. El respeto de estas normas quedará sujeto al control de una autoridad independiente.

Por último, en este superficial repaso traemos a colación el Tratado de Funcionamiento de la Unión Europea (en adelante, TFUE), especialmente su artículo 16:

> Artículo 16. TFUE.
>
> 1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.
>
> 2. El Parlamento Europeo y el Consejo establecerán, con arreglo al procedimiento legislativo ordinario, las normas sobre protección de las personas físicas respecto del tratamiento de datos de carácter personal por las instituciones, órganos y organismos de la Unión, así como por los Estados miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación del Derecho de la Unión, y sobre la libre circulación de estos datos. El respeto de dichas normas estará sometido al control de autoridades independientes. Las normas que se adopten en virtud del presente artículo se entenderán sin perjuicio de las normas específicas previstas en el artículo 39 del Tratado de la Unión Europea.

El reconocimiento normativo de la CDFUE y la referencia expresa a la regulación del derecho fundamental a la protección de datos personales por el transcrito artículo 16 TFUE establecen una base reguladora de cierta entidad.
Por último, la norma de referencia es el Reglamento de la Unión Europea 679/2016 (en adelante, RGPD) (Unión Europea 2016), que será ampliamente comentado al recoger muchas de las indicaciones de la Directiva que regulaba la materia durante un largo periodo, la Directiva 95/46/CE que deroga, así como ser el articulado al que alude de manera directa la nueva ley orgánica española, la 3/2018 de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (España 2018b), cuya finalidad es garantizar mayores niveles de seguridad jurídica (España Martí 2019). El objeto de la citada Directiva era procurar que la garantía del derecho a la protección de datos personales no supusiese un obstáculo a la libre circulación de los datos en el seno de la Unión, estableciendo así un espacio común de garantía del derecho que, al propio tiempo, asegurase que en caso de transferencia internacional de los datos, su tratamiento en el país de destino estuviese protegido por salvaguardas adecuadas a las previstas en la propia directiva.

3. Información e inteligencia artificial

La saturación de información hace que un ilusorio intento de aglutinar toda la información existente sobre una cuestión no deje de ser eso, un planteamiento ilusorio. El espacio para almacenar y procesar toda la información sobre la cuestión que sea es limitado, somos seres limitados. Y ahí entra en juego la inmensa capacidad de gestión de información derivada de la IA, que implica necesariamente el tratamiento de datos masivos, dentro de los cuales se incluyen diferentes categorías de datos personales por lo que resulta importante un control y una regulación apropiada para el tratamiento de dichos datos personales con el fin de mitigar riesgos para sus titulares (Martínez Devia 2019, 7). De ahí que Martínez Vázquez (2019) afirme que la extendida percepción del uso ilícito, abusivo o fraudulento de los datos es una medida de la vulnerabilidad del derecho fundamental a la protección de datos, que ha pasado al primer plano del nuevo catálogo de derechos que deben ser protegidos en la sociedad digital.

En el Preámbulo de la Ley Orgánica 3/2018 (España 2018), en concreto en su inciso cuarto, se presenta internet como una "realidad omnipresente tanto en nuestra vida personal como colectiva". En dicho preámbulo ya se constata una realidad claramente visible en nuestro día a día y es que la irrupción de las denominadas tecnologías de la información y la comunicación (en adelante, TIC) ha supuesto un cambio radical en todos los órdenes de la vida, que están fundamentados, por la propia naturaleza humana, en la información y transmisión de la misma. He ahí el aspecto que debe tenerse especialmente en cuenta en la presente investigación: la información como eje que posibilita el desarrollo, no solo de otros derechos, sino de la misma dinámica humana. Además, la Ley Orgánica 3/2018 no solo ha supuesto "un cambio de paradigma en cuanto al modelo de protección adoptado", sino que ha incorporado en nuestro ordenamiento jurídico "nuevos derechos para la era digital, no necesariamente relacionados con la protección de datos personales" (Martínez Vázquez 2019). Pese a ello, no faltan autores que observan lagunas o aspectos a mejorar y desarrollar tras sus inicios (Tejerina 2019).

Pese a que identifiquemos con cierta facilidad las oportunidades, pero también los riesgos, que conlleva el uso masivo de TIC, lo cierto es que es gracias a la gestión de la información proporcionada por ellas que se ha generado un

elemento diferenciador sin precedentes en la tramitación de la información. El *big data* ha devenido en clave para infinidad de circunstancias llegando, incluso, a no concebir una salida de los problemas humanos sin su utilización, teniendo en cuenta la ingente cantidad de información gestionable y procesable. Pero no conviene soslayar, al mismo tiempo, que el derecho más vulnerable en nuestra vida digital contemporánea deriva del gobierno de nuestros datos personales y la custodia de nuestra privacidad (Martínez Vázquez, 2019), cuya alineación con los más evolucionados sistemas de IA ha impactado en muy diversas materias, sobre las que la casuística ha generado muchas y variadas situaciones a analizar. Sobre ello podemos focalizar algunos ejemplos, como en el escenario educativo con el reconocimiento de la identidad del alumno ante los exámenes (Martínez Martínez 2020a); en cuestiones relativas a la gestión audiovisual de los derechos televisivos deportivos (Martínez Martínez 2019a) y, por encima de todo, en lo relativo a la gestión de la pandemia producida por la COVID-19 (Martínez Martínez 2020b; Cotino 2020a; Cotino 2020b; entre otros).

