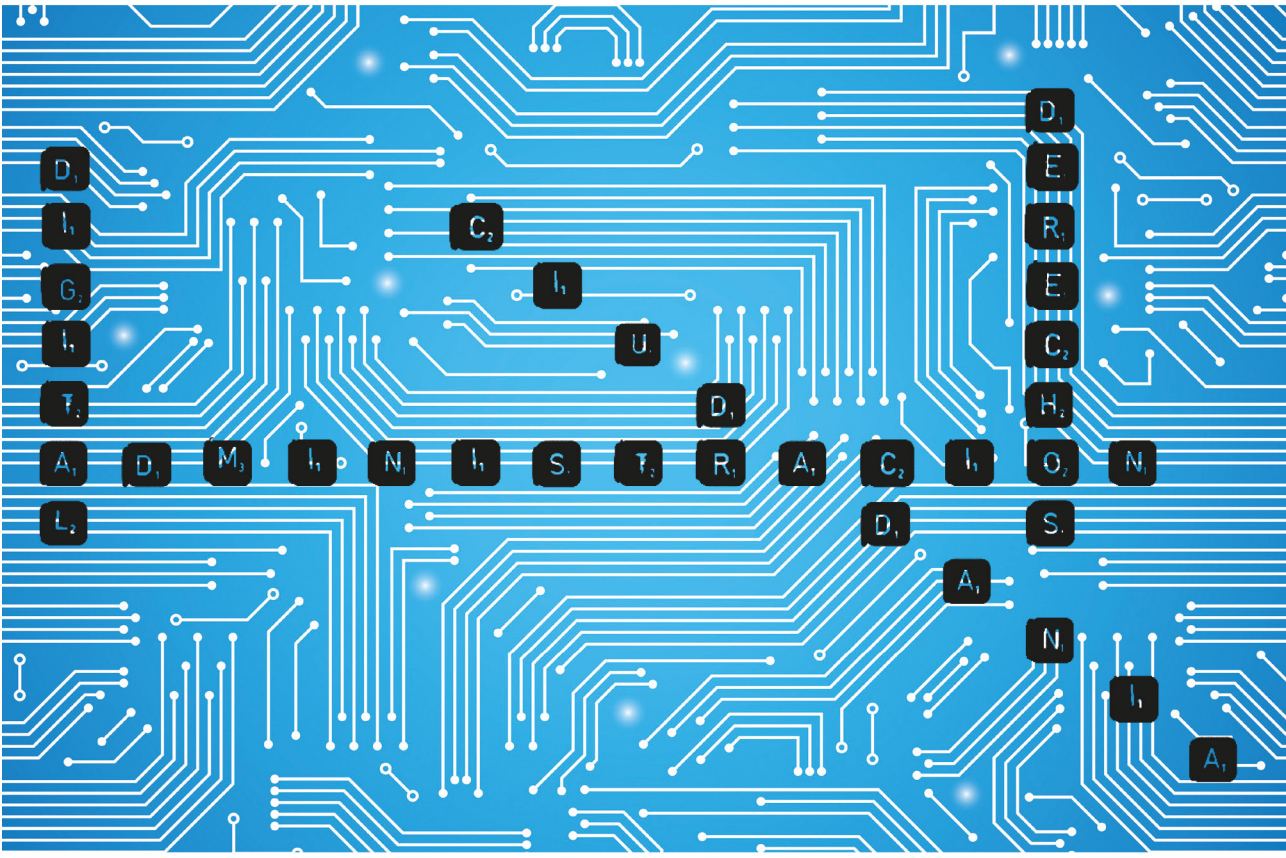
LOS DERECHOS DE LA CIUDADANÍA ANTE LA ADMINISTRACIÓN DIGITAL



MANUEL MEDINA GUERRERO (coord.)

CENTRO DE ESTUDIOS POLÍTICOS Y CONSTITUCIONALES

LOS DERECHOS DE LA CIUDADANÍA ANTE LA ADMINISTRACIÓN DIGITAL

LOS DERECHOS DE LA CIUDADANÍA ANTE LA ADMINISTRACIÓN DIGITAL

Manuel Medina Guerrero (coord.)

CENTRO DE ESTUDIOS POLÍTICOS Y CONSTITUCIONALES
Madrid, 2023

Catálogo general de publicaciones oficiales
https://cpage.mpr.gob.es

De esta edición, 2023

Plaza de la Marina Española, 9
28071 Madrid

http://www.cepc.gob.es
Twitter: @cepcgob

NIPO CEPC EN PAPEL: 091-23-034-3
NIPO CEPC PDF: 091-23-035-9
ISBN CEPC EN PAPEL: 978-84-259-1998-5
ISBN CEPC PDF: 978-84-259-1997-8
Depósito legal: M-29481-2023

Realización: Carlos Ponce Aguilella

Impreso en España — *Printed in Spain*

ÍNDICE

PRESENTACIÓN

La creciente e imparable utilización de las nuevas tecnologías tanto en el ámbito público como privado ha impactado de plano en prácticamente todos los sectores del ordenamiento, y desde luego la Constitución no podía ser una excepción a este respecto. Es evidente que el entorno digital exige repensar instituciones tradicionales del Derecho Constitucional, y por tanto obliga a los iuspublicistas a reciclarnos.

Esta ineludible adaptación resulta especialmente sentida en la órbita de los derechos fundamentales, como ya lo puso de manifiesto a principios de los años noventa Laurence Tribe al plantear abiertamente hasta qué punto el ejercicio de los derechos tradicionales podía transformarse cuando se desenvolvían en ese nuevo entorno al que se dio en denominar «ciberespacio» (*The Constitution in Cyberspace: Law and Liberty Beyond the Electronic Frontier*), término que había popularizado años atrás William Gibson en ese clásico de la ciencia ficción que es la novela *Neuromancer*.

