



# Inteligencia Artificial, derecho administrativo y protección de datos personales. Entre la dignidad de la persona y la eficacia administrativa

ARTIFICIAL INTELLIGENCE, ADMINISTRATIVE LAW AND PERSONAL DATA PROTECTION. IN BETWEEN PERSON'S DIGNITY AND ADMINISTRATIVE EFFICIENCY

**José Luis Domínguez Álvarez**

Personal Investigador en Formación (FPU)<sup>1</sup>

Área de Derecho Administrativo

Universidad de Salamanca

[jldoal@usal.es](mailto:jldoal@usal.es) 0000-0003-4101-9632

Recibido: 30 de abril de 2021 | Aceptado: 03 de junio de 2021

## RESUMEN

Es un lugar común referirse sistemáticamente a las transformaciones del Derecho público, circunstancia esta que, como insiste en señalar buena parte de la doctrina, se encuentra agravada en el caso del Derecho administrativo. El avance tecnológico y los crecientes procesos de modernización de las diferentes Administraciones públicas, las cuales no son ajenas en forma alguna al actual tsunami digital, ha permitido evidenciar la necesidad de contar con un ordenamiento jurídico-administrativo adaptado a la realidad en red, capaz de combatir el pernicioso alcance que el impulso de la digitalización y datificación de la sociedad posee en la esfera vital de la ciudadanía. En efecto, el transcurso del tiempo y el progreso digital no han hecho más que acentuar la preeminencia del Derecho administrativo, entendido como dique de contención capaz de preservar la dignidad de la persona ante las tribulaciones propiciadas por la (r)evolución tecnológica. Dificultosa travesía que encuentra en la tutela jurídica de la protección de datos de carácter personal uno de sus principales desafíos, y a cuyo estudio se dedican las próximas páginas.

## PALABRAS CLAVE

Inteligencia artificial  
Administración pública  
Derecho administrativo  
Protección de datos personales  
Dignidad  
Eficacia administrativa

1. Personal Investigador en Formación (FPU 17/01088) Ministerio de Educación, Cultura y Deporte. Miembro del Grupo de Investigación Reconocido "Next Generation UE – Derecho Administrativo" de la Universidad de Salamanca (NEGUEDA-USAL).

## ABSTRACT

It became a systematical tendency to refer to all the changes developing in Public law, a circumstance which, as much of the literature insists on pointing out, is aggravated in the case of Administrative law. The technological advance and the increasing processes of modernization of the different public administrations, which are not foreign in any way to the current digital tsunami, has made it possible to demonstrate the need for a legal system -adapted to the "in network" reality, in order to be able to combat the pernicious scope that the impulse of society digitalization and datification possesses have in the vital sphere of the citizenship. In fact, the pass of time and the digital progress have only accentuated the pre-eminence of Administrative law, understood as a barrier capable of preserve person's dignity do to the tribulations caused by technological (r)evolution. Difficult journey that finds in the legal protection of personal data one of its main challenges, and to whose study the next pages are dedicated.

## KEYWORDS

Artificial intelligence  
Public administration  
Administrative law  
Personal data protection  
Dignity  
Administrative effectiveness

## I. EL DERECHO PÚBLICO ANTE LAS ABRUPTAS TRANSFORMACIONES PROPICIADAS POR EL TSUNAMI DE LA DIGITALIZACIÓN Y DATIFICACIÓN DE LA SOCIEDAD

Hablar de (r)evolución digital en nuestros días requiere, necesariamente, hacer referencia obligada al universo de los sistemas algorítmicos<sup>2</sup> y al fenómeno de la Inteligencia Artificial. Esta poderosa herramienta está llamada a ser una de las cinco tecnologías emergentes encargadas de transformar las diferentes esferas de la sociedad en un horizonte temporal no muy lejano (United States Government Accountability Office, 2018: 26). Su importancia no pasa inadvertida para nadie, tampoco para el conjunto de las Administraciones públicas, toda vez que nos encontramos ante el fundamento de la incipiente cuarta revolución industrial<sup>3</sup> (Schwab, 2016: 13-20), hito que representa la

2. En los últimos tiempos hemos asistido a la proliferación del universo de los algoritmos, entendidos como «un conjunto metódico de pasos que pueden emplearse para hacer cálculos, resolver problemas y alcanzar decisiones. Un algoritmo no es un cálculo concreto, sino el método que se sigue cuando se hace el cálculo» (Harari, 2016: 100).

3. Numerosos autores, insisten en subrayar que esta cuarta oleada industrializadora no puede entenderse de otra forma que no sea contextualizándola dentro de la Era de la Información, fenómeno anterior, descrito y teorizado extraordinariamente por Castells como «(...) un acontecimiento histórico al menos tan importante como lo fue la revolución industrial del siglo XVIII, inductor de discontinuidad en la base material de la economía, la sociedad y la cultura. A diferencia de cualquier otra revolución, el núcleo de la transformación que estamos experimentando en la revolución en curso remite a las tecnologías del procesamiento de la información y de la comunicación. La tecnología de la información es a esta revolución lo que las nuevas fuentes de energía fueron a las sucesivas revoluciones industriales del motor de vapor a los combustibles fósiles e incluso a la energía nuclear, ya que la generación y distribución de energía fue el elemento clave subyacente en la sociedad industrial» (Castells, 2008: 57).

apertura de un periodo de profundas transformaciones tanto para las personas, como para la sociedad y el propio Derecho (Ponce, 2019: 1-52).

Sin embargo, esta escurridiza realidad, capaz de atraer la atenta mirada de gran parte de la academia y la doctrina iuspublicista (Fernando y Terrón, 2019: 397-410; Terrón y Domínguez, 2019, 230-241; Huergo, 2020: 23-87), no es un fenómeno de reciente aparición. En efecto, el término Inteligencia Artificial (en adelante IA), fue empleado por vez primera<sup>4</sup> en el año 1956 por John McCarthy para referirse a «la ciencia y la ingeniería de crear máquinas inteligentes, especialmente programas de computación inteligente» (McCarthy *et al*, 1955). A grandes rasgos podemos definir este fenómeno como aquella ciencia compleja construida con fundamentos extraídos principalmente de la filosofía, las matemáticas, la economía, la teoría de la información, las neurociencias, la psicología, la ingeniería computacional (hardware y software), la teoría del control, la cibernética y la lingüística (Russel y Norvig, 1995: 7-19).

Sin embargo, como es sabido por todos, fue Alan Turing quien primero desarrollo una visión general de la IA en su famoso artículo «*Computing Machinery and Intelligence*» (1950), obra en la que introdujo el que devino en llamarse Test de Turing, el aprendizaje automático, los algoritmos genéticos y el aprendizaje por refuerzo. Ciertamente, en este y otros trabajos se vislumbra el pensamiento premonitorio de un investigador, Turing, que argumentaba ya en el pasado siglo que en un plazo de unos 50 años habría ordenadores inteligentes capaces de llevar a cabo deducciones lógicas, de aprender adquiriendo nuevos conocimientos —tanto inductivamente como por experiencia y evolución— y capaces de comunicarse mediante interfaces humanizadas (Turing, 1937: 230-265; Turing, 1950: 433-460; Turing, 1968: 107-127).

Transcurrido más de medio siglo desde esa primera referencia a la IA, el Grupo de Alto Nivel en Inteligencia Artificial (AI – HLEG) creado por la Comisión Europea con la misión de desarrollar la Estrategia Europea de Inteligencia Artificial ha utilizado dicho término para hacer referencia a aquellos «*sistemas que manifiestan un comportamiento inteligente, al ser capaces de analizar el entorno y realizar acciones, con cierto grado de autonomía, con el fin de alcanzar objetivos específicos*» (Comisión Europea, 2018:1).

La amplia concepción europeísta de este fenómeno<sup>5</sup> permite entrever que bajo la etiqueta IA subyacen múltiples y variadas tipologías de soluciones tecnológicas que

---

4. Es comúnmente aceptado que la génesis de la IA está asociada a los nombres de Warren McCulloch y Walter Pitts, quienes en un trabajo titulado «*A logical calculus of the ideas immanent in nervous activity*» propusieron un modelo computacional constituido por neuronas artificiales (McCulloch y Pitts, 1943: 115-133).

5. La Comisión Europea presentó el pasado 21 de abril el nuevo paquete de normas y medidas, así como una propuesta de reglamento sobre la inteligencia artificial. Se trata del primer marco jurídico sobre esta tecnología y está enfocado a garantizar la seguridad y los derechos fundamentales de las personas y las empresas, al mismo tiempo que pretende convertir a Europa en el centro mundial de la inteligencia artificial apostando por la inversión y la innovación (Comisión Europea, 2021: 2 y ss.).

La propuesta de reglamento clasifica los sistemas de IA en cuatro niveles diferenciados atendiendo a un enfoque de riesgo, atendiendo, principalmente, a la severidad del daño y la probabilidad de que este ocurra, y, en consecuencia, a mayores cotas de riesgo mayor número e intensidad de obligaciones deberá respetar el responsable de los sistemas de IA:

emplean distintas técnicas (Cotino, 2019: 4), y entre las que conviene destacar aquellas que sustentan su actuación en el denominado machine learning o aprendizaje automatizado<sup>6</sup> (Agencia Española de Protección de Datos, 2020: 2).