Un aspecto, asimismo, que no queremos dejar pasar por alto es la polémica relativa al artículo 58 bis de la LOREG, que se añade por la disposición final 3.2 de la Ley Orgánica 3/2018. Posteriormente, se declara contrario a la Constitución y nulo el apartado 1, por Sentencia del TC 76/2019, de 22 de mayo. Su redacción actual es la siguiente:

> Artículo cincuenta y ocho bis. Utilización de medios tecnológicos y datos personales en las actividades electorales.
>
> 1. (Anulado)
>
> 2. Los partidos políticos, coaliciones y agrupaciones electorales podrán utilizar datos personales obtenidos en páginas web y otras fuentes de acceso público para la realización de actividades políticas durante el periodo electoral.
>
> 3. El envío de propaganda electoral por medios electrónicos o sistemas de mensajería y la contratación de propaganda electoral en redes sociales o medios equivalentes no tendrán la consideración de actividad o comunicación comercial.
>
> 4. Las actividades divulgativas anteriormente referidas identificarán de modo destacado su naturaleza electoral.

> 5. Se facilitará al destinatario un modo sencillo y gratuito de ejercicio del derecho de oposición.

Lo que queremos poner de relieve es que la aprobación del citado artículo generó un importante ruido mediático basado en la afirmación de que la ley permitía crear bases de datos personales con perfiles ideológicos, enviar propaganda personalizada y realizar spam electoral masivo. Rallo sostiene que la intención del legislador no ha sido otra que intensificar la protección de datos en las actividades electorales (Rallo, 2019b), y que la intervención del TC anulando el primer inciso del artículo solo ha puesto en cuestión la técnica normativa empleada. Sea como fuere, la clave de la cuestión apuntada es que la susceptibilidad social respecto al modo en el que se traten los datos personales y la privacidad de los ciudadanos, ya en escenarios informáticos desarrollados en el marco de la IA, es un tema que no resulta indiferente a nadie y sobre el que conviene una profunda y clarificadora reflexión.

Por toda esta concatenación de circunstancias, a principios de 2020, la Agencia Española de Protección de Datos (en adelante, AEPD) publicó una guía relativa a todas estas cuestiones (2020) que lleva por título: "Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial. Una introducción". La finalidad del documento es proporcionar una "primera aproximación para la adecuación al Reglamento (UE) 2016/679, General de Protección de Datos de productos y servicios que incluyan componentes de Inteligencia Artificial"., llegando a la conclusión de que "el cumplimiento de lo establecido en el RGPD exige cierto nivel de madurez a las soluciones IA que permita determinar de forma objetiva la adecuación de los tratamientos y la existencia de avales y medidas para gestionar sus riesgos".

Adicionalmente, cabe indicar que el impacto de la IA en los derechos humanos es una de las claves a tener en cuenta, tal y como pone de manifiesto el Consejo de Europa (2019). En particular estudian la Carta Ética Europea sobre el uso de la inteligencia artificial en los sistemas judiciales, las directrices sobre inteligencia artificial y protección de datos, la Declaración del Comité de Ministros sobre la manipulación de capacidades de los procesos algorítmicos y el Estudio sobre las dimensiones de los derechos humanos de las técnicas automatizadas de procesamiento de datos y las posibles implicaciones regulatorias, así como el Informe del Relator Especial de las Naciones Unidas sobre la promoción y protección de la libertad de opinión y expresión, que

aborda las implicaciones de tecnologías de inteligencia artificial para los derechos humanos en el entorno de la información. Se basa, en consecuencia, en el marco universal, vinculante y procesable existente proporcionado por el sistema internacional de derechos humanos, incluidos los instrumentos de derechos humanos del Consejo de Europa.

Como nos recuerda la profesora Ramón (2020), el artículo 22 del Reglamento (UE) 2016/679 se refiere a la existencia de decisiones automatizadas (cuya equivalencia en la Ley Orgánica 3/2018 se da en el artículo 11), entre las que se incluyen la elaboración de perfiles, en los casos del precepto mencionado, en el apartado 1 («todo interesado tendrá derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar») y el apartado 4 [«Las decisiones a que se refiere el apartado 2 no se basarán en las categorías especiales de datos personales contempladas en el artículo 9, apartado 1, salvo que se aplique el artículo 9, apartado 2, letra a) o g), y se hayan tomado medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado»], podrá solicitarse información que sea significativa acerca de la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.