Ha llovido mucho desde entonces: lo que entonces era ciencia ficción es hoy en buena medida una realidad de uso cotidiano, como lo acredita el frecuente empleo de sistemas algorítmicos en el proceso de toma de decisiones, que evidentemente también se ha extendido con naturalidad en el sector público. Utilización de las nuevas tecnologías por parte de las administraciones públicas que, como es palmario, recibió un impulso determinante durante la pandemia.

Es en este contexto en el que el Centro de Estudios Políticos y Constitucionales impulsó la organización de un Seminario sobre «Administración digital», que se celebró el 4 de octubre de 2022. Durante su transcurso se puso de manifiesto que no se trata solamente de determinar cómo puede —*rectius*: debe— redefinirse el contenido de los tradicionales derechos fundamentales para garantizar su vigencia en el entorno digital, sino también de reconocer e implantar nuevos específicos derechos conectados directamente con la actuación de los poderes públicos en el «ciberespacio».

Por otra parte, en la medida en que las diferentes administraciones, cada vez más, desempeñan sus funciones y prestan los servicios públicos a través de decisiones basa-

das, total o parcialmente, en algoritmos, el desarrollo de la Administración digital supone una verdadera prueba de resistencia para la virtualidad de la legislación reguladora de la transparencia: al fin y al cabo, el «contenido esencial» de esta legislación reside en asegurar que la ciudadanía esté en condiciones de conocer cómo se toman las decisiones atinentes a la cosa pública. Aunque también la Administración digital plantea interrogantes semejantes en el marco del Reglamento General de Protección de Datos, ya que igualmente reconoce cierto derecho a acceder a la información sobre las decisiones públicas automatizadas, el cual, sin embargo, se ve rodeado de particulares límites y condicionantes. Pero es que, además, como se desveló a lo largo del Seminario, la entrada en vigor de este Reglamento General de Protección de Datos —que, pese a ser heredero de la Directiva 95/46/CE, incorpora sustanciales novedades— invita también a preguntarse, como hipótesis de trabajo, en qué medida afecta al funcionamiento de los principios y reglas con los que hemos venido resolviendo hasta la fecha el inesquivable conflicto entre transparencia y el derecho a la protección de datos personales (art. 15 LTAIBG).

Sobre estas y otras cuestiones conexas hubo ocasión de debatir en el curso del Seminario. En las siguientes páginas no podemos hacernos eco de todas ellas, pero sí encuentran acomodo las más significativas.

Manuel Medina Guerrero
Catedrático de Derecho Constitucional. Universidad de Sevilla

CAPÍTULO 1

DETRÁS DE LA PANTALLA: TRANSICIÓN DIGITAL, ADMINISTRACIÓN PÚBLICA Y CIUDADANÍA[1]

Rafael Jiménez Asensio

Consultor Sector Público
Doctor en Derecho UPV/EHU
Acreditado como catedrático de Universidad

«Que el futuro sea digital; pero, ante todo, que sea un futuro humano»

Shoshana Zuboff, *El capitalismo de la vigilancia*, Paidós, 2020, p. 690.

«La comunicación digital elimina el encuentro personal, el rostro, la mirada, la presencia física. De ese modo, acelera la desaparición del otro»

Byung-Chul Han, *No cosas. Quiebras del mundo de hoy*, Taurus, 2021, p. 74)

SUMARIO

[1] Esta ponencia pretende situar conceptualmente los términos de un problema que ha emergido con fuerza tras la pandemia, aunque en cierto modo ya estaba incubado. Evidentemente, las reflexiones que siguen se retroalimentan de la trayectoria profesional de quien escribe y, especialmente, de algunos programas formativos, colaboraciones puntuales y trabajos o estudios de consultoría realizados en los últimos años, así como de determinadas reflexiones puntuales sobre este tema en diferentes entradas en el Blog *La Mirada Institucional*. Pero, especialmente, el trabajo de mayor calado que se ha realizado sobre este importante tema es la elaboración de un extenso Estudio de Consultoría que, en 2021, sirvió a la institución del Ararteko para publicar el Informe editado por la citada institución que lleva por título *Administración digital y relaciones con la ciudadanía; su aplicación a las administraciones públicas vascas*, y que daba continuidad a la Recomendación General del Ararteko 4/2020, esta centrada en la primera etapa de la pandemia. En el Estudio citado se pueden ampliar muchas de las reflexiones aquí contenidas; aunque en este texto se hace referencia a algunos documentos que, dada la fecha de su aprobación o difusión, no se reflejaban en el trabajo inicial.

I. ENCUADRE: ¿ES ACEPTABLE UNA DIGITALIZACIÓN DEL SECTOR PÚBLICO QUE EMPEORE LA ATENCIÓN O LA PRESTACIÓN DE SERVICIOS A LA CIUDADANÍA FRENTE A LA SITUACIÓN EXISTENTE EN LAS RELACIONES PRESENCIALES?

La digitalización de la sociedad es, sin duda, imparable. Y, como es obvio, tal proceso impacta sobre las Administraciones Públicas, así como, especialmente, sobre las relaciones entre los poderes públicos y la ciudadanía. La preocupación por esta cuestión es creciente, también por lo que implica de hipotética afectación a los derechos de la ciudadanía en sus constantes e inevitables relaciones con las Administraciones Públicas.

Nadie duda, en efecto, que la digitalización ha de ser inclusiva. Tampoco admite duda alguna que, en la transición digital y en la mejora de la prestación de los servicios públicos que tal estrategia comporta, es donde la legitimidad de los poderes públicos se juegan buena parte del crédito de confianza de la ciudadanía. Lo que es inaceptable en términos de legitimidad democrática es que la prestación de servicios y la atención a la ciudadanía empeoren con la digitalización. Y algo de esto está pasando hoy en día. Cabe preguntarse por qué y, asimismo, cuáles son los remedios para evitar esas patologías que están empezando a estar muy extendidas.