- Riesgo inadmisibles. Se prohibirá un conjunto muy limitado de usos especialmente nocivos de la IA que contravienen los valores de la Unión al violar los derechos fundamentales (por ejemplo, puntuación social por parte de los Gobiernos, explotación de los puntos débiles de los niños, uso de técnicas subliminales y, salvo contadas excepciones, determinados sistemas de identificación biométrica remota en directo en espacios públicos con fines policiales).
- Alto riesgo. Este nivel abarca, entre otras, tecnologías de IA empleadas en infraestructuras críticas, como transportes, que pueden poner en peligro la vida y la salud de los ciudadanos; formación educativa o profesional que pueden determinar el acceso a la educación y la carrera profesional o componentes de seguridad de los productos, como pudiera ser la aplicación de IA en cirugía asistida por robots. El reglamento también tiene en cuenta otros sistemas en áreas como la aplicación de las leyes, la administración de justicia o la gestión de la migración, el asilo y el control de fronteras.
- De conformidad con la regulación propuesta, los sistemas de alto riesgo deberán aportar un registro de la actividad para garantizar la trazabilidad de los resultados y deberán contar con sistemas adecuados de evaluación y mitigación de riesgo o responder a una alta calidad de los conjuntos de datos que alimentan el sistema, aportar documentación detallada sobre el sistema y su finalidad, proporcionar información clara y adecuada al usuario y tener un alto nivel de solidez, seguridad y precisión, así como contemplar medidas apropiadas de supervisión humana para minimizar el riesgo.
- Riesgo limitado. En este nivel se incluyen sistemas como chatbots o robots conversacionales, que deberán cumplir unas medidas específicas de transparencia. A este respecto, se establece la obligación de informar a los usuarios de que están interactuando con una máquina para poder tomar una decisión informada de continuar o no.
- Riesgo mínimo o nulo. La propuesta de la Comisión permite el uso gratuito de aplicaciones tales como videojuegos basados en inteligencia artificial o filtros de correo basura. Ya que la amplia mayoría de los sistemas de IA entran en esta categoría, el proyecto de Reglamento no interviene aquí debido a su limitado riesgo sobre los derechos o la seguridad de los individuos (Huergo Lora, 2021).

6. Existen diversas formas de aproximarse a una solución de IA: mediante redes neuronales, sistemas basados en reglas, lógica borrosa, aprendizaje automático, sistemas expertos, sistemas adaptativos, algoritmos genéticos, sistemas multiagente, etc., términos que se solapan unos con otros. Lo que pretenden todas estas técnicas es conseguir modelos para tratar sistemas complejos para los que no se sabe cómo, o no es posible tratar con algoritmos secuenciales, por su dificultad para modelar comportamientos regidos por múltiples variables. Entre estas variables se establecen relaciones no lineales, o que no es posible aproximar a métodos lineales, y que incluso pueden variar con el tiempo.

Una de las ramas de la IA con más éxito en aplicaciones comerciales es el Aprendizaje Automático o Machine Learning (ML). El ML diseña modelos predictivos que construyen por sí mismos la relación entre las variables a estudiar mediante el análisis de un conjunto inicial de datos, la identificación de patrones y el establecimiento de criterios de clasificación. Una vez fijados los criterios, al introducir un nuevo conjunto de datos el componente IA es capaz de realizar una inferencia. El aprendizaje automático está, relacionado con las técnicas de minería de datos, optimización y big data. A su vez, existen distintos tipos de aprendizaje automático como el supervisado, no supervisado, de refuerzo y sus variantes, que emplean distintas técnicas. Así mismo se encuentran especializaciones del ML como el Deep Learning o Aprendizaje Profundo, y diferentes modelos de aprendizaje, como el centralizado, el descentralizado o el federado. Un sistema con un componente de IA podemos decir que es adaptativo cuando el modelo de inferencia se ajusta dinámicamente en función de cada nuevo conjunto de datos de entrada, refinando las relaciones ya establecidas.

En este punto, conviene recordar que la IA se fundamenta, en gran medida, en la utilización de algoritmos y de datos (West & Allen, 2018), en muchos casos, de carácter personal. Esta potente combinación de elementos empleada de manera adecuada, ofrece una oportunidad única para fortalecer la preeminencia de la Administración pública, ya sea mediante el impulso de nuevas formas de ejercicio de sus potestades tradicionales, en aras de una mayor eficacia y eficiencia administrativa, o por medio de la configuración de nuevas fórmulas de intervención pública orientadas a la consecución de los intereses generales —art. 103.1 CE— (Domínguez, 2021a: 205-227). Estas premisas cobran una especial relevancia en sectores esenciales, estrechamente imbricados con la esencia del Estado y con la propia razón de ser del poder público, tales como la naturaleza prestacional de las Administraciones públicas, el fortalecimiento de la seguridad, la salvaguarda de los derechos y libertades fundamentales de la ciudadanía o la pervivencia de los sistemas democráticos (Comisión Europea, 2020a: 2), cuestiones que se ven seriamente amenazadas por el surgimiento de nuevos desafíos que se vislumbran ante el avance del horizonte de la digitalización, a saber: incremento de la ciberdelincuencia; aparición de nuevas formas de desigualdad; proliferación de *fake news*; alteración de los procesos electorales; ausencia de una verdadera cultura de la privacidad; mayor exposición de las infraestructuras críticas del Estado; dependencia tecnológica, etc.

Todos estos planteamientos posibilistas no deben obviar que la IA es ya en nuestros días una realidad tangible<sup>7</sup>, en la medida en que constituye un componente más de los

---

7. Los avances en la potencia informática, la disponibilidad de enormes cantidades de datos y el diseño de nuevos algoritmos han permitido el despegue de la IA en los últimos años, concediéndole un papel central en la transformación digital de la sociedad, lo que la ha convertido en una de las principales prioridades de la Unión Europea. En efecto, la IA está cada vez más presente en nuestras vidas: sirve para ayudar a que la ciudadanía mejore la atención y asistencia sanitaria, para incrementar la seguridad de los medios de transporte y para impulsar productos y servicios personalizados, baratos y duraderos en sectores esenciales, tales como la economía verde y circular, maquinaria, agricultura, salud, moda, turismo, etc. También facilita el acceso a la información, educación y formación, lo que se puso especialmente de manifiesto con la necesidad de generalizar el aprendizaje a distancia tras el estallido de la crisis sociosanitaria propiciada por la COVID-19. Además, la IA puede contribuir a hacer de los lugares de trabajo espacios más seguros, y a generar nuevos nichos de empleo a medida que la industria y las empresas avancen en el camino hacia la adaptación tecnológica. La IA también está llamada a disponer de un papel protagonista en la consecución de los objetivos del Pacto Verde Europeo (Fernández de Gatta, 2020) y la modernización de la actividad prestacional de las Administraciones públicas, mediante el refuerzo de servicios públicos esenciales tales como el transporte público, la educación, la energía o la gestión de los residuos.

Ahora bien, los resultados de la IA dependen de su uso y de los datos utilizados. Existe la posibilidad de sesgar, intencional o involuntariamente, tanto el diseño como los datos. Otro de los peligros es utilizar la inteligencia artificial para tomar decisiones influenciadas por la etnia, el sexo o la edad incluidos en los datos al contratar o despedir, ofrecer préstamos o incluso en procesos penales. La IA también supone riesgos para la privacidad y la protección de datos al utilizarse, por ejemplo, en equipos de reconocimiento facial o para el seguimiento en línea y la creación de perfiles de personas. Así mismo, esta tecnología presenta riesgos para la democracia, al crear, por ejemplo, cámaras de eco por internet basadas en el comportamiento previo de alguien en la red, al mostrar solo un contenido específico. Los sistemas de IA también pueden usarse para crear vídeos, audios o imágenes falsos pero realistas, conocidos como «*deepfakes*». Este contenido puede implicar riesgos financieros, daños reputacionales y problemas en las tomas de decisiones. Todo esto podría conducir a la separación

tratamientos de datos realizados por los responsables y que, en muchos casos, aparece en forma de soluciones desarrolladas por terceros, todo ello sin que exista una ordenación normativa del alcance y de los límites a los que debe estar sujeta esta poderosa herramienta. En efecto, como ha reconocido la propia Unión Europea en diversos pronunciamientos, la IA genera numerosas dudas entre los usuarios, investigadores, especialistas, autoridades y la propia industria encargada de su desarrollo. En singular, estas preocupaciones se centran en lo que concierne a los aspectos relativos al cumplimiento normativo, el respeto de los derechos y libertades fundamentales de los interesados (privacidad, igualdad de género, dignidad, etc.) o la seguridad jurídica de todos los intervinientes en aquellos procesos en los que la innovación digital se erige como componente primordial; cuestiones esenciales que, ante la inacción de los poderes públicos, terminan por constituir un importante freno para el correcto desarrollo tecnológico<sup>8</sup>.