3.1 Las decisiones automatizadas

Las decisiones basadas únicamente en el tratamiento automatizado representan la capacidad de tomar decisiones por medios tecnológicos sin la participación del ser humano (AEPD 2020). Como vimos *supra*, el artículo 22.1 RGPD no reconoce el derecho a no ser objeto de una decisión o a la elaboración de un perfil, sino a basar ambos en un tratamiento automatizado de datos con efectos jurídicos, o por el que el interesado se vea afectado significativamente. Como ejemplos concretos, el considerando 71 menciona la denegación automática de una solicitud de crédito en línea o los servicios de contratación en red en los que no media intervención humana. Los perfiles consisten en un tratamiento de datos personales que evalúe aspectos de la persona relativos a una persona física, como "analizar o predecir aspectos relacionados con el rendimiento en el trabajo, la situación económica, la salud,

las preferencias o intereses personales, la fiabilidad o el comportamiento, la situación o los movimientos del interesado en la medida que produzcan efectos jurídicos o le afecten significativamente de modo similar". Por el contrario, se deben permitir las decisiones basadas en un tratamiento automatizado, incluida la elaboración de perfiles si lo autoriza el derecho europeo o de los Estados miembros aplicable al responsable del tratamiento, "incluso con fines de control y prevención de fraude y la evasión fiscal... y para garantizar la seguridad y fiabilidad de un servicio prestado por el responsable del tratamiento, o necesario para la conclusión o ejecución de un contrato entre el interesado y un responsable de tratamiento", o si el interesado ha consentido para ello. En cualquier caso, además del respeto a los principios del RGPD, se debe informar de forma específica al interesado y preverse el derecho a obtener una intervención humana, a que el interesado exprese su opinión, a recibir una explicación de la decisión tomada tras la evaluación y a impugnar la decisión. Esta medida, termina el considerando 71, no debe afectar a un menor.

El derecho anterior no se aplicará, dice el artículo 22.2 RGPD, si la decisión es necesaria para la celebración o la ejecución de un contrato entre el sujeto interesado y el responsable del tratamiento; es una decisión autorizada por el Derecho de la Unión, o de los Estados miembros aplicable al responsable del tratamiento, pero ha de establecer medidas adecuadas para proteger los derechos y los intereses legítimos del interesado; o si la decisión se basa en el consentimiento explícito del interesado.

En los casos primero y tercero, dice el artículo 22.3 RGPD, "el responsable del tratamiento adoptará las medidas adecuadas para salvaguardar los derechos y los intereses legítimos del interesado, como mínimo el derecho a obtener intervención humana por parte del responsable, a expresar su punto de vista y a impugnar la decisión".

Por último, según el artículo 22.4 RGPD, las decisiones permitidas, a tenor del artículo 22.1, no podrán fundamentarse en categorías especiales de datos del artículo 9.1 RGPD salvo que se aplique el artículo 9.2 a) o g) RGPD y se hayan adoptado medidas adecuadas para proteger los derechos, libertades e intereses legítimos del interesado.

3.2 Algunas cuestiones específicas

En la IA, la utilización de datos personales es el elemento clave, puesto que se nutre del *big data*, de los datos recabados, para poder operar. De ahí que el RGPD regule la IA en la misma medida que cualquier otra herramienta utilizada para procesar datos personales. Ahora bien, destacan tres elementos específicos del tratamiento concreto de datos cuando interactúa la IA. El primero de los cuales es que se requiere de un procesamiento justo. Viene recogido en su artículo 5 y hace referencia a que los controladores consideren el impacto probable de su uso de IA en las personas y lo reevalúen continuamente. Lo que se exige, en consecuencia, es requiere que los sistemas de IA no produzcan sesgos. Este tema es especialmente espinoso por las dificultades de entablar un sistema de IA lo suficientemente transparente para poder determinar estas cuestiones. La propia capacidad de autoaprendizaje de la IA supone una barrera infranqueable, a medio plazo, para poder determinar con exactitud el procedimiento operado con el tratamiento de esos datos. Desde luego, la preocupación del legislador es razonable, ahora bien, el modo de restringir el problema que puede derivarse parece más complejo.

En segundo lugar destacamos el principio de minimización de datos establecido en el Artículo 5 del RGPD, que requiere que los datos personales sean "adecuados, relevantes y limitados a lo que es necesario en relación con los fines para los cuales son procesados." La inexactitud del precepto se deriva de su propia naturaleza y de la paradoja resultante. Para inferir resultados con menor margen de error la IA necesita de una gran cantidad de datos. A mayor capacidad de información, especialmente en la fase de entrenamiento del algoritmo, mayor fiabilidad se desprenderá del análisis de la IA. Y, desde la perspectiva opuesta, a mayor cantidad de datos suministrados, mayor probabilidad habrá de que se transgredan ciertas líneas en cuanto a la privacidad y suministro de información personal de los ciudadanos. De nuevo, es razonable la prevención del legislador, pero deriva la resolución del problema a un escenario posterior. Además, cuanto más delicado sea el tema a tratar, véase la salud, mayor será la necesidad de ajustar la inferencia de la IA a través de los datos, por estar en juego la propia salud de eventuales pacientes. Ahora bien, precisamente por tratarse de un tema de especial intimidad, mayor será la dificultad para recabar esa información sin socavar derechos

fundamentales de los ciudadanos. Como vimos en el anterior elemento a considerar, también en esta ocasión ninguna solución parece especialmente satisfactoria.

Por último destacamos las evaluaciones de impacto, que están diseñadas para evaluar el impacto de una actividad de procesamiento en la protección de datos personales, donde es probable que el procesamiento genere un alto riesgo para los derechos y libertades de las personas físicas. De nuevo, el planteamiento es abierto a la casuística. Lo que se persigue con ello es establecer una serie de parámetros sobre los que decidir si el uso de la IA, y por tanto la gestión de la información y de los datos personales, es procedente para un caso concreto. Pero cuando se requiere una consulta con la autoridad de protección de datos es porque existe un riesgo residual en el uso del sistema, por ello esta tiene la última palabra sobre si el uso de la IA es permisible o no. Esto puede resultar en la restricción de todo el sistema de IA, o potencialmente solo en los aspectos del algoritmo que se consideran no conformes.