De todos es conocido cómo la pandemia no solo supuso una innegable aceleración de la digitalización, sino que, por lo que ahora interesa, implicó una tendencia marcada hacia el encastillamiento de las Administraciones Públicas que, justificándose en medidas de protección sanitaria de los empleados públicos y mediante las barreras que implicaban unas frías y anónimas pantallas, obligaron de forma fáctica (a pesar del evidente derecho de opción reconocido en las disposiciones legales vigentes) a que, salvo excepciones muy puntuales, los ciudadanos no obligados normativamente se tuvieran que relacionar también de forma exclusiva con las organizaciones públicas por medios telemáticos. Se generalizó, así, en un contexto de excepción un sistema denominado de *cita previa,* que ya venía funcionando en determinados ámbitos de la actuación administrativa, pero siempre mediante un sistema de acceso multicanal en el que la atención presencial no estaba excluida, como con la pandemia sucedió. El problema se agravó cuando el acceso a una solicitud de cita previa se contrajo hasta límites insólitos, llegando incluso a extenderse una *mafia* de obtención de citas previas que, mediante pago de cantidades, buscaban solución a situaciones muchas veces angustiosas para tramitar determinados procedimientos ante la Administración. Todavía hoy siguen existiendo esos canales oscuros de obtención de cita previa, previo pago de cantidades, en algunos ámbitos de las Administraciones Públicas. Pero ello se produjo, además, porque los canales alternativos a la presencialidad y a la tramitación telemática tampoco funcionaron, como ha sido el caso de la atención telefónica, que también en no pocas situaciones ha fracasado por comple-

to. Los teléfonos de la Administración hay veces, y no pocas, que nadie los coge. No hay respuesta. Es una nueva modalidad de silencio administrativo, más hiriente si cabe que la no respuesta; es el desprecio hacia el ciudadano que solicita una información o busca un cauce para llevar a cabo un trámite administrativo.

Sin embargo, el escándalo de la cita previa, ahora tan aireado, no es más que la punta del iceberg. Resulta llamativo cómo la crisis Covid19 fue una situación excepcional que, sin embargo, implicó cambios de tendencia estructurales (o con intentos de convertirse en tales) en el (mal) funcionamiento de buena parte del sector público español y de sus estructuras burocráticas. Todo esto con el silencio cómplice de una política gubernamental que frente estas cuestiones aparentemente instrumentales, pero que forman parte del ADN existencial del sector público, apenas ha venido prestando atención alguna. Sorprende así cómo responsables políticos ministeriales, autonómicos o locales miran para otro lado cuando en las dependencias administrativas de sus respectivos departamentos se pisan un día sí y otro también los derechos de la ciudadanía. Aún estamos esperando que el Parlamento o las Cámaras autonómicas, por no decir los plenos de los respectivos ayuntamientos, aprueben alguna declaración institucional en este sentido. Nadie se da por convocado o interpelado. Es un problema hiriente, pero que a la clase política, acomodada en sus prerrogativas y poco o nada interesada por los problemas tan prosaicos como este, no parece afectarle lo más mínimo.

Se olvida con frecuencia que, además, fue precisamente la pandemia la que aceleró una implantación excepcional y un tanto caótica de una modalidad de prestación de la actividad profesional en el empleo público como era el teletrabajo, que hasta entonces dormitaba (casi) inaplicado con la puntual excepción (tomada con cuentagotas) de la conciliación entre la vida laboral y familiar, que no es ni debería ser una justificación real del trabajo a distancia. Fruto de ese contexto excepcional, comenzó un reverdecer del teletrabajo en el sector público, animado por un mala e improvisada regulación normativa que convertía en estructural lo que hasta entonces se había configurado como excepcional; a lo que se unió una gestión desordenada de la puesta en marcha del teletrabajo desde el punto de vista organizativo, olvidando algunas cuestiones clave. Y estos puntos centrales a los que el teletrabajo debe dar respuesta no son otros que, por ejemplo, los siguientes:

1) Qué servicios se deben mantener siempre abiertos presencialmente;
2) Qué tareas y con qué intensidad pueden ser objeto de teletrabajo;
3) Qué objetivos se deben cumplir en el trabajo a distancia;
4) Qué medios de supervisión y control existen;
5) Y, en fin, qué modalidad de evaluación del cumplimiento de las tareas se desarrollará y con qué efectos.

La acelerada implantación de un teletrabajo que comenzó por una situación excepcional como era la pandemia (como indicó un gestor público: «Coge el ordenador

y corre a refugiarte en tu domicilio»), no se hizo ninguna de tales preguntas. El legislador que reguló esta materia, tanto en los iniciales reales decretos-leyes 28 y 29/2020, como posteriormente en la Ley 11/2021, tampoco se complicó mucho la vida con esas imprescindibles premisas para que esa modalidad de trabajo a distancia funcionaria realmente. Menos aún lo hizo el legislador del teletrabajo en el empleo público, suya regulación final del artículo 47 bis del EBEP, es sencillamente decepcionante. Y con esos mimbres normativos no podía salir mejor el cesto aplicativo. Primó, así, el derecho de los empleados (como se decía, mal regulado y peor aplicado) frente a los intereses públicos, eufemismo que esconde los innegociables derechos de la ciudadanía. Y de aquellos vientos, vienen algunas tempestades. Si los medios son malos, difícilmente podremos obtener un buen fin de la Administración. El teletrabajo, si no da respuesta correcta a las cuestiones planteadas, puede provocar (como en muchos casos está sucediendo) un empeoramiento de la prestación de los servicios públicos y de la propia atención a la ciudadanía. Y eso es una consecuencia grave, muy grave. No se pueden mejorar los derechos de los empleados públicos a disponer de un mayor confort en el ejercicio de sus prestaciones a costa de los derechos de la ciudadanía. Si se rompe la razón existencial de las Administraciones Públicas, que no es otra que hacer la vida más fácil a los ciudadanos, con mejores servicios y prestaciones, tal como se decía, la erosión de la legitimidad pública puede llegar a afectar a los cimientos del Estado Constitucional Social y Democrático de Derecho. Y no es ninguna broma.