Con la finalidad de disipar los interrogantes que envuelven el prodigioso avance de las nuevas tecnologías (Comisión Europea, 2020b), en especial la IA, es urgente que el poder público ofrezca una respuesta decidida, tendente al establecimiento de «los cimientos de un Derecho de la Inteligencia Artificial, cuyo principio básico sea proteger la naturaleza humana biocultural de los peligros derivados del desarrollo transhumanista<sup>9</sup> de la IA» (López, 2020: 163). Esta tarea, lejos de presentarse como un quehacer sencillo, se convierte en nuestros días en una complicada y necesaria travesía que encuentra en el trasiego de la burocrática prosa de las normas que componen el Derecho Administrativo, el paulatino reconocimiento de los derechos digitales, la inclusión de la *perspectiva de género* en los procesos de desarrollo de los sistemas algorítmicos o la plena garantía del derecho a la protección de datos personales<sup>10</sup> (Comisión Europea, 2020b: 4), algunas

---

y polarización en la esfera pública y manipular las elecciones. De igual forma, la libertad de reunión y protesta está también amenazada por la IA, ya que ésta podría rastrear y controlar a las personas vinculadas a ciertas creencias o acciones.

8. Como ha señalado recientemente la Comisión Europea, «la inteligencia artificial se está desarrollando rápido. Cambiará nuestras vidas, pues mejorará la atención sanitaria, aumentará la eficiencia de la agricultura, contribuirá a la mitigación del cambio climático y a la correspondiente adaptación, mejorará la eficiencia de los sistemas de producción a través de un mantenimiento predictivo, aumentará la seguridad de los europeos y nos aportará otros muchos cambios que de momento solo podemos intuir. Al mismo tiempo, la IA conlleva una serie de riesgos potenciales, como la opacidad en la toma de decisiones, la discriminación de género o de otro tipo, la intromisión en nuestras vidas privadas o su uso con fines delictivos» (Comisión Europea, 2020a: 2).

9. El transhumanismo es un movimiento cultural e intelectual internacional que tiene como objetivo final transformar la condición humana mediante el desarrollo y fabricación de tecnología ampliamente disponibles, que mejoren las capacidades humanas, tanto a nivel físico como psicológico o intelectual. Los pensadores transhumanistas estudian los posibles beneficios y peligros de las nuevas tecnologías que podrían superar las limitaciones humanas fundamentales, como también la tecnoética adecuada a la hora de desarrollar y usar esas tecnologías (Ferry, 2017: 20).

10. Desde 2014, la Comisión Europea ha adoptado una serie de medidas de profundo calado. El Reglamento General de Protección de Datos ha permitido crear un sólido marco para la confianza digital. Otras iniciativas que han establecido las bases para el desarrollo de la economía de los datos son el Reglamento relativo a la libre circulación de datos no personales, el Reglamento sobre la Ciberseguridad y la Directiva sobre datos abiertos.

de las estaciones obligatorias en las que debe detenerse el itinerario que la sociedad debe emprender hacia el ansiado «humanismo tecnológico»<sup>11</sup>.

Asistimos, por tanto, a una revolución silenciosa (Rodríguez, 2021:159-178) que, sin aparente resistencia, amenaza con transformar radicalmente nuestra realidad social, lo que exige revigorizar el papel del Derecho, entendido este como instrumento de ordenación social. Ahora bien, las relaciones entre el ordenamiento jurídico y la innovación tecnológica parecen estar desde sus inicios en una situación de conflicto permanente (Esteve, 1999), toda vez que el avance digital plantea una serie de interrogantes indiscutibles para ciertos valores constitucionales y derechos fundamentales, entre los que se encuentran el derecho a la igualdad, el derecho a la intimidad y la protección de datos de carácter personal, e incluso la propia seguridad jurídica, instituciones todas ellas cuyo contenido esencial parece diluirse ante los envites propiciados por los vertiginosos procesos de digitalización y datificación a los que se expone el conjunto de la población en nuestros días.

## II. EL PAULATINO DESPLIEGUE DE LA ADMINISTRACIÓN AUTOMATIZADA Y SUS IMPLICACIONES PARA LA ESFERA VITAL DE LA CIUDADANÍA

Es habitual referirse sistemáticamente a las transformaciones del Derecho público, circunstancia esta que, como insisten precursores muy autorizados, se encuentra agravada en el caso del Derecho administrativo (Duguit, 1913; Bauer, 1992; Muñoz, 2011; Parejo, 2012). No en vano, Hauriou en 1916 escribía en el prólogo de la segunda edición de sus *Principes de droit public*, haciendo referencia a esta condición de continuo cambio de las normas que integran el Derecho Administrativo<sup>12</sup>, que los juristas de la época vivían en un «*état perpétuellement révolutionnaire*» (Hauriou, 1916: 11).

Un siglo después, el Derecho administrativo se enfrenta a un *nuevo tiempo de tribulación*, intentando comprender las abruptas transformaciones provocadas por los profundos procesos de digitalización y datificación que está experimentando la sociedad, lo que exige no solamente la adopción de respuestas jurídico-administrativas innovadoras para preservar la vigencia de los intereses públicos en liza, ante las virulentas acometidas propiciadas por el desarrollo tecnológico, sino también *rediseñar* los esquemas normativos<sup>13</sup> de tal forma que permitan incorporar los innumerables avances propiciados al calor de esta cuarta revolución industrial en la acción cotidiana de las diferentes

11. Hay varias formas de afrontar el mundo digital donde todos estamos inmersos: «ignorándolo, o haciendo cuerpo común con él, o sirviéndose de sus adelantos para conseguir ciertos fines, o de estas dos últimas maneras conjuntamente, postura que sería la más completa y efectiva» (Romorajo, 2019: 11).

12. Dos de las características más destacadas del Derecho administrativo son la velocidad y la continuidad con que se transforma (Cassese, 2006: 188).

13. La reciente promulgación del tardío Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos constituye una manifestación palmaria de esta acuciante necesidad (Campos, 2021: 14).

Administraciones públicas<sup>14</sup>, especialmente en lo que se refiere a la mejora y simplificación de las relaciones entre los administrados y las Administraciones públicas o la modernización de los servicios públicos prestados por estas últimas (Valero, 2006: 115).

Ahora bien, la preocupación por clarificar la *interconexión* existente entre informática y Derecho no es una novedad, se remonta a inicios de la segunda mitad del siglo XX, momento en el que algunos avezados estudiosos vislumbraron, con carácter premonitorio, el advenimiento de un nuevo concepto de Administración pública (Mehl, 1957: 410-419), coincidente en mayor o menor medida con lo que hoy denominamos *Administración automatizada*<sup>15</sup>.

En efecto, la aparición de nuevas tecnologías ha dado lugar a una revolución tecnológica de indudables consecuencias en el ámbito económico y social que está afectando, de igual forma, a la Administración pública<sup>16</sup> y, con ello, a la propia forma de entender el Derecho administrativo<sup>17</sup>. Ante esta tesitura, el legislador español adoptó la Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos (LAECSP) hito normativo por el cual se reconoce el derecho de los ciudadanos a relacionarse con las Administraciones públicas por medios electrónicos y se regulan los aspectos básicos de la utilización de las tecnologías de la información en la actividad administrativa (Valero, 2007; Palomar, 2007; Puente, 2007; o Martínez, 2007). De igual forma, el anexo de definiciones de la LAECSP realiza una primera definición del concepto de actuación administrativa automatizada, conceptualizando la misma como aquella «*actuación administrativa producida por un sistema de información adecuadamente programado sin necesidad de intervención de una persona física en cada caso singular*».

No obstante, conviene señalar que esta institución jurídica ya existía en nuestro ordenamiento con anterioridad a esta Ley<sup>18</sup>. Efectivamente, la Ley 58/2003, de 17 de diciembre,

---

14. Como han subrayado diversos teóricos, la tecnología informática supone para las Administraciones públicas la aparición de un factor nuevo para afrontar sus problemas crónicos (Martínez, 1984: 133).

15. De esta forma, la Administración pública tradicional (basada en el binomio hombre-papel) da paso a una nueva fase, la Administración automatizada, «en la que el ordenador sustituye (aunque parcialmente) ya sea el elemento humano, efectuando directamente los cálculos y las comparaciones exigidos por un acto administrativo, así como el elemento papel, ya que la memoria magnética sustituye los archivos y el medio de comunicación es el impulso eléctrico» (Frosini, 1984: 453-454).

16. Ciertamente, como ya indicara Martín Delgado hace más de una década, «la revolución tecnológica ha tenido su eco en el ámbito de lo público y, en concreto, en el ámbito de la Administración. Lo tuvo hace unos años *ad intra*, cuanto comenzaron a utilizarse medios informáticos y electrónicos para la realización de las distintas gestiones que llevan a cabo las unidades administrativas (ordenadores, faxes, programas, etc.) y, más recientemente, lo está teniendo también *ad extra*, esto es, en las relaciones de los distintos órganos administrativos con los ciudadanos» (Martín, 2009: 310-311).

17. Todos estos cambios alumbrados por el desarrollo tecnológico permiten incluso plantear la reconfiguración de las categorías jurídicas, ya que el uso de los algoritmos puede modificar el comportamiento y la forma de vida de los individuos, incidiendo en última instancia de forma decisiva en la reconfiguración de la sociedad (Fernando, 2003).