4. Sobre el derecho al olvido

La gran proliferación de datos personales ocasionada por las tecnologías derivadas del *big data* así como la perenne memoria virtual que supone internet, han propiciado la aparición del derecho al olvido frente a las demandas de los ciudadanos ante las distintas prácticas de almacenamiento, procesamiento y transferencia masiva de información personal que han conllevado, en ocasiones, una vulneración del derecho de privacidad. Para contrarrestar estos problemas, con el derecho al olvido digital se permite a los interesados el cifrado y borrado online de sus datos personales cuando éstos sean perjudiciales para sus derechos fundamentales (Sancho 2019, 436).

El derecho al olvido puede plantear un conflicto con el derecho a la información que puede actuar de límite constitucional al ejercicio del derecho a la protección de datos. Y el derecho al olvido en relación con la protección de datos personales recoge los matices que ese conflicto presenta cuando en la exposición de la intimidad de la persona y la protección de sus datos personales interfiere la tecnología, en particular internet. Por ello, el Derecho y

la jurisprudencia deben ajustarse a esta situación, reconociendo, entre otras cuestiones, que el derecho al olvido es una vertiente del derecho a la protección de datos y un mecanismo de garantía para la preservación de los derechos a la intimidad y al honor con los que está íntimamente relacionado, aunque se trate de un derecho autónomo, como ha reconocido el Tribunal Constitucional.

A este respecto, la STC 58/2018, de 4 de junio, (FJ 5) (España 2018a), señala que los matices, además de las tecnologías e internet, tienen que ver "con la forma en que las herramientas informáticas desarrolladas para facilitar el acceso a la información, como los buscadores, afectan singularmente a los datos personales de la ciudadanía; con el modo en que el transcurso del tiempo puede llegar a influir en los equilibrios entre derecho al honor y la intimidad (artículo 18.1 CE) y las libertades informativas [artículo 20.1. d) CE], haciendo nacer un "derecho al olvido" y con la intervención de los medios de comunicación, que también se sirven de las herramientas informáticas hoy disponibles, en el contexto de la garantía de las libertades informativas que, con el uso de aquellas herramientas, se transforman en libertades de alcance global, y que expanden su eficacia hacia atrás en el tiempo de un modo complejo".

En el caso que examina el TC, se solicita la supresión de datos personales que están recogidos en una noticia digitalizada, que por este motivo ha podido ser enlazada a motores de búsqueda generales por internet. La noticia se enmarca en el derecho a la información veraz, pues transmite hechos noticiables, de relevancia pública y de interés general, sin incorporar a la misma juicios de valor. La noticia se ha enlazado a motores de búsqueda sin ningún impedimento, ya que el editor de la noticia primera no empleó protocolos de exclusión para suprimir dicha información del índice de los motores. En el caso en concreto, las sentencias de las instancias fallan a favor de la desindexación de la noticia de los motores de búsqueda, de acuerdo con la doctrina de TJUE en el asunto Google, por entender que la injerencia que provocan en los derechos a la vida privada y a la protección de datos es excesiva. Lo que se pide ahora al TC en la instancia del amparo va más allá de esa doctrina y es que se proceda a la desindexación de la noticia de la hemeroteca digital del periódico que la publicó por primera vez y el rechazo a ocultar los nombres de las personas objeto de la noticia, o bien la negativa a

disimularlos. No es por tanto un nuevo conflicto con los motores de búsqueda (solucionado ya por el TJUE y por el TS, Por todas, vid. SSTS 1917/2016, de 21 de julio; 1618/2016, de 4 de julio; 210/2016, de 16 de marzo) sino que nos hallamos "ante un conflicto circunscrito al uso de nombres propios como criterio de búsqueda y localización de noticias en el entorno de una hemeroteca digitalizada. En este contexto, los derechos que colisionan son, de un lado, el derecho a la supresión de datos de una base informatizada (artículo 18.4 CE), en relación mediata e instrumental con la garantía del derecho al honor y la intimidad de las personas a las que conciernen los datos (artículo 18.1 CE) y las libertades informativas ex artículo 20.1 d) CE (FJ 6)".

A este respecto, el TC, tras recordar su doctrina sobre la libertad de información, reconoce que la noticia, pese a ser veraz, se ha convertido por el transcurso de los años en una noticia antigua que es traída al presente por medio de la hemeroteca digital. Por la antigüedad de lo transmitido, su relevancia pública puede ser discutida. Con carácter general, la relevancia pública de la noticia viene precisada tanto por la materia de la misma como por la condición de la persona a la que se refiere. Aunque el fondo de la noticia puede ser de interés público (el tráfico de drogas, en el caso ante el TC), la actualidad de la misma puede ser determinante para su valoración en relación con la afectación a los derechos de la persona. En efecto, aunque en abstracto la noticia sea relevante, el TC estima que si se refiere a un hecho acontecido hace años, sin poder mantener una conexión con un hecho actual, "puede haber perdido parte de su interés público o de su interés informativo para adquirir, o no, un interés histórico, estadístico o científico. No obstante su importancia indudable, ese tipo de intereses no guarda una relación directa con la formación de una opinión pública informada, libre y plural, sino con el desarrollo general de la cultura que, obviamente, actúa como sustrato de la construcción de las opiniones. Por esa razón podría ponerse en duda, en estos casos, la prevalencia del derecho a la información [artículo 20.1 d) CE] sobre el derecho a la intimidad de una persona (artículo 18.1 CE) que, pasado un lapso de tiempo, opta por solicitar que estos datos e información, que pudieron tener relevancia pública en su día, sean olvidados. Por supuesto, cuando la noticia en cuestión ha sido digitalizada y se contiene en una hemeroteca, la afectación del derecho a la intimidad viene acompañada del

menoscabo del derecho a la autodeterminación informativa (art. 18.4 CE)" (FJ 7).