Así, no sorprende cómo cada vez con más insistencia los medios de comunicación se hacen eco de las disfunciones que genera el teletrabajo en la prestación de servicios públicos o, en fin, del enorme eco que tiene la presencia del teletrabajo en el sector público a diferencia del privado. Como muestra dos ejemplos recientes. Comenzando por este aspecto, es llamativo, según se publicó en el diario digital *The Objective* (16 de abril de 2023), que el peso porcentual del teletrabajo en el sector privado sea en 2023 el 12 por ciento, mientras que en el sector público alcanza al 41 por ciento de la plantilla. Sorprende, por tanto, que el sector público, cuya vocación natural es de servicio y atención a la ciudadanía, disponga de esos porcentajes tan elevados; mientras que el sector privado limite o acote mucho más su uso. Y, en relación con el mal funcionamiento de los servicios públicos como consecuencia de una mala gestión del teletrabajo, los medios digitales están plagados de denuncias; por ejemplo, esta reciente publicada en el *Diario de Avisos* (17 de abril de 2023), en un reportaje que lleva por enunciado «Canarias, en emergencia burocrática», y en el que el Presidente de la Federación Provincial de Empresarios de la Construcción de Santa Cruz de Tenerife (FEPECO), aparte de quejarse amargamente por el mal funcionamiento de los servicios burocrático-administrativos, concluía sus reflexiones del siguiente modo: *«La implantación del teletrabajo ha hecho que las dependencias públicas de cualquier Administración se parezcan a una tienda de muebles en saldo, porque solo se ven mesas, sillas vacías, luces encendidas, aire acondicionado funcionando, armarios cerrados, alguna alma en pena. Los verdaderos héroes son los vigilantes de seguridad.»* No puede ser más gráfico y desgarrador

el testimonio. Tal vez, los responsables públicos del sector público español no han sido nunca consciente (o si lo han sido, aún sería más preocupante) de que con un sistema de empleo público que no sabe gestionar la diferencia y que carece de cualquier instrumento objetivo y efectivo de seguimiento y evaluación del rendimiento y del desempeño de las tareas realizadas, es totalmente imposible que el teletrabajo pueda funcionar siquiera sea con un mínimo de resultados en la gestión. De ahí al mayor deterioro del servicio público solo va un paso. Únicamente aquellas organizaciones públicas que consigan medir los resultados de las tareas realizadas a distancia, previa fijación de estándares, seguimiento o medición de resultados podrán ver cómo no se deteriora o degrada su propio funcionamiento, con afectación directa a la ciudadanía. Hoy por hoy, son muy pocas las Administraciones Públicas (más bien anecdóticas) que esos procesos los pueden llevar a cabo.

Un reciente ejemplo sangrante de limitación de derechos a la ciudadanía, es el denunciado por la organización CIVIO en relación con la tramitación del Ingreso Mínimo Vital. Un robot diseñado por CIVIO estuvo durante 18 días haciendo llamadas automatizadas cada media hora al teléfono oficial del IMV que gestiona dudas. Durante 150 llamadas nadie respondió. Y en la llamada 151 por fin se oyó una voz humana. Ni qué decir tiene que para cuando se contestó a esa llamada, más de 15 días después, muy probablemente el demandante de la información ya habría perdido sus derechos al finalizar los plazos reglamentarios de tramitación de la ayuda. Algo muy grave falla cuando la entidad oficial que gestiona las ayudas para paliar la pobreza extrema tiene esos déficit de gestión, que en este caso puedan tacharse de inhumanos.

Bien es cierto que, tras múltiples y reiterados atropellos de los derechos de la ciudadanía, esa deriva inicial como consecuencia de la pandemia parece iniciar ahora un lento proceso de reflujo hacia una relativa y tímida apertura de unas Administraciones Públicas que estaban cerradas a cal y canto. Pero la situación objetiva sigue siendo muy desigual. Cuando han transcurrido más de tres años desde el inicio de la pandemia, el retorno a la normalidad burocrático-administrativa en cuando a la atención presencial a la ciudadanía está siendo una operación compleja y dista muchísimo aún de haberse normalizado. El teletrabajo se ha considerado como una suerte de derecho adquirido en una situación excepcional que se pretende exportar sin matices a una situación de normalidad, la cita previa también se considera aún en muchas organizaciones públicas como el medio natural de canalizar la entrada de documentos por vía presencial, y mientras tanto los sufridos ciudadanos ven afectados directamente sus derechos sin que haya siquiera una justificación legal que avale tales atropellos. En efecto, hay aún innumerables Administraciones Públicas que siguen exigiendo cita previa (habitualmente telemática) para atender a la ciudadanía o para que se puedan presentar documentos en las oficinas de asistencia en materia de registros (con los problemas que ello implica de afectación a plazos y de vulneración del derecho de acceso al procedimiento administrativo o de las garantías del interesado, en su caso). Hay ejemplos hirientes, muy aireados en los medios de comunicación y en las redes sociales, como son los servicios administrativos de inmi-

gración, también determinados servicios sociales o prestaciones de esas características, pero especialmente el escándalo ha tomado unos visos de ser enorme en algunos territorios en lo que afecta a la gestión de la Seguridad Social y, en particular, en el acceso a las prestaciones del Ingreso Mínimo Vital o, más aún, en lo que afecta a las prestaciones por jubilaciones, donde ha habido innumerables quejas y denuncias ciudadanas sobre la imposibilidad material de obtener hora y día para gestionar tales asuntos.