18. Recuérdese que ya la propia Ley 30/1992, de 26 de noviembre, se propuso incorporar las posibilidades de la informática a la acción administrativa. Mucho antes incluso, como subraya RIVERO ORTEGA «la Ley de Procedimiento Administrativo de 1958 avanzó tales previsiones, teniendo presentes las rudimentarias técnicas de su momento histórico» (Rivero, 2016: 77).

General Tributaria contemplaba ya en su art. 96, referente a la utilización de tecnologías informáticas y telemáticas, el empleo por parte de la Administración tributaria de las nuevas tecnologías en el desarrollo de su actividad y para el ejercicio de sus competencias<sup>19</sup>.

La promulgación de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones públicas (en adelante, LPACAP) supuso un paso decisivo en el impulso de la digitalización administrativa, al reconocer, por un lado, ex art. 13.b) LPACAP, el derecho de toda persona física o jurídica «*a comunicarse con las Administraciones públicas a través de un Punto de Acceso General electrónico de la Administración*» (Martín, 2016: 23). Y, por otro, aunque ya solamente para las personas físicas, el derecho a «*elegir en todo momento si se comunican con las Administraciones públicas para el ejercicio de sus derechos y obligaciones a través de medios electrónicos*» (art. 14 LPACAP). Disposiciones que, como ha insistido en subrayar buena parte de la doctrina, representan la generalización de «la obligación de relacionarse electrónicamente con la Administración con escasas garantías» (Cotino, 2018: 6) o la «progresiva transfiguración del derecho a relacionarse por medios electrónicos en un deber» (Gamero, 2016: 15).

Por su parte, la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público (en adelante, LRJSP) incorpora menos referencias a la administración electrónica, pero suficientemente significativas. De esta forma, la Ley recoge, con las adaptaciones necesarias, las normas hasta ahora contenidas en la Ley 11/2007, de 22 de junio, en lo relativo al funcionamiento electrónico del Sector público, y algunas de las previstas en el Real Decreto 1671/2009, de 6 de noviembre, por el que se desarrolla parcialmente la anterior. Se integran así materias que demandaban una regulación unitaria, como corresponde con un entorno en el que la utilización de medios electrónicos ha de ser lo habitual, como la firma<sup>20</sup> y sedes electrónicas, el intercambio de datos en entornos cerrados de comunicación y la actuación administrativa automatizada. Para ello, también se contempla como nuevo principio de actuación la interoperabilidad de los medios electrónicos y sistemas y la prestación conjunta de servicios a los ciudadanos<sup>21</sup>.

De igual forma, establece una *vacua* regulación de la actuación administrativa automatizada, una vez más sin las debidas garantías que contribuyan a dotar de certidumbre el despliegue de esta *nueva* forma de acción administrativa. Así, el art. 41 LRJSP preceptúa lo siguiente:

1. Se entiende por actuación administrativa automatizada, cualquier acto o actuación realizada íntegramente a través de medios electrónicos por una

19. Concretamente, en el tercer apartado de ese mismo artículo hace una mención directa a la posibilidad de adopción de decisiones de forma automatizada, al precisar que «*cuando la Administración tributaria actúe de forma automatizada se garantizará la identificación de los órganos competentes para la programación y supervisión del sistema de información y de los órganos competentes para resolver los recursos que puedan interponerse*» (Martín, 2009: 355-356).

20. Esta cuestión ha sido reforzada recientemente mediante la promulgación de la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.

21. *Vid.* Preámbulo de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

Administración pública en el marco de un procedimiento administrativo y en la que no haya intervenido de forma directa un empleado público.

2. En caso de actuación administrativa automatizada deberá establecerse previamente el órgano u órganos competentes, según los casos, para la definición de especificaciones, programación, mantenimiento, supervisión y control de calidad y, en su caso, auditoría del sistema de información y de su código fuente. Asimismo, se indicará el órgano que debe ser considerado responsable a efectos de impugnación.

Todo ello nos conduce a un contexto plagado de incertidumbre e inseguridad, en el que las Administraciones públicas comienzan a implementar la utilización de la IA en el desarrollo de sus actividades cotidianas y, muy especialmente, en la prestación de servicios públicos, en vista de las enormes potencialidades que estas soluciones tecnológicas comportan<sup>22</sup>. Ahora bien, la implementación paulatina de estas herramientas y el progresivo despliegue de la actuación administrativa automatizada presenta importantes interrogantes no solamente desde el prisma de los derechos y libertades fundamentales de la ciudadanía (dignidad, privacidad, igualdad, etc.), sino también acerca del papel que el Derecho positivo (Hoffmann-Riem, 2018: 59), como instrumento de ordenación de la sociedad, juega en una realidad cada vez más digitalizada y sometida a los avances científicos (Canals, 2019: 2).

Una de las principales preocupaciones, al menos a medio y largo plazo, es la de acotar el alcance y desarrollo de los sistemas algorítmicos, así como promover el establecimiento de mecanismos de control, cuya implementación exponencial, también en el ámbito de lo público, nos sitúa en un terreno pantanoso<sup>23</sup>. Se trata, por tanto, de la dificultosa tarea de reorientar el funcionamiento de los sistemas algorítmicos, minimizando los riesgos y el impacto nocivo que estos poderosos instrumentos ejercen, de forma velada, sobre la esfera vital de los ciudadanos o administrados. Esta labor, «además de técnica y referida a la manera de programar estas herramientas algorítmicas, es también jurídica, cuando no esencialmente jurídica» (Boix, 2020: 226), y en ella cobra especial trascendencia la necesidad de revigorar el principio de precaución (Fernando, 2021: 111), especialmente cuando son empleados para la adopción de decisiones con capacidad para imponerse coactivamente a los ciudadanos (Scherer, 2016: 353). Esta última idea es especialmente relevante a la hora de minimizar la capacidad que poseen estos sistemas algorítmicos para reproducir y reforzar los estereotipos de género (Domínguez, 2021b) y normas

---

22. Como señala Cerrillo i Martínez, «[a]unque no lo están haciendo (...) con la misma intensidad que el sector privado, cada vez son más las Administraciones públicas que utilizan la inteligencia artificial para analizar datos o para personalizar los servicios públicos (por ejemplo, para prestar servicios de información, asesoramiento y atención ciudadana)» (Cerrillo, 2019: 15).

23. En torno a esta problemática cuestión resulta especialmente ilustrativa la Sentencia del Tribunal del Distrito de la Haya, de 5 de febrero de 2020, Caso C/09/550982, pronunciamiento judicial de necesaria consulta que pone coto a la implantación de modelos opacos de comportamiento predictivo. Disponible en: <https://bit.ly/3sd4fKR>

sociales discriminatorias existentes<sup>24</sup>, circunstancia que produce una afectación directa para el pleno y correcto ejercicio de los derechos y libertades fundamentales de la ciudadanía, como se pondrá de relieve en las próximas páginas.

### III. ÉTICA Y DERECHO COMO PRESUPUESTO PARA GARANTIZAR LA IGUALDAD DE GÉNERO ANTE EL HORIZONTE DIGITAL

Como ha subrayado la Unión Europea en diversos pronunciamientos, «*la inteligencia artificial es una tecnología estratégica que ofrece numerosas ventajas a los ciudadanos, las empresas y la sociedad en su conjunto, siempre y cuando sea antropocéntrica, ética y sostenible y respete los derechos y valores fundamentales (...) teniendo en cuenta el enorme impacto que puede tener la IA en nuestra sociedad y la necesidad de que esta suscite confianza, resulta clave que la inteligencia artificial europea se asiente en nuestros valores y derechos fundamentales, como la dignidad humana y la protección de la privacidad*» (Comisión Europea, 2020: 2).

Urge, por tanto, avanzar en el establecimiento de soluciones normativas que permitan delimitar el potencial y pernicioso alcance del desarrollo tecnológico, desde una órbita humanista, supeditando el avance digital al servicio de la sociedad en su conjunto. Todo ello hace que los poderes públicos no puedan asistir impasibles, como meros observadores, a este cambio de paradigma en el que están en juego los derechos y libertades fundamentales de la ciudadanía, especialmente en lo que se refiere a la dignidad, la igualdad y la privacidad del individuo, institutos jurídicos que el paso del tiempo y la (r)evolución digital amenazan con desdibujar casi por completo. En este sentido, reviste especial importancia ahondar en el papel protagonista que el Derecho administrativo<sup>25</sup>, posee a la hora de contener los perniciosos efectos que los crecientes procesos de digitalización y datificación de la sociedad entrañan para el conjunto de la población.

Junto a este carácter proteccionista del Derecho administrativo, la ética de la IA (O'Neil, 2016), entendida como aquella perspectiva de la ética digital<sup>26</sup> encargada de

---

24. Son múltiples y variadas las manifestaciones de las discriminaciones que el universo de los sistemas algorítmicos provoca en la esfera de la igualdad de género. Uno de los ejemplos más claros de esta perniciosa tendencia lo encontramos en la herramienta experimental de *machine learning* empleada por la multinacional Amazon para seleccionar su personal, la cual otorgaba un criterio de preferencia a los varones en detrimento de las aspiraciones laborales del género femenino. Más información disponible en: <https://reut.rs/2N3WA1P>

25. Como recuerda Rodríguez-Arana Muñoz, «desde sus orígenes el Derecho administrativo se nos presenta dependiente del interés general, de aquellos asuntos supraindividuales que a todos afectan por ser comunes a la condición humana y que reclaman una gestión y administración equitativa y que satisfaga las necesidades colectivas en un marco de racionalidad y de justicia». (Rodríguez-Arana, 2015: 12).