En definitiva, pese a reconocer que la noticia es veraz, la materia de la noticia de interés general, y sus protagonistas ni son ni eran personajes públicos (su relevancia pública solo deriva de su participación en un hecho noticiable como es la comisión de un delito), dice el TC en el FJ 8, tras señalar las funciones de la prensa de garante de la publicidad informativa y de archivo de noticias publicadas periódicamente, principal la primera de ellas y secundaria esta última, que "la noticia relata hechos pasados sin ninguna incidencia en el presente. No se trata de una noticia nueva sobre hechos actuales, ni de una nueva noticia sobre hechos pasados, que pueden merecer una respuesta constitucional distinta. Su difusión actual en poco contribuye al debate público". Por el contrario, el daño que la difusión actual de la noticia provoca en los derechos al honor, a la intimidad y a la protección de datos del sujeto resulta especialmente grave, por lo que de descrédito en su vida personal y profesional origina. Además, este daño resulta desproporcionado frente al interés actual que la noticia suscita en el presente, debido principalmente al transcurso del tiempo.

El TC valora el sacrificio que se exige a la libertad de información frente a la intimidad y a la protección de datos, y en las sociedades actuales de la información y con el recurso a las hemerotecas, entiende que la prohibición de indexar datos personales para su uso por el motor de búsqueda interno del medio de comunicación digital es una medida limitativa de la libertad de información idónea, necesaria y proporcionada para evitar una difusión de la noticia que sea lesiva para los derechos mencionados. La limitación para poder acceder a datos personales identificativos de las personas tiene como finalidad impedir que la curiosidad individual y focalizada pueda dar con la noticia de manera fácil a través de los buscadores, pues quien tiene interés público en conocer la noticia, puede acceder por medio de una búsqueda "temática, temporal, geográfica o de cualquier otro tipo" (STC 58/2014, de 4 de junio, FJ 8).

A continuación, debemos analizar que el derecho al olvido está regulado en el artículo 17 RGPD como el derecho a obtener, sin dilación indebida por parte del responsable del tratamiento, la supresión de los datos que a él se refieran y

este a efectuarla en las circunstancias que recoge el precepto. El artículo 15 de la Ley Orgánica 3/2018 se remite para el ejercicio de este derecho a lo establecido en el artículo 17 RGPD, salvo en el caso del ejercicio previo del derecho de oposición del artículo 21.1 RGPD. El derecho al olvido se ejercita, de acuerdo con el artículo 17.1 RGPD, cuando los datos personales ya no son necesarios en relación con los fines para los que se recogieron o tratados de otro modo. La separación entre la finalidad del tratamiento y el dato en cuestión puede venir por distintos motivos (por ejemplo, puede tratarse de datos inadecuados o excesivos), salvo para constatar que la desaparición de la finalidad no justifica ya el tratamiento legal de los datos, por lo que de mantenerse este último se convertiría en un tratamiento ilegal. Cuando los datos han sido tratados ilícitamente desde un principio, se puede solicitar igualmente el derecho al olvido (artículo 17.1 d) RGPD).

Igualmente, puede ejercitarse tal derecho si el interesado ha retirado el consentimiento que sirve de base al tratamiento, de acuerdo con el artículo 6, apartado 1, letra a) o el artículo 9, apartado 2, letra a) y no existe otra base que justifique el tratamiento al margen del consentimiento.

Por último, cuando el interesado se oponga al tratamiento de acuerdo al artículo 21, apartado 1 y no existan otros motivos legítimos prevalentes, o bien si el interesado se opone al tratamiento con arreglo al art. 21, apartado 2. En el primer caso, el derecho de supresión resulta una consecuencia normal y legítima tras el ejercicio del derecho de oposición en las circunstancias que relata el art. 21.1 RGPD. En concreto, cuando el tratamiento sea necesario "para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento" (art. 6.1.e) RGPD), o bien si el tratamiento es necesario para la satisfacción de los intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que no prevalezcan los intereses o derechos y libertades fundamentales del interesado, en particular si el interesado es un niño (art. 6.1 f) RGPD). En el segundo caso, el derecho al olvido se ejercita frente a los tratamientos de datos con fines de mercadotecnia directa ante los cuales se ha ejercitado previamente el derecho de oposición al citado tratamiento, incluida la elaboración de perfiles relacionados con fines de amplitud de mercados comerciales.