Todo ello ha conllevado, además, intervenciones puntuales de las instituciones de defensa de los derechos de la ciudadanía (defensores del pueblo autonómicos y más tarde el Defensor del Pueblo estatal) e incluso unas efectivas campañas a través de las redes sociales y por diferentes blogs, (particularmente intensa ha sido la campaña promovida en las redes por el abogado gallego Diego Gómez) que han terminado por crear un clima de presión ciudadana que han hecho repensar algunos de esos cierres administrativos a la atención ciudadana directa o personalizada que habían sido sustituidos por la cómoda (para la Administración y para aquellas personas con amplias competencias digitales y recursos tecnológicos adecuados) atención telemática a través de las sedes electrónicas, distintas y muy diferenciadas en cuanto su accesibilidad y facilidad de uso, de las también nada homogéneas Administraciones Públicas. Sin embargo, sigue habiendo Administraciones Públicas que mantienen aún sus sistemas de cita previa inclusive para las oficinas de asistencia en materia de registros, ignorando las recomendaciones de las defensorías o no prestando ninguna atención a las innumerables quejas y denuncias de los medios de comunicación y de las redes sociales. Como antes se decía, no se dan por aludidos. Es una suerte de irresponsabilidad difusa. Nadie asume que la decisión es suya o que en su mano está cambiar ese estado de cosas. Es, sencillamente, una tomadura de pelo, que hace de los proyectos tan aireados de Gobierno abierto, Gobernanza colaborativa, transparencia participativa y otras lindezas, una rotunda mentira pública. La fragmentación administrativa en ese mosaico de estructuras gubernamentales superpuestas en el que se ha convertido este Estado llamado España, introduce más aún, dadas las también innumerables «sedes electrónicas» existentes (cada una con su factura propia), mayores dificultades para que los ciudadanos interrelacionen con esas Administraciones que, como siempre se dice en tono demagógico, están abiertas a la ciudadanía, ya que —según los discursos oficiales, que desmiente una y otra vez la práctica cotidiana— «lo importante son las personas» y «no dejar a nadie atrás». Eslóganes vacíos o mentiras piadosas, para autoconsumo interno.

II. DIGITALIZACIÓN DEL SECTOR PÚBLICO COMO PROCESO DE INTERACCIÓN DE NORMAS, ESTRUCTURAS, PROCEDIMIENTOS Y PERSONAS

No cabe duda que esas tendencias de (mal) funcionamiento organizativo de los servicios públicos que arrancan de hacer frente a una situación excepcional, fueron

modulando, sin apenas darnos cuenta, una Administración pública que descubrió en la digitalización y en la atención telemática, la solución definitiva a muchos de sus pretendidos problemas. En suma, ese cóctel de situaciones de excepcionalidad estructural-organizativa y de (mala) gestión de personas como intensa resaca de la pandemia, ha terminado generando en algunos casos un deterioro paulatino del funcionamiento de las organizaciones y de los servicios públicos en claro detrimento de los derechos de la ciudadanía. La inevitable interacción entre normas, estructuras, procesos y personas en lo que a resultados de la gestión pública afecta, se advierte aquí con toda su plenitud. La digitalización ha de comportar, tal como se decía más arriba, mejoras sustantivas en la calidad de prestación de los servicios públicos. No se puede desagregar la digitalización como proceso y abordar aisladamente medidas como si no tuvieran relación entre ellas, pues cualquier decisión puntual afecta directamente al corazón y al propio bombeo de sangre al sistema organizativo en su conjunto.

En efecto, si se quiere lograr una digitalización efectiva e inclusiva, tanto desde la dimensión interna de la propia Administración como especialmente de sus relaciones con la ciudadanía, debe existir una plena armonía entre los cuatro polos que conforman la transformación digital del sector público; a saber:

a) la tecnología;
b) los procesos;
c) la organización y gestión de personas;
d) la ciudadanía.

No basta que las Administraciones Públicas inviertan mucho en recursos tecnológicos si estos no mejoran la efectividad de los resultados de gestión. Cualquier proceso de digitalización obliga a la organización a adoptar medidas de transformación, y asimismo a ser conscientes de que una digitalización efectiva impactará inevitablemente sobre las tareas y rediseño de los puestos de trabajo, pues debe implicar como finalidad última la prestación de mejores servicios a la ciudadanía y el fortalecimiento de la atención (también presencial), así como el acompañamiento a las personas con limitadas competencias digitales o déficit de recursos tecnológicos en el complejo proceso de transición digital, que al fin y a la postre es la última razón existencial de lo público y de la propia política.

Dicho de otro modo, una digitalización que no parta de los parámetros expuestos es, lisa y llanamente, un proceso condenado al fracaso. Si la digitalización no altera las estructuras, los procesos o las formas de trabajar, y sobre todo no mejora los resultados de la gestión de forma cuantitativa y cualitativa, lo único que se está logrando es incorporar tecnología a una máquina que carece de sentido y finalidad, que ha perdido la orientación, ocultado su misión y cuya visión se ha anulado, por no hablar de que sus valores se han extraviado. La clave a la respuesta frente a estos problemas está, por un lado, en la configuración de un modelo holístico de digitalización en el

sector público y, por otro, en la articulación de una transición efectiva que no descuide nunca a las personas que, por los motivos que fueren, se quedan al margen del proceso, en un papel de excluidos digitales, con lo que ello conlleva de potencial pérdida de derechos.