26. Cuando hablamos de ética digital nos referimos al código social necesario para solucionar los problemas que el uso de Internet está ocasionando en múltiples esferas, tales como el derecho de propiedad intelectual, los ciberataques a la seguridad, los límites a la libertad de expresión, la regulación de las grandes corporaciones, la desconexión digital, la conducta en redes sociales y la privacidad de nuestros datos personales.

perseguir la protección de valores tales como la dignidad, la libertad, la democracia, la igualdad de género<sup>27</sup>, la autonomía del individuo y la justicia frente al gobierno de un razonamiento mecánico (Agencia Española de Protección de Datos, 2020: 7), esta llamada a ser otro de los elementos capitales a la hora de avanzar en el establecimiento de un desarrollo tecnológico antropocéntrico, ético, sostenible, igualitario y respetuoso con los derechos y valores fundamentales que integran la concepción de ciudadanía europea (Comisión Europea, 2020b).

Como se ha señalado con anterioridad, la Comisión Europea trabaja en la definición de una IA confiable, y establece que, para ello, ha de cumplir con siete requisitos clave: acción y supervisión humanas, solidez técnica y seguridad, gestión de la privacidad y los datos, transparencia, diversidad, no discriminación y equidad, bienestar social y ambiental y rendición de cuentas (Comisión Europea, 2019: 4).

Estos requisitos deben ser evaluados a lo largo de todo el ciclo de vida de un sistema de IA de forma continua<sup>28</sup>. Por ello, es preciso estar alerta y supervisar tanto la legitimidad ética de los tratamientos de datos personales como los efectos inesperados de estos, prestando especial atención, entre otras muchas cuestiones, a la adopción de medidas pertinentes con el fin de minimizar los sesgos de género (Ministerio de Igualdad, 2020:57), evitando con ello el establecimiento de nuevas fuentes de desigualdad entre mujeres y hombres ante el avance digital<sup>29</sup>.

## 1. La protección de datos de carácter personal como barrera de contención del avance de la Inteligencia Artificial

La protección de la vida privada ha visto transcurrir un periodo de casi tres cuartos de siglo desde su primera formulación teórica por Warren y Brandeis (1890: 193-220) hasta su reconocimiento jurisdiccional en Estados Unidos o su aparición en nuestro ordenamiento jurídico con la Constitución española de 1978. Pese a todo ello, el derecho a la protección de datos personales se ha asentado en nuestro sistema normativo con una

---

27. Recuérdese también que tanto la Recomendación del Consejo de la OCDE sobre la IA como los Principios de IA del G20 enfatizan la importancia de que los sistemas algorítmicos contribuyan a reducir la desigualdad de género.

28. Es decir, hay que analizar la solución IA per se, pero también en el marco del tratamiento en el que se integra, y las relaciones de dicho tratamiento con el entorno en varios aspectos: en el aspecto cultural, con su escala de valores; en el contexto en el que se despliega el servicio, con sus requisitos de calidad; en los aspectos que se derivan de la interconexión masiva de componentes en la sociedad de la información (Agencia Española de Protección de Datos, 2020: 7).

29. Un aspecto crítico de los sistemas de IA es el de la posible existencia de sesgos. Un sesgo ("bias" en inglés) es una desviación inadecuada en el proceso de inferencia. Los sesgos son particularmente graves cuando, por ejemplo, derivan en discriminaciones de un grupo en favor de otro. Esta problemática ya fue señalada por Friedman y Nissenbaum, según los cuales: «*systematically and unfairly discriminate against certain individuals or groups of individuals in favor of others. A system discriminates unfairly if it denies an opportunity or a good or if it assigns an undesirable outcome to an individual or group of individuals on grounds that are unreasonable or inappropriate*» (Friedman y Nissenbaum, 1996: 330).

rapidez inusitada teniendo en cuenta sus especiales características morfológicas y la técnica jurisprudencial que ha determinado su nacimiento (Martínez Martínez, 2007, 4).

En la actualidad, el derecho fundamental a la protección de datos está desarrollado en un marco normativo que actualmente comprende el Reglamento 679/2016 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 (RGPD), y se complementa en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD) además de toda la normativa sectorial publicada antes y después de la entrada en vigor del RGPD (Piñar, 2016: 26-29).

Esta poderosa regulación, proporciona una extraordinaria flexibilidad<sup>30</sup> para poder garantizar y demostrar la adecuación de un tratamiento a la norma (Agencia Española de Protección de Datos, 2018). Sin embargo, hay un conjunto mínimo de condiciones *sine qua non* que deben cumplirse para garantizar que el tratamiento de datos personales empleado para desarrollar soluciones de IA (Casey y Niblett, 2016: 423-442) es conforme a la vigente regulación de datos de carácter personal. Entre estos aspectos clave pueden citarse los siguientes:

- La existencia de una base para legitimación del tratamiento de datos personales, (arts. 6 al 11 RGPD). El establecimiento de una base jurídica legitimadora es el primer paso para determinar el cumplimiento de la solución de IA con el RGPD. La legitimación para las distintas etapas del ciclo de vida y para cada tratamiento se tiene que establecer en la fase de concepción del tratamiento, sea este tratamiento la propia creación de un componente IA o un tratamiento que plantee la utilización de un componente IA. Desde el punto de vista de la protección de datos, la legitimación es el primer elemento que hay que establecer dentro de la fase de concepción del tratamiento. Si no se encuentra una base legitimadora no se debe realizar el tratamiento de datos de carácter personal para no vulnerar los derechos y libertades fundamentales de la ciudadanía. En este sentido, el art. 6 RGPD establece las seis bases jurídicas por las cuales el tratamiento de datos personales se puede considerar lícito. Las bases jurídicas más habituales que legitimarán el tratamiento en una solución de IA son:
  - ▶ El tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte, o para la aplicación de medidas precontractuales a petición de este. Podría ser el caso de desarrolladores que contraten a sujetos para hacer uso de sus datos personales en la etapa de entrenamiento del sistema. También podría ser que el responsable del tratamiento, y que proporciona

30. No debe obviarse que el RGPD nace con vocación de erigirse como el instrumento normativo encargado de dar respuesta y solución al tsunami tecnológico en el que se sumerge la sociedad actual (Rallo y García, 2015).

un servicio a terceros interesados que incluye la solución de IA, utilizara los datos de estos en el marco del contrato del servicio.

- ▶ El interés legítimo<sup>31</sup>, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un menor.
- ▶ El consentimiento de los interesados, que, como establece el art. 4.11 RGPD, es toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen.

Y en ciertos casos más especiales desde el punto de vista de soluciones IA, también pueden ser bases jurídicas:

- ▶ La protección de intereses vitales.
- ▶ Razones de interés público o ejercicio de poderes públicos<sup>32</sup>.
- ▶ Cumplimiento de obligaciones legales.

Ahora bien, es muy importante tener en cuenta que las dos últimas bases jurídicas han de establecerse vía derecho de la Unión Europea o de los Estados miembros, que establecerá la base jurídica del tratamiento. Es decir, un responsable no podrá arrogarse razones, por ejemplo, de interés público si no está establecido en una norma del rango apropiado<sup>33</sup>.

- La obligación de informar a los sujetos de los datos y ser transparente<sup>34</sup> (arts. 12 al 14 RGPD). La información que cada responsable ha de proporcionar a los

---

31. El Dictamen 06/2014 sobre el concepto de interés legítimo, del Grupo del Artículo 29, desarrolló en detalle cómo evaluar los factores que legitiman el interés del responsable para realizar un tratamiento de datos personales y equilibrarlo con los derechos y los intereses, también legítimos, de los interesados. El interés legítimo es una alternativa de legitimación para tratamientos que requieren, como en algunos casos de ML, acceso a datos de entrenamiento, siempre que se den las circunstancias que permiten su utilización.

32. Como es el caso de Smartcities o control de fronteras.

33. Otro aspecto importante es que se debe tener en cuenta el principio de limitación del tratamiento. Una base jurídica no habilita para el uso de los datos para cualquier propósito y en todo momento, sino que debe restringirse a aquellos fines determinados, explícitos y legítimos que se hayan identificado, evitando tratarlos de manera incompatible con esos fines. Además, los interesados cuyos datos son tratados, deben ser conscientes de cómo se van a utilizar, lo que está íntimamente relacionado con el principio de información y transparencia.