En esta sede se observa claramente que el modo de proceder de los motores de búsqueda, evolucionados exponencialmente por el desarrollo de la IA, genera la posibilidad de recopilar y proporcionar información desde una dimensión imposible de asumir por los seres humanos, pero ello provoca también, tangencialmente, el perjuicio de derechos fundamentales, de ahí la necesidad, ya acuciante, de que se regulara el derecho a no verse sometido, debido a la "eficiencia" de la IA, a la primera plana de hechos ocurridos mucho tiempo atrás.

5. Conclusiones

La inteligencia artificial es el presente y el futuro de la humanidad, ya que cada vez más dependemos de la tecnología para realizar nuestras actividades diarias (Martínez Devia 2019). Y el peligro, difícilmente remediable, es la existencia de sesgos en el modo de llegar a resoluciones por ella misma. Por ello, uno de los principales problemas de las soluciones de IA no es la IA en sí, sino cómo van a usar las personas la tecnología IA y los nuevos sesgos psicológicos que se derivan de su empleo. En particular, es necesario prestar especial atención a atribuir responsabilidades a componentes IA sin supervisión y sin adoptar una posición crítica (AEPD, 2020, 49). A ello se une la tendencia, sobre todo a partir de la segunda década del siglo XXI, de avanzar en el ámbito de la transparencia en cuanto al acceso a la información, de hecho en España la Ley 19/2013 supuso un avance considerable en ese aspecto, aunque en el escenario de la IA la transparencia presenta no pocas aristas. Además, esos avances no deben, en ningún caso, suponer una merma de los derechos humanos, recogidos en la Declaración Universal de 1948, ni de los derechos derivados de los pactos internacionales de 1966, ni, en la actualidad, desviarse de los Objetivos de Desarrollo Sostenible. El aspecto ético debe estar presente en toda esta cuestión, ya que aunque el acceso a los documentos públicos tiene una larga trayectoria y regulación, como por ejemplo por parte del Consejo de Europa (2009), la capacidad evolutiva de la IA requiere de la necesaria puesta al día de la regulación y control de la privacidad de y los derechos fundamentales de los ciudadanos.

La evolución tecnológica hace presagiar que las cuestiones relativas al reconocimiento facial, por ejemplo, serán cuestiones de primera magnitud en

cuanto a la protección de derechos de los ciudadanos. La intersección entre avance tecnológico y privacidad será cada vez más difícil de gestionar. Pero no solo hablamos de un futuro próximo: "en agosto de 2019 la autoridad sueca de protección de datos imponía una sanción de 200.000 coronas suecas a una entidad local por utilizar el reconocimiento facial para controlar la asistencia a clase de los alumnos. En noviembre de 2019 la CNIL, el regulador franciés en la materia, publicó un informe titulado "*Reconnaissance faciale: pour un débat à la hauteur des enjeux*" con orientaciones interesantes sobre esta cuestión" (Martínez Vázquez 2019).

Estas cuestiones apuntadas van dirigidas al estudio de una implementación ética de la IA en el derecho, en la sociedad y, en definitiva, en los entornos democráticos en los que se inserta. El no sometimiento a decisiones automatizadas y la posibilidad de ejercer el derecho al olvido son dos muestras de acciones que redundan en una temática más profunda, la protección de la dignidad de las personas, expresamente recogida, de hecho en nuestro artículo 10 CE.

Agradecimientos

Trabajo realizado en el marco del Proyecto MICINN Retos «Derechos y garantías frente a las decisiones automatizadas en entornos de inteligencia artificial, IoT, big data y robótica» (PID2019-108710RB-I00).

6. Bibliografía

AEPD, 2020. *Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial. Una introducción*. Disponible en: https://www.aepd.es/sites/default/files/2020-02/adecuacion-rgpd-ia.pdf

ARELLANO TOLEDO, W., 2007. Las comunidades autónomas en la sociedad de la información: acceso a la información y servicio universal. En COTINO HUESO, L., *Democracia participación y voto a través de las nuevas tecnologías*. Granada: Comares. ISBN: 978-84-9836-232-9.

CASTELLANOS CLARAMUNT, J., 2020. Democracia, Administración pública e inteligencia artificial desde una perspectiva política y jurídica. *Revista Catalana de Dret Públic*, 60, pp. 137-147. ISSN: 1885-5709. https://doi.org/10.2436/rcdp.i60.2020.3344

CONSEJO DE EUROPA, 1950. Convenio Europeo de Derechos Humanos. Roma, 04/11/1950. [Consulta: 30 de noviembre de 2020]. Disponible en: https://www.echr.coe.int/documents/convention_spa.pdf.

CONSEJO DE EUROPA, 2009. Convenio sobre el acceso a los documentos públicos, 18/06/2009. [Consulta: 26 de noviembre 2020]. Disponible en: https://www.oas.org/es/sla/ddi/docs/acceso_informacion_desarrollos_convenio_consejo_europeo.pdf.

CONSEJO DE EUROPA, 2019. *Unboxing artificial intelligence: 10 steps to protect human rights* [Commissioner's Recommendation on Artificial Intelligence and Human Rights]. [Consulta: 30 de noviembre de 2020]. Disponible en: https://www.coe.int/en/web/commissioner/-/unboxing-artificial-intelligence-10-steps-to-protect-human-rights

CORTINA RAMOS, A., 2017. *Humanismo avanzado: para una sociedad biotecnológica*. Madrid: Ediciones Teconté. ISBN: 9788484693963.