Fracasar en este modelo holístico de digitalización implica, por consiguiente, ahondar la fractura de falta de legitimidad y desconfianza que hoy en día impregna a las relaciones de la ciudadanía con el sector público, que cada día es mas honda. El descrédito de lo público no solo ha tocado a las puertas de la Administración, sino que ha entrado hasta sus últimos despachos y mesas de trabajo. Hay una percepción cada vez más generalizada de que las Administraciones Públicas maltratan a la ciudadanía, especialmente por un abandono irresponsable de la política gubernamental frente a este tipo de cuestiones, pero también por un marcado déficit organizativo y una pésima concepción sobre cómo implantar un proceso de digitalización, que cada vez será más disruptivo, y que orilla frecuentemente a los colectivos más vulnerables por razones de edad, económicas, sociales, de discapacidad o de género; pero asimismo ese desdén afecta a buena parte de una ciudadanía que encuentra un sinfín de *barreras digitales* en sus relaciones telemáticas con un sector público fracturado en miles de sedes electrónicas (oficinas virtuales) a las que se debe acceder en muchos casos tras la lectura y análisis de otros tantos centenares de manuales de instrucciones, a veces con una estructura compleja, lenguaje opaco y explicaciones tortuosas. Cualquier ciudadano español se relaciona al menos con tres niveles de gobierno (municipal, autonómico y central), pero también con innumerables departamentos o silos, por no hablar de estructuras administrativas inferiores. Cualquier nueva gestión telemática (ayudas o subvenciones, asistencia sanitaria, trámite de pensiones de jubilación, inscripciones o solicitudes de cualquier tipo, demanda de información o un larguísimo etcétera) implica habitualmente darse de bruces con una realidad digital adversa, que puede generar ansiedad, frustración, cabreo o incluso pérdida de derechos, en ciertos casos existenciales o de primera importancia. No es un tema menor, precisamente.

III. EL NUDO DEL PROBLEMA. DIGITALIZACIÓN DEL SECTOR PÚBLICO, CIUDADANÍA Y TRANSICIÓN DIGITAL

El presente trabajo parte de la premisa de que la digitalización en el sector público, y sus impactos sobre la ciudadanía, es un proceso abierto desde hace años (inclusive décadas), que se ha basado principalmente en determinadas estrategias públicas lideradas por la Comisión Europea. Esas estrategias europeas han tenido su reflejo mimético en el ámbito español, posteriormente trasladadas al campo normativo y asimismo a instrumentos de *soft law* en su versión más castiza. Pero sobre esos instrumentos ha intervenido asimismo un contexto de transformación acelerado del *statu quo* heredado de la era analógica como consecuencia de una revolución tecnológica altamente dis-

ruptiva; fenómeno que se ha visto multiplicado por la particular situación de excepción pandémica antes expuesta.

Lo realmente importante de este proceso es que esa disrupción que afecta directamente a las Administraciones Públicas y a sus relaciones con la ciudadanía, solo puede afrontarse con un mínimo éxito (o con unas secuelas que no terminen siendo heridas abiertas de difícil resolución) mediante *una transición digital ordenada y planificada*. Este es el punto clave del problema expuesto: una transición digital de tales características requiere no solo inversiones y medidas de incentivación crecientes, sino también un cambio radical en el modo y manera de entender esas relaciones. Al fin y a la postre un cambio de cultura política y administrativa sobre cómo encarar este complejo problema; que, de no afrontarse de forma decidida, se irá agravando con el paso del tiempo. Hay un cierto paralelismo, salvando las distancias, con la transición ecológica, sobre todo con los devastadores efectos del cambio climático, aspecto en el cual hay una cierta percepción cargada en algunos casos de irresponsabilidad política y ciudadana de que nada realmente sucede porque los efectos no son constantes sino a veces imperceptibles o de lenta, pero implacable, ejecución. Los resultados se advierten cuando nada parece tener remedio. Las advertencias de Philippe Blom o de Bruno Latour al respecto son esclarecedoras, pero también estremecedoras. La digitalización también avanza de forma silente en lo que respecta a sus letales efectos de exclusión social o de afectación puntual. Es una suma de individuos anónimos quienes se ven afectados. Su voz apenas se escucha, salvo en las redes sociales y, excepcionalmente, cuando reciben eco puntual y esporádico en algún medio de comunicación.

Llevar a cabo un proceso de transición digital ordenado y planificado exige, por tanto, un cambio radical de actitud de las organizaciones públicas, de sus líderes políticos, directivos y empleados públicos, lo que conlleva un despliegue de recursos vinculados con la empatía, la atención directa y el apoyo permanente a todos aquellos colectivos y personas que estén fuera, parcial o totalmente, de esos procesos disruptivos tecnológicos, corriendo el riesgo de quedarse en los márgenes de la sociedad y fuera, por tanto, de las prestaciones públicas que, en teoría, se ofrecen a toda la ciudadanía. El papel de la política es fundamental, debiendo poner en el punto de atención central a las personas, no solo de manera retórica, sino de modo efectivo. Y hasta ahora la política está prácticamente ausente a la hora de dar respuesta a semejante desafío. Asimismo, los responsables directivos o ejecutivos del sector público tienen que incorporar en su liderazgo una noción inclusiva de la integridad que alcance a la ética del cuidado. Ni que decir tiene que, por su parte, el papel de los funcionarios y del resto de empleados públicos, como facilitadores y protagonistas de una atención empática, directa y de apoyo a la ciudadanía en este campo, se muestra trascendental. Volver a situar los valores de servicio a la ciudadanía y de respeto efectivo por sus derechos en el centro de la acción político-burocrática de las estructuras gubernamentales se torna un objetivo imprescindible. Y, asimismo, los sindicatos del sector público deben ate-

nuar su exclusiva mirada corporativa (que promueve solo la defensa de los intereses de los empleados públicos) y abrir sus ojos a una realidad, a veces sangrante por su injusticia, que supone cercenar los derechos de la ciudadanía por una digitalización poco inclusiva o, en algunos casos, excluyente.

La transición digital planteada en términos correctos implica también una mayor atención del marco normativo vigente y del cúmulo cada vez mayor de instrumentos de *soft law* o de estrategias de digitalización a las personas y, concretamente, a aquellos colectivos o personas que se encuentran fuera de los circuitos digitales, sea por estar incluidos en grupos desaventajados o excluidos de la digitalización, o ya sea porque tienen dificultades para llevar a cabo diferentes trámites administrativos o gestiones burocráticas con el sector público de las que no pocas veces dependen soluciones existenciales de primera importancia para alguna de tales personas o colectivos (ayudas, subvenciones, pensiones, etc.).