34. Según el Considerando 78 RGPD, el principio de transparencia es una medida de privacidad por defecto para permitir, entre otros, que los interesados puedan supervisar el tratamiento al que están sometidos. El principio de transparencia se desarrolla en los Considerandos 39 y 58 RGPD. En estos Considerandos se interpreta la obligación de información a los interesados de un modo que va más allá de lo dispuesto en la letra de los arts. 13 y 14 RGPD. En particular, los Considerandos

interesados se establece en los arts. 13 y 14 RGPD, y el contenido concreto se tendrá que adaptar a la etapa del ciclo de vida de la IA en la que se esté realizando el tratamiento. El art. 11 LOPDGDD establece la posibilidad al responsable de ofrecer esta información mediante una aproximación por capas o niveles: una primera capa, de carácter general, con información básica del tratamiento y una segunda capa que completa la información de la primera con mayor nivel de detalle y que sea accesible desde esta de forma fácil e inmediata, incluso por medios electrónicos:

Así, en la primera capa deberá consignarse la siguiente información:

- ▶ La identidad del responsable del tratamiento o de su representante.
- ▶ La finalidad del tratamiento.
- ▶ La posibilidad de ejercer los derechos 15 al 22 RGPD.
- ▶ Si el tratamiento incluye la elaboración de perfiles o decisiones automatizadas.
- ▶ Si los datos personales objeto del tratamiento no han sido obtenidos directamente del afectado, la información básica incluirá también: las categorías de datos objeto de tratamiento y las fuentes de las que procedieran los datos.

En la segunda capa, el resto de la información establecida en los arts. 13 y 14 RGPD.

- La obligación de proporcionar a los sujetos de los datos mecanismos para el ejercicio de sus derechos subjetivos (Álvarez, 2016; Adsuara, 2019). Los responsables que hagan uso de soluciones de IA para tratar datos personales, elaborar perfiles o tomar decisiones automatizadas, han de ser conscientes de que los interesados tienen derechos en el ámbito de la protección de datos que deben ser atendidos (arts. 15 al 23 RGPD).

---

comentan la obligación de que «toda información y comunicación relativa al tratamiento de dichos datos sea fácilmente accesible y fácil de entender», «sea concisa», «se utilice un lenguaje sencillo y claro», que «en su caso, se visualice», que «podría facilitarse en forma electrónica», que se proporcione «información añadida para garantizar un tratamiento leal y transparente» y que los interesados «deben tener conocimiento de los riesgos, las normas, las salvaguardias» del tratamiento.

En el caso de tratamientos basados en IA, la transparencia puede ser considerada un aspecto crítico. Debe permitir a los interesados ser conscientes del impacto que el empleo de dichas soluciones puede llevar asociado. De ahí que la transparencia esté dirigida tanto a los interesados como a los operadores del tratamiento. En particular, la transparencia está ligada con una información veraz sobre la eficiencia, las capacidades y las limitaciones reales de los sistemas de IA, que evite la creación de falsas expectativas, en los usuarios y los interesados, que puedan ocasionar una mala interpretación de las inferencias que se realizan en el marco del tratamiento (Agencia Española de Protección de Datos, 2020: 33).

La transparencia no se reduce a un instante puntual, sino que debe ser entendida como un principio en torno al que orbita de forma dinámica el tratamiento realizado y que afecta a todos y cada uno de los elementos y participantes que intervienen en la solución.

Por lo tanto, durante la fase de concepción del tratamiento, los responsables han de ser conscientes de que tienen que establecer mecanismos y procedimientos adecuados para poder atender las solicitudes que reciban, y que dichos mecanismos deberán estar adecuadamente dimensionados para la escala del tratamiento que están efectuando.

- La aplicación del principio de responsabilidad proactiva<sup>35</sup> (arts. 24 al 43 RGPD) que establece la necesidad de incorporar una serie de garantías adicionales, más allá de un mínimo, documentadas y orientadas a gestionar el riesgo para los derechos y libertades de los individuos. En particular, la obligación de mantener un registro de actividades de tratamiento (art. 30 RGPD).
- El cumplimiento de las condiciones para poder realizar transferencias internacionales de datos<sup>36</sup> (artículos 44 al 50 RGPD). El desarrollo o despliegue de un componente de IA basado en servicios en la nube, la comunicación de los datos de los usuarios a terceros para evolucionar el modelo de IA, o la distribución de componente de IA en el caso de que existan datos personales inherentes al modelo, pueden implicar flujos transfronterizos de datos a terceros países. No tienen consideración de transferencia internacional de datos los flujos de datos que se producen dentro del marco del Espacio Común Europeo<sup>37</sup>.

Dichas transferencias han de aplicar las garantías que se establecen en el Capítulo V del RGPD. Especialmente importante es establecer mecanismos para permitir que las contrataciones que se realicen en este contexto de transferencias internacionales se gestionen con fluidez, asegurando al mismo tiempo que el cliente responsable tiene información suficiente sobre los contratistas, o potenciales contratistas, y mantiene la capacidad de tomar decisiones. Cuando existen transferencias internacionales hay que informar a los interesados en los términos del art. 13 y 14 RGPD e incluirlo en el registro de actividades de tratamiento.

Además de demostrar el cumplimiento de estas previsiones mínimas, los grandes promotores tecnológicos deben tener en cuenta otra serie de cuestiones orientadas a garantizar la efectividad de la normativa de protección de datos personales (Recio, 2018) ante el avance de la IA, minimizando el riesgo para los derechos y libertades fundamentales

---

35. Este principio implica que el responsable del tratamiento tiene que garantizar la licitud, la lealtad y la transparencia en todo el proceso del tratamiento de datos con relación al interesado. Pero su responsabilidad no termina aquí, toda vez que el legislador le impone a dicho responsable la obligación de poder acreditar que efectivamente dicho tratamiento ha reunido las características especificadas en el apartado 5.1 RGPD (Puyol, 2016: 140).

36. Recuérdese que el pasado 16 de julio de 2020 el Tribunal de Justicia de la Unión Europea (TJUE) publicó una sentencia crucial por la que se anula la Decisión 2016/1250 de la Comisión que declaraba el nivel adecuado de protección del esquema del Escudo de Privacidad (*Privacy Shield*) para las transferencias internacionales de datos a EEUU. Esta Decisión sustituía a su vez a Puerto Seguro, que también fue declarado inválido por el TJUE en octubre de 2015. *Vid.* STJUE de 23 de julio de 2020, Comisaria de Protección de Datos/Facebook Irlanda y Maximilian Schrems (Asunto C-311/18).

37. Es decir, los Estados de la Unión Europea más Islandia, Noruega y Liechtenstein.

de la ciudadanía. En este sentido, con la finalidad de sistematizar las medidas adoptadas en materia de privacidad sería conveniente promover la adopción de políticas de protección de datos (art. 24 RGPD)<sup>38</sup> en el seno de las organizaciones encargadas de impulsar el avance del desarrollo tecnológico, así como implementar la realización de evaluaciones de impacto en protección de datos (Saiz, 2019: 387-430), cuestión esencial para identificar cuáles son los requisitos de privacidad a incorporar y poder aplicar, de manera efectiva, las medidas de privacidad desde el diseño y por defecto en los procesos de selección e implementación de las diferentes soluciones de IA.

La educación para la digitalización como mecanismo para potenciar la inclusión de la perspectiva de género en los procesos de digitalización de la sociedad

Como es bien sabido por todos, la LOPDGDD fue concebida como un instrumento normativo tendente a desbordar las fronteras propias de la protección de datos personales, al apostar de forma decidida por la introducción de aspectos reguladores en determinados elementos que se vinculan a los derechos digitales de la ciudadanía<sup>39</sup>, cuya conexión con el derecho a la protección de datos en sentido estricto es más que evidente<sup>40</sup>.

Un claro ejemplo de esta tendencia lo encontramos en la positivización, a propuesta de la Agencia Española de Protección de Datos, del Derecho a la educación digital ex art. 83.1 LOPDGDD, cuyo tenor literal establece que: «[e]l sistema educativo garantizará la plena inserción del alumnado en la sociedad digital y el aprendizaje de un uso de los

---

38. Esta política convivirá con una política de calidad, una política de sistemas de información, una de seguridad y una política de toma de decisiones, entre otras.

39. La transformación digital de nuestra sociedad es una realidad en constante desarrollo, lo que ha propiciado que países de nuestro entorno más inmediato como Italia o Francia hayan aprobado diferentes instrumentos normativos con la finalidad de reforzar los derechos digitales de la ciudadanía. En nuestro caso, ese impulso de la regulación del mundo digital se produce por medio de la inclusión del Título X de la LOPDGDD. Esta idea aparece consignada en el propio Preámbulo de la norma, según el cual «el legislador debe abordar el reconocimiento de un sistema de garantía de los derechos digitales que, inequívocamente, encuentra su anclaje en el mandato impuesto por el apartado cuarto del artículo 18 de la Constitución Española, [...] el Título X de esta ley acomete la tarea de reconocer y garantizar un elenco de derechos digitales de los ciudadanos conforme al mandato establecido en la Constitución. Y así lo confirma su art. 1 b) al fijar el objeto de la ley: «La presente ley orgánica tiene por objeto: [...] Garantizar los derechos digitales de la ciudadanía conforme al mandato establecido en el art.18.4 de la Constitución». Por tanto, con la promulgación de la LOPDGDD asistimos a un hito normativo sin precedentes, ya que esta Ley Orgánica representa el punto de partida de la garantía de los derechos digitales en el continente europeo. Hasta la fecha, ningún país europeo había adoptado una Ley que garantizara, de forma sistemática, los derechos digitales de los ciudadanos (Rallo, 2019: 28).