COTINO HUESO, L., 2020a. Inteligencia Artificial y vigilancia digital contra la COVID-19 y contra la privacidad. El diablo está en los detalles. *bie3: Boletín IEEE*, 18, pp. 588-597. ISSN-e: 2530-125X. Disponible en: https://publicaciones.defensa.gob.es/media/downloadable/files/links/b/o/boletin_ieee_18.pdf

COTINO HUESO, L., 2020b. Inteligencia artificial, big data y aplicaciones contra la COVID-19: privacidad y protección de datos. *Revista de Internet, Derecho y Política*, 31. ISSN-e: 1699-8154. https://doi.org/10.7238/idp.v0i31.3244

ESPAÑA, 1978. Constitución española. *BOE*, 311, de 23/12/1978. [Consulta: 30 de noviembre de 2020]. Disponible en: https://www.boe.es/buscar/pdf/1978/BOE-A-1978-31229-consolidado.pdf

ESPAÑA, 1985. Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, hecho en Estrasburgo el 28 de enero de 1981. *BOE*, 274, de 15/1/1985. [Consulta: 30 de noviembre de 2020]. Disponible en: https://www.boe.es/boe/dias/1985/11/15/pdfs/A36000-36004.pdf

ESPAÑA, 1985. Ley Orgánica 5/1985, de 19 de junio, del Régimen Electoral General. *BOE*, 147, de 21/6/1985. [Consulta: 30 de noviembre de 2020]. Disponible en: https://www.boe.es/buscar/pdf/1985/BOE-A-1985-11672-consolidado.pdf

ESPAÑA, 1994. Instrumento de ratificación del Acuerdo de Adhesión del Reino de España al Convenio de aplicación del Acuerdo de Schengen de 14 de junio de 1985 entre los Gobiernos de los Estados de la Unión Económica Benelux, de la República Federal de Alemania y de la República Francesa, relativo a la supresión gradual de los controles en las fronteras comunes, firmado en Schengen el 19 de junio de 1990, al cual se adhirió la República Italiana por el Acuerdo firmado en París el 27 de noviembre de 1990, hecho el 25 de junio de 1991. *BOE*, 81, de 5/4/1994. [Consulta: 30 de noviembre de 2020]. Disponible en: https://www.boe.es/boe/dias/1994/04/05/pdfs/A10390-10422.pdf

ESPAÑA, 2001. Pleno. Sentencia 292/2000, de 30 de noviembre de 2000. Recurso de inconstitucionalidad 1.463/2000. Promovido por el Defensor del Pueblo respecto de los arts. 21.1 y 24.1 y 2 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Vulneración del derecho fundamental a la protección de datos personales. Nulidad parcial de varios preceptos de la Ley Orgánica. *BOE* [en línea] núm. 4, de 4 de enero de 2001, pp. 104-118. Disponible en: https://www.boe.es/buscar/doc.php?id=BOE-T-2001-332

ESPAÑA, 2013. Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno. *BOE* [en línea], núm. 295, de 10/12/2013. [Consulta: 26 de noviembre 2020]. Disponible en: https://www.boe.es/buscar/doc.php?id=BOE-A-2013-12887.

ESPAÑA, 2018a. Sala Primera. Sentencia 58/2018, de 4 de junio de 2018. Recurso de amparo 2096-2016. Promovido por D.F.C. y M.F.C., respecto de la sentencia dictada por la Sala de lo Civil del Tribunal Supremo en proceso por vulneración del derecho al honor, la intimidad y la propia imagen entablado frente a Ediciones El País, SL. Vulneración de los derechos al honor, la intimidad y la protección de datos: ejercicio del denominado derecho al olvido respecto de datos veraces que figuran en una hemeroteca digital; prohibición de indexación de nombres y apellidos como medida limitativa de la libertad de información idónea. *BOE*, núm. 164, de 7 de julio de 2018, pp. 68409-68433. Disponible en: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2018-9534

ESPAÑA, 2018b. Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. *BOE*, 294, de 06/12/2018. [Consulta: 30 de noviembre de 2020]. Disponible en: https://www.boe.es/boe/dias/2018/12/06/pdfs/BOE-A-2018-16673.pdf

ESPAÑA, 2020. Orden PCM/1030/2020, de 30 de octubre, por la que se publica el Procedimiento de actuación contra la desinformación aprobado por el Consejo de Seguridad Nacional. *BOE* [en línea], núm. 292, de 05/11/2020. [Consulta: 29 de noviembre de 2020]. Disponible en: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2020-13663.

ESPAÑA MARTÍ, M., 2019. La aplicación práctica de la Ley Orgánica de Protección de Datos y garantía de los derechos digitales. *Diario la Ley*, Sección Ciberderecho, Wolters Kluwer, 34. ISSN: 1989-6913. Disponible en: https://diariolaley.laleynext.es/dll/2019/12/06/la-aplicacion-practica-de-la-ley-organica-de-proteccion-de-datos-y-garantia-de-los-derechos-digitales

MARTÍNEZ DEVIA, A., 2019. La inteligencia artificial, el big data y la era digital: ¿una amenaza para los datos personales? *La Propiedad Inmaterial*, 27, pp. 5-23. ISSN-e: 2346-2116. https://doi.org/10.18601/16571959.n27.01

MARTÍNEZ MARTÍNEZ, R., 2019. De la transparencia estática a la dinámica en las aplicaciones móviles: lecciones aprendidas del caso de «La Liga de Futbol Profesional». *Diario la Ley*, Wolters Kluwer, 9463. ISSN: 1989-6913.