Sorprende la insensibilidad inicial que las disposiciones normativas e instrumentos de *soft law*, tanto europeos como españoles, han mostrado a esta problemática de la exclusión digital y, en particular, a los medios de reparar tales déficits. Poco a poco esta tendencia parece remitirse, pero aún dista mucho de estar resuelta o ni siquiera encauzada. La transición digital, desde el punto de vista de las relaciones entre Administraciones Públicas y ciudadanía no ha pasado hasta fechas recientes de un mero recordatorio a veces lapidario incorporado en las normas o en las diferentes estrategias aprobadas tanto en la Unión Europea como en España. Una breve e incompleta referencia a este primer momento de este largo proceso puede ser necesaria.

En cualquier caso, hay una reflexión colateral que en estos momentos se torna necesaria. La digitalización comporta, en principio, el uso de diferentes medios para canalizar su uso; si bien, no cabe duda que en estos momentos (y más tras la pandemia) el teléfono móvil inteligente se ha convertido en un instrumento casi más importante que la propia documentación de identificación personal. Sorprende que, sea a través de ese medio electrónico o sea a través de otro cualquiera, a la ciudadanía se le haya obligado a disponer de instrumentos digitales para sus relaciones (también su identificación) con las Administraciones Públicas. Desde un punto de vista de ejercicio de libertades, no cabe duda que las personas no disponen ya de derecho de opción frente a esas exigencias. Si la persona es un huérfano de la digitalización se transformas fácilmente en un paria y su visibilidad administrativa es inexistente. Ello tiene serias implicaciones sobre los derechos de la ciudadanía, que ya están condicionados en su ejercicio por el fenómeno digital, que es puramente instrumental pero que afecta de lleno a la sustancia del ejercicio de tales derechos, al margen de que inaugure (y desarrolle hasta su plenitud) un capitalismo de vigilancia (Zuboff) o, incluso, un control con ribetes de autoritarismo de la actividad de las personas a través de su huella digital y el trazado, siempre identificable, de sus actividades telemáticas que consumen buena parte de su actividad vital.

IV. ESTRATEGIAS EUROPEAS DE DIGITALIZACIÓN E INCLUSIÓN DIGITAL. DE LA DIGITALIZACIÓN DE LA ECONOMÍA A LA INCLUSIÓN DIGITAL

No cabe orillar que la inclusión digital ha estado siempre presente en las estrategias europeas de digitalización, aunque ese protagonismo al inicio fuera muy tibio y se ha ido haciendo más creciente conforme el proceso ha adquirido ribetes más disruptivos y acelerados. Así, en 2010, la Comunicación de la Comisión Europea, *Una Agenda Digital para Europa,* se hizo eco de tal enfoque. Sin embargo, su incidencia mayor se proyectó sobre la falta de capacitación de los usuarios por no tener una alfabetización digital adecuada y en los problemas de brecha digital derivados de la discapacidad, aunque también incidentalmente se refería a los grupos sociales desfavorecidos. La Comisión centró el foco durante los años siguientes en lo que se denominó como *Una Estrategia para el Mercado Común Único Digital de Europa*, que tenía por objeto central fomentar la competitividad de la UE, en un mercado cada vez más globalizado y con dos potencias que eran muy fuertes en este terreno (Estados Unidos y China). Buscar un cierto equilibrio será, a partir de entonces, una línea de actuación central de la UE. Pero en este enfoque el ciudadano se diluía, salvo en lo que afectaba a su protección de datos personales (RGPD de 2016), que ha sido uno de los puntos fuertes de la legislación europea frente al menos incisivo marco regulatorio estadounidense en materia de privacidad de datos personales (no digamos nada del totalitarismo digital que se ha terminado imponiendo en la República Popular China en lo que a protección de datos personales respecta).

Aun así, en el marco de esa estrategia, el propio Parlamento europeo instó a la Comisión a llevar a cabo «una mejor cooperación entre las administraciones públicas y ofrece(r) un servicio mejor, más fácil y personalizado a todos los ciudadanos». Recomendaba, por tanto, la confección de «planes de acción», pero sus medidas iban dirigidas a salvaguardar la seguridad, la protección de datos, la accesibilidad y otras cuestiones conexas, no prestando atención específica a la brecha o exclusión digital.

Años después, la Comunicación de la Comisión titulada *Generar confianza en la inteligencia artificial centrada en el ser humano* (COM (2019) 168 final), como su propio enunciado indica, «coloca a la persona en el centro del desarrollo de la Inteligencia Artificial», buscando articular un «marco ético y jurídico apropiado». Así, el *Libro Blanco sobre la inteligencia artificial: un enfoque europeo orientado a la excelencia y la confianza*, es plenamente consciente de que, sin perjuicio de que la IA se está desarrollando rápido (y de que) cambiará nuestras vidas», esta tecnología disruptiva «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». Así, se enuncia con claridad el papel central de la persona en el uso de tal tecnología, lo que se ha configurado como una visión antropomórfica de la IA.

Este es el trazado argumental del citado *Libro Blanco*: «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»; debiendo generarse en el sector público «un ecosistema de confianza», por los evidentes riesgos a los derechos fundamentales que puede comportar su (mal) uso. Pero siendo importantísimo este enfoque, en verdad lo que se pretende proteger en este caso son los derechos fundamentales de *toda la ciudadanía*; esto es, no se adopta aquí un tratamiento sesgado o parcial de esta tecnología disruptiva aplicada a ciertos colectivos o personas, sino al conjunto de la población. Este objetivo general puede generar, paradójicamente, una dispersión de efectos y una pérdida del foco selectivo que esa política de digitalización debería tener en torno a una mirada orientada, como se decía, a la transición digital, que por esencia afecta desigualmente a las personas y a los diferentes colectivos de la sociedad. En todo caso, se añade a modo de justificación que «la adopción de una IA ética y fiable en toda la economía de la UE», implica configurar esta tecnología bajo la óptica de «estar al servicio de las personas y ser una fuerza positiva para la sociedad». Este enfoque impregnará, sin duda, la *Estrategia Nacional de Inteligencia Artificial*, que se asienta sobre esos mismos fundamentos.

Quizás, uno de los documentos más importantes que sobre esta materia ha generado estos últimos años la Comisión Europea sea el titulado *Shaping the Digital Transformation in Europe* (2020), en el que, partiendo de estrategias y enfoques anteriormente aplicados por la Comisión, incide en crear ecosistemas tecnológicos, dotarse de un liderazgo digital, pero también incide en un punto muy relevante a nuestros efectos como *la gestión prudente de la transición digital y de sus riesgos.* En efecto, esta estrategia Europea de carácter holístico sobre el alcance y los efectos de la digitalización (que transita desde los impactos de la digitalización sobre el cambio climático, la salud, la educación, el empleo o, entre otros muchos ámbitos, sobre la propia ciudadanía y el tejido empresarial, así como sobre los aspectos éticos en sus aplicaciones), advierte desde el inicio de los riesgos que comportan las tecnologías disruptivas en términos de incremento de las desigualdades, por lo que resulta necesario adoptar un conjunto de medidas que conformen a esa transformación digital en un fenómeno inclusivo y sostenible. Parte el citado documento de que en torno al 22 por ciento de los empleos se verán afectados en Europa por la digitalización, cuyo porcentaje cabe presumir que será mayor en la Administración Pública, especialmente en aquellos empleos cuyas tareas dominantes sean de gestión o trámite administrativo, siempre más fáciles de automatizar o a de aplicar programas de Inteligencia Artificial. Asimismo, en el marco de la suscripción de nueve iniciativas para orientar el camino hacia la digitalización, el citado documento pone hincapié en cómo garantizar un impacto social positivo, en el sentido de que se recojan medidas de inclusión social que contrapesen los potenciales efectos adversos que los riesgos de una digitalización desordenada pudiesen comportar.

Se puede decir que, con esas nuevas bases conceptuales que refuerzan el papel inclusivo de la digitalización, es cómo se deben construir en Europa los esfuerzos de digitalización permanente a los que llama la Comisión, particularmente a través del esfuerzo inversor que implican las diferentes estrategias semestrales y, en especial, tras la dura

y compleja pandemia con la puesta en marcha del programa *Next Generation EU* y con los programas estructurales de inversión articulados a través del Marco Financiero Plurianual 2021-2027. Ambos ejes de actuación ponen el foco, como se verá de inmediato en la digitalización como eje central de las actuaciones inversoras con el fin de reforzar la transformación y la resiliencia de las diferentes economías de la Unión Europea.

En efecto, todos esos documentos europeos sobre digitalización someramente expuestos, adquieren hoy en día más importancia por un dato objetivo en nada menor: la incorporación de la transformación digital como una de las líneas-fuerza de los proyectos de inversión enmarcados en el Instrumento Europeo de Recuperación y, concretamente, en el Mecanismo de Recuperación y Resiliencia, o en lo que convencionalmente se ha denominado como los fondos europeos extraordinarios dirigidos a poner en marcha una política anticíclica de estímulos que puso en circulación la Unión Europea a partir de 2020 por medio de los fondos *Next Generation EU*, dotados para España, como es sabido, inicialmente con 140.000 millones de euros (hoy en días ampliados a una cifra superior a los 150.000 millones de euros) en concepto de ayudas no reembolsables y préstamos en condiciones ventajosas; transferencias financieras que están sujetas o condicionadas, como también es sabido, a la puesta en marcha de una serie de reformas estructurales. A partir de la aprobación de tales fondos (julio 2020) y de su concreción normativa, primero tras el Reglamento (UE) 2020/2094, del Consejo, de 14 de diciembre de 2020, por el que se establece un Instrumento de Recuperación de la Unión Europea para apoyar la recuperación tras la crisis Covid-19, y después, por medio del Reglamento (UE) 2021/241, del Parlamento Europeo y del Consejo, de 12 de febrero de 2021, por el que se establece el Mecanismo de Recuperación y Resiliencia (MRR), el papel de la digitalización en la sociedad y en su tejido empresarial, en las administraciones públicas (o en el sector público en su conjunto) y sobre la propia ciudadanía adquirirá una velocidad de vértigo en los próximos años. A todo ello se ha unido más recientemente la estrategia europea en el plano de la energía, que se concreta en el Plan para poner fin a la dependencia de la UE con respectos a los combustibles fósiles rusos (*REPowerEU*), que se ha concretado, entre otras acciones normativas, alineadas más con la transición verde, pero con algunos reflejos más tangenciales en el ámbito de la digitalización: por ejemplo, en el Reglamento (UE) 2022/1369 del Consejo, de 5 de agosto, sobre medidas coordinadas para la reducción del gas, y en el Reglamento (UE) 2022/1032 del Parlamento Europeo y del Consejo de 29 de junio de 2022 por el que se modifican los Reglamentos (UE) 2017/1938 y (CE) 715/2009 en relación con el almacenamiento de gas; ambos reglamentos dictados en el marco del citado Plan *REPowerEU* presentado en mayo de 2022, bajo las pautas establecidas en la Comunicación de la Comisión de 8 de marzo de 2022 «REPowerEU: Acción conjunta para una energía más asequible, segura y sostenible».

Ese refuerzo a la digitalización procedente de la Unión Europea ha ido adoptando un giro (aún parcial y de cierta timidez) desde postulados más económicos y tecnológicos hacia un mayor protagonismo de las personas y, por tanto, de la trascendencia

que la transición digital tiene para alcanzar que tan complejo proceso no implique fracturas sociales y exclusiones digitales que puedan enturbiar sus resultados.

Y esa tendencia se advierte de modo mucho más marcado a partir de otros documentos más recientes de la Unión Europea, como son, por ejemplo, la Comunicación de 9 de marzo de 2021, *Brújula Digital 2030: el enfoque de Europa para el Decenio