40. Esta idea que ahora señalamos ha sido igualmente señalada por Rallo Lombarte, según el cual «[l]a Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales, constituye un ejemplo palmario de la transformación provocada por la tecnología en la sociedad contemporánea. Si el derecho a la protección de datos personales sirvió durante las últimas décadas para preservar los derechos individuales frente a buena parte de los efectos generados por las tecnologías de la información y del conocimiento, la sociedad digital en la que nos hallamos completamente inmersos demanda un haz de derechos que se extienda a la práctica totalidad de los ámbitos en que el individuo se desarrolla en sociedad. Los nuevos derechos digitales son, en buena medida, el corolario de una evolución en la que el derecho a la protección de datos ha servido como auténtica punta de lanza frente a la realidad digital» (Rallo, 2017: 637).

*medios digitales que sea seguro y respetuoso con la dignidad humana, los valores constitucionales, los derechos fundamentales y, particularmente con el respeto y la garantía de la intimidad personal y familiar y la protección de datos personales. Las actuaciones realizadas en este ámbito tendrán carácter inclusivo, en particular en lo que respecta al alumnado con necesidades educativas especiales»<sup>41</sup>.*

En base al citado precepto<sup>42</sup>, el sistema educativo no solamente deberá garantizar la plena inserción del alumnado en la sociedad digital y promover que el aprendizaje del uso de los medios digitales sea seguro, respetuoso con la dignidad humana, los valores constitucionales y los derechos fundamentales, con especial atención a la igualdad de género, la intimidad personal y familiar y la protección de datos personales. Incluye, asimismo, la previsión de que, dentro del diseño de las asignaturas de libre configuración, se incluirá «la competencia digital» y los «elementos relacionados con las situaciones de riesgo derivadas de la inadecuada utilización de las TIC». Se preceptúa, igualmente, que, a tal efecto, «el profesorado recibirá las competencias digitales y la formación necesaria», así como que, en los planes de estudio de las titulaciones universitarias encaminadas al desempeño profesional del profesorado en la formación de los alumnos, se garantizará esa formación. Y se añade, por último, la regla siguiente: los temarios de las pruebas selectivas a los cuerpos superiores docentes incorporarán «materias relacionadas con la garantía de los derechos digitales y la protección de datos personales», mandato que las Administraciones públicas, y especialmente las Universidades, deberían haber dotado de efectividad antes del 5 de diciembre de 2019.

En los últimos tiempos hemos asistido al empoderamiento y/o aceleración de los avances derivados de la (r)evolución digital. Estas abruptas transformaciones han instituido el autoconocimiento y la educación para la digitalización como una alternativa cierta para garantizar no solamente el uso responsable y seguro de los medios digitales y promover una cultura de la privacidad, elementos imprescindibles para garantizar el cumplimiento de la normativa de protección de datos; sino también, y lo que es más importante, como presupuesto indispensable para promover la incorporación de la perspectiva de género en los procesos de diseño y desarrollo tecnológico, lo que sin duda permitirá minimizar las desviaciones en la implementación de los crecientes procesos algorítmicos, evitando con ello la aparición de novedosas formas de desigualdad, y avanzar en la tortuosa travesía hacia el ansiado humanismo tecnológico<sup>43</sup>.

41. Este precepto ha sido recientemente modificado por la disposición final cuarta de la Ley Orgánica 3/2020, de 29 de diciembre, por la que se modifica la Ley Orgánica 2/2006, de 3 de mayo, de Educación.

42. Igualmente relevante resulta el Plan de Acción de Educación Digital de la Comisión Europea, de 17 de enero de 2018 [COM (2018) 22 final], donde se recogen una serie de prioridades de acción en el ámbito de la digitalización educativa.

43. La revolución digital ha transformado profundamente nuestros paradigmas y abre muchas oportunidades, pero también nos plantea numerosos retos. Las posibilidades son infinitas y los resultados serán positivos o negativos en función del uso que hagamos de las herramientas de la Industria 4.0. El humanismo digital es la respuesta a cómo debemos usar estos instrumentos y posibilidades. Es un esquema que nos mueve a restaurar los valores humanistas en el uso y los fines de la tecnología, que debe estar siempre al servicio del ser humano para hacer nuestra vida más sencilla y plena (Pardo, 2019).

## IV. CONCLUSIONES

En nuestros días, hablar de desarrollo tecnológico requiere, necesariamente, hacer alusión a los conceptos de privacidad y protección de datos de carácter personal. Este derecho fundamental, más allá de alzarse en nuestros días como el instituto básico para la plena eficacia y garantía del conjunto de derechos fundamentales reconocidos constitucionalmente, se erige como piedra angular del Estado social y democrático de Derecho ante los envites de la (r)evolución digital.

Esta necesidad de garantizar la plena efectividad de la normativa de protección de datos de carácter personal es especialmente relevante en el supuesto concreto de las Administraciones públicas, quienes en los últimos tiempos se han visto obligadas a impulsar un vertiginoso proceso de modernización, de la mano de la implementación de una serie innovaciones tecnológicas, entre las que se encuentran, como no podía ser de otra manera, la administración electrónica, en primer término, y más recientemente la introducción de los sistemas algorítmicos en el Sector Público. Sin embargo, lamentablemente, este proceso de tecnificación de la estructura y la acción administrativa, no ha venido acompañado del diseño e introducción de las garantías pertinentes para blindar los derechos de los administrados (oscurantismo, desinformación, inobservancia de la normativa de protección de datos, etc.), alterando el normal funcionamiento del conjunto de las Administraciones públicas en busca de la ansiada eficacia y eficiencia del poder público. Esta perniciosa tendencia se ha visto fuertemente acentuada tras el estallido de la COVID-19, y sin solución de continuidad nos aboca a repensar el equilibrio entre desarrollo tecnológico y dignidad de la persona.

$$x + y = z$$

(desarrollo tecnológico) + (privacidad) = dignidad

La caprichosa realidad nos ha demostrado que la ausencia de privacidad (y), dificulta, cuando no imposibilita el avance del desarrollo tecnológico (x), toda vez que es el presupuesto lógico para lograr la raigambre de la libertad y la dignidad del individuo (z). Este razonamiento, por si solo, motiva la importancia fundamental de garantizar la plena efectividad y vigencia de la normativa de protección de datos de carácter personal ante el avance digital, finalidad última en la que el establecimiento de una cultura de privacidad y el fomento de la educación para la digitalización poseen un destacado protagonismo, al ser el vehículo idóneo para alcanzar una concepción antropocéntrica, ética y sostenible del desarrollo tecnológico, antesala del esperado humanismo tecnológico. Transformaciones todas ellas de profundo calado que exigen la acción decidida del conjunto de los poderes públicos, y muy especialmente, la acción concertada de las Administraciones públicas, quienes deben liderar y abanderar la transición justa hacia una sociedad digital, ecológica y socialmente cohesionada.

## BIBLIOGRAFÍA

- Adsuares Varela, B. (2019). Derechos de rectificación, supresión (olvido) y portabilidad de los datos. En A. Rallo Lombarte. *Tratado de protección de datos. Actualizado con la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos personales y Garantía de los Derechos Digitales*. Tirant lo Blanch.
- Agencia Española de Protección de Datos (2018), *Listado de cumplimiento normativo*.
- Agencia Española de Protección de Datos (2020), *Guía para la adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial. Una introducción*.
- Álvarez Caro, M. (2016). El derecho de rectificación, cancelación, limitación del tratamiento, oposición y decisiones individuales automatizadas. En J.L. Piñar Mañas. *Reglamento General de Protección de Datos. Hacia un modelo europeo de privacidad*. Editorial Reus.
- Bauer, H. (1992). Verwaltungsrechtslehre im Umbruch? *Die Verwaltung* (3).
- Boix Palop, A. (2020). Los algoritmos son reglamentos: la necesidad de extender las garantías propias de las normas reglamentarias a los programas empleados por la Administración para la adopción de decisiones. *Revista de Derecho Público: Teoría y Método* (1).
- Campos Acuña, M.C. (2021). Las 15 claves del Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos. *Actualidad administrativa* (5).
- Canals Ametller, D. (2019). El proceso normativo ante el avance tecnológico y la transformación digital (Inteligencia artificial, redes sociales y datos masivos). *Revista General de Derecho Administrativo* (50).
- Casey, A.J. y Niblett, A. (2016). Focus feature: Artificial Intelligence, Big Data, and the future of law. *University of Toronto, Law Journal*, vol. 66 (4).
- Cassese, S. (2006). *La globalización jurídica*, Marcial Pons-Instituto Nacional de Administración Pública.
- Cassese, S. (2009). Le Droit tout puissant et unique de la société. Paradossi del Diritto amministrativo. *Rivista Trimestrale di Diritto Pubblico* (4).
- Cerrillo i Martínez, A. (2019). El impacto de la inteligencia artificial en el derecho administrativo. ¿Nuevos conceptos para nuevas realidades técnicas? *Revista General de Derecho Administrativo* (50).
- Comisión Europea (2018), *Inteligencia artificial para Europa*, [COM(2018) 237 final].
- Comisión Europea (2019), *Generar confianza en la inteligencia artificial centrada en el ser humano*, [COM(2019) 168 final].
- Comisión Europea (2020), *Informe sobre las repercusiones en materia de seguridad y responsabilidad civil de la inteligencia artificial, el internet de las cosas y la robótica*, [COM(2020) 64 final].
- Comisión Europea (2020), *Libro blanco sobre la inteligencia artificial, un enfoque europeo orientado a la excelencia y la confianza*, [COM(2020) 65 final].
- Comisión Europea (2020), *Una Estrategia de Datos*, [COM(2020) 66 final].
- Comisión Europea (2020), *Configurar el futuro digital de Europa*, [COM(2020) 67 final].
- Comisión Europea (2021), *Proposal for a Regulation of the European Parliament of the Council, Laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts* [COM(2021) 206 final].
- Cotino Hueso, L. (2019a). La obligación de relacionarse electrónicamente con la Administración y sus escasas garantías. *IDP: Revista de Internet, Derecho y Política* (26).