MARTÍNEZ MARTÍNEZ, R., 2020a. Tecnología de verificación de identidad y control en exámenes online. *Revista de educación y derecho. Education and law review*, 22, (Covid-19: Docencia online y protección de derechos y garantías fundamentales). ISSN: 2013-584X. https://doi.org/10.1344/REYD2020.22.32357

MARTÍNEZ MARTÍNEZ, R., 2020b. Los tratamientos de datos personales en la crisis del COVID-19. Un enfoque desde la salud pública. *Diario la Ley*, Wolters Kluwer, 9604. ISSN: 1989-6913.

MARTÍNEZ VÁZQUEZ, F., 2019. El uso ilícito de datos personales un año después de la aprobación de la Ley Orgánica 3/2018, de 5 de diciembre. *Diario la Ley*, Sección Ciberderecho, Wolters Kluwer, 34. ISSN: 1989-6913. Disponible en: https://repositorio.comillas.edu/xmlui/bitstream/handle/11531/44948/Diario%20la%20Ley%205%20de%20diciembre%202019.pdf?sequence=-1&isAllowed=y

ONU, 1948. Asamblea General, *Declaración Universal de Derechos Humanos*, 10 diciembre 1948, núm. 217 A (III), [Consulta: 25 de noviembre de 2020]. Disponible en: https://www.refworld.org.es/docid/47a080e32.html.

ONU, 1966. Asamblea General, *Pacto Internacional de Derechos Civiles y Políticos. Adoptado y abierto a la firma, ratificación y adhesión por la Asamblea General en su resolución 2200 A (XXI), de 16 de diciembre de 1966*, 16 Diciembre 1966, Naciones Unidas, Serie de Tratados, vol. 999, p. 171, [Consulta: 25 de noviembre de 2020]. Disponible en: https://www.refworld.org.es/docid/5c92b8584.html.

ONU, 2015. *Resolución A/RES/70/1 Transformar nuestro mundo: la Agenda 2030 para el Desarrollo Sostenible*, 25 de noviembre de 2015. [Consulta: 25 de noviembre de 2020]. Disponible en: http://www.un.org/es/comun/docs/?symbol=A/RES/70/1.

RALLO LOMBARTE, A., 2019a. El nuevo derecho de protección de datos. *Revista Española de Derecho Constitucional*, 116, pp. 45-74. ISSN: 0211-5743.

RALLO LOMBARTE, A., 2019b. La LOPDGDD y el art. 58 bis LOREG. *Diario la Ley*, Sección Ciberderecho, Wolters Kluwer, 34. ISSN: 1989-6913.

RALLO LOMBARTE, A., 2020. Una nueva generación de derechos digitales. *Revista de estudios políticos*, 187, pp. 101-135. ISSN: 0048-7694.

RAMÓN FERNÁNDEZ, F., 2020. El acceso a los datos y contenidos gestionados por prestadores de servicios de la sociedad de la información de personas fallecidas: análisis de los límites. *MÉI: Métodos de Información,* 11(20), pp. 59-87. ISSN: 2173-1241. DOI: https://dx.doi.org/10.5557/IIMEI11-N20-059087.

REBOLLO DELGADO, L., y SERRANO PÉREZ, M. M., 2019. *Manual de Protección de Datos* (3ª edición). Madrid: Dykinson, S.L. ISBN: 978-84-1324-089-3.

SAMANO, L. A., y ARELLANO TOLEDO, W., 2010. Las tres facultades del derecho a la información en la web 2.0 y sus consideraciones éticas. En *Las audiencias activas, nuevas formas de participación pública. Consideraciones éticas y jurídicas*. 8.º Congreso Internacional de Ética y Derecho de la Información. Valencia: Fundación COSO, pp. 337-355.

SANCHO LÓPEZ, M., 2019. El derecho al olvido y el requisito de veracidad de la información. Comentario a la STS de España núm. 12/2019, de 11 de enero (ROJ/19/2019). *Revista Boliviana de Derecho*, 28, pp. 432-443. ISSN: 2070-8157.

TEJERINA RODRÍGUEZ, O., 2019. Lo que nos falta de la LOPDGDD. *Diario la Ley*, Sección Ciberderecho, Wolters Kluwer, 34.

UNIÓN EUROPEA, 2000. Carta de los Derechos Fundamentales de la Unión Europea. *Diario Oficial de las Comunidades Europeas*, C 364 [Consulta: 29 de noviembre de 2020]. Disponible en: https://www.europarl.europa.eu/charter/pdf/text_es.pdf

UNIÓN EUROPEA, 2012. Versión consolidada del Tratado de Funcionamiento de la Unión Europea. *Diario Oficial de la Unión Europea* (2012/C 326/47). [Consulta: 27 de noviembre de 2020]. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:12012E/TXT&from=ES

UNIÓN EUROPEA, 2016. 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) (Texto pertinente a efectos del EEE). DOUE, L119/1, de 04/05/2016. *Diario Oficial de la Unión Europea* [Consulta: 30 de noviembre de 2020]. Disponible en: https://www.boe.es/doue/2016/119/L00001-00088.pdf