- Cotino Hueso, L. (2019b). Riesgos e impactos del Big Data, la inteligencia artificial y la robótica: enfoques, modelos y principios de la respuesta del derecho. *Revista General de Derecho Administrativo* (50).
- Domínguez Álvarez, J.L. (2021a). La efectividad de la normativa de protección de datos de carácter personal ante el avance de la Inteligencia Artificial. Una revisión del binomio libertad y seguridad. En D. Terrón Santos y J.L. Domínguez Álvarez. *Inteligencia Artificial y Defensa. Nuevos horizontes*. Thomson Reuters-Aranzadi.
- Domínguez Álvarez, J.L. (2021b). Sistemas algorítmicos, protección de datos y nuevas formas de desigualdad. La necesidad de afrontar los sesgos ante el avance digital. En M. del Pozo Pérez. *Estudios interdisciplinarios de género*. Thomson Reuters-Aranzadi.
- Duguit, L. (1913). *Les transformations du Droit Public*. Editorial Colin.
- Esteve Pardo, J. (1999). *Técnica, riesgo y Derecho*. Ariel.
- Fernando Pablo, M.M. (2003). Sobre i-administración: el Derecho administrativo de la sociedad del conocimiento (I). *E-Derecho Administrativo* (9).
- Fernando Pablo, M.M. y Terrón Santos, D. (2019). Sobre la gobernanza de la inteligencia artificial. En I. del Guayo Castiella y A. Fernández Carballal. *Los desafíos del derecho público en el siglo XXI*. Instituto Nacional de Administración Pública.
- Fernando Pablo, M.M. (2021). Inteligencia artificial y derecho administrativo: de la precaución a la garantía de los derechos. En D. Terrón Santos y J.L. Domínguez Álvarez. *Inteligencia Artificial y Defensa. Nuevos horizontes*. Thomson Reuters-Aranzadi.
- Ferry, L. (2017). *La révolution transhumaniste*. Editorial Plon.
- Friedman, B. y Nissenbaum, H. (1996). Bias in computer systems. *ACM Transactions on Information Systems*, vol. 14 (3).
- Frosini, V. (1984). Informática y Administración pública. *Revista de Administración Pública*, (105).
- Gamero Casado, E. (2016). Panorámica de la administración electrónica en la nueva legislación administrativa básica. *Revista Española de Derecho Administrativo* (175).
- Hauriou, M. (1916). *Principes de droit public*. Editorial Larose.
- Hoffmann-Riem, W. (2018). *Big Data. Regulative Herausforderungen*, Nomos.
- Huergo Lora, A.J. (2020). Una aproximación a los algoritmos desde el Derecho Administrativo. En A.J. Huergo Lora. *La regulación de los algoritmos*. Thomson Reuters-Aranzadi.
- Huergo Lora, A. J. (2021). *El proyecto de Reglamento sobre la Inteligencia Artificial*. Almacén de Derecho. Recuperado el 1 de junio de 2021, de <https://bit.ly/3wLmfxo>
- López Oneto, M. (2020). *Fundamentos para un Derecho de la Inteligencia Artificial. ¿Queremos seguir siendo humanos?* Tirant lo Blanch.
- Martín Delgado, I (2009a). Naturaleza, concepto y régimen jurídico de la actuación administrativa automatizada. *Revista de Administración Pública*(180).
- Martín Delgado, I. (2009b). La Administración electrónica como reto del Derecho Administrativo en el siglo XXI. En F.M. García Costa y M.M. Pardo López. *Los retos del Derecho en el siglo XXI*. Tirant lo Blanch.
- Martín Delgado, I. (2016). El impacto de la reforma de la Administración electrónica sobre los derechos de los ciudadanos y el funcionamiento de las Administraciones Públicas. En M. Almeida Cerrada y L. Míguez Macho. *La actualización de la Administración electrónica*. Andavira.
- Martínez Díez, R. (1984). El proceso de informatización de la Administración pública española. *Documentación administrativa* (200).

- Martínez Gutiérrez, R. (2007). Administración electrónica: origen, definición institucional y contexto actual. *Revista Aranzadi de Derecho y Nuevas Tecnologías* (14).
- Martínez Martínez, R. (2007). El derecho fundamental a la protección de datos: perspectivas». *IDP: revista de Internet, derecho y política= revista d'Internet, dret i política* (5).
- Mccarthy, J., Minsky, M. L., Rochester, N. y Shannon, C.E. (1955). *A proposal for the Dartmouth Summer Research Project on Artificial Intelligence*.
- Mcculloch, W. S. y Pitts, W.H. (1943). A logical calculus of the inmanent in nervous activity. *Bulletin of Mathematical Biophysics*, vol. 5 (4).
- Mehl, L. (1957). La cybernétique et l'administration. *La Revue Administrative*, vol. 10 (58).
- Ministerio de Igualdad (2020), *Mujeres y digitalización. De las brechas a los algoritmos*.
- Muñoz Machado, S. (2011). Hacia un nuevo Derecho Administrativo. En A. Blasco Esteve. *El Derecho público de la crisis económica. Hacia un nuevo Derecho administrativo*. Instituto Nacional de Administración Pública.
- O'Neil, C. (2016). *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*. Broadway Books.
- Palomar Olmeda, A. (2007). *La actividad administrativa efectuada por medios electrónicos. A propósito de la Ley de Acceso Electrónico a las Administraciones Públicas*. Thomson-Aranzadi.
- Parejo Alfonso, L. (2012), *Transformación y ¿reforma? del Derecho Administrativo en España*. INAP-Editorial Derecho Global.
- Piñar Mañas, J.L. (2016). Reglamento Europeo de Protección de Datos: retos y oportunidades para la abogacía. *Abogados, Revista del Consejo General de la Abogacía* (98).
- Puente Gómez, M. (2007). La administración electrónica. En T.R. Fernández Rodríguez. *La Autorización administrativa. La Administración electrónica. La enseñanza del Derecho Administrativo hoy*. Aranzadi.
- Puyol Montero, J. (2016). Los principios del derecho a la protección de datos. En J.L. Piñar Mañas. *Reglamento General de Protección de Datos. Hacia un modelo europeo de privacidad*. Editorial Reus.
- Rallo Lombarte, A. y García Mahamut, R. (2015). *Hacia un nuevo derecho europeo de protección de datos. Towards a new European Data Protection Regime*. Tirant lo Blanch.
- Recio Gayo, M. (2018). *Protección de datos e innovación: ¿(in) compatibles?* Editorial Reus.
- Rivero Ortega, R. (2016). La administración electrónica en las leyes 39 y 40/2015. *Cuadernos de Derecho Local* (41).
- Rodríguez-Arana Muñoz, J. (2015). *Derecho administrativo y derechos sociales fundamentales*. Global Law Press e Instituto Nacional de Administración Pública.
- Romero Montero, R. (2019). *Las humanidades en el mundo digital/El mundo digital en las humanidades*. Tirant lo Blanch.
- Russel, S. J. y Norvig, P. (1995). *Artificial Intelligence: A modern Approach*. Prentice Hall.
- Saiz Peña, C.A. (2019). Seguridad de los datos, evaluación de impacto, códigos de conducta y certificación. En A. Rallo Lombarte. *Tratado de protección de datos. Actualizado con la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos personales y Garantía de los Derechos Digitales*. Tirant lo Blanch.
- Scherer, M.U. (2016). Regulating artificial intelligence systems: Risks, challenges, competencies, and strategies. *Harvard Journal of Law and Technology* (29).
- Terrón Santos, D. y Domínguez Álvarez, J.L. (2019), *Nueva regulación de la protección de datos y su perspectiva digital*. Comares.

- Turing, A. (1937). On computable Numbers, with an application to the Entscheidungsproblem. *Proceedings of the London Mathematical Society* (42).
- Turing, A. (1950). Computing machinery and Intelligence. *Mind*, vol. 59 (236).
- Turing, A. (1968). Intelligent machinery. En C.R. Evans y A.D. Robertson. *Cybernetics*, University Park Press.
- Valero Torrijos, J. (2006). Protección de datos personales y Administración electrónica. *Revista Española de Protección de datos* (1).
- Valero Torrijos, J. (2007). *El régimen jurídico de la e-Administración el uso de medios informáticos y telemáticos en el procedimiento administrativo*. Comares.
- Warren, S.D. y Brandeis, L.D. (1890). The right to privacy. *Harvard Law Review*, vol. IV (5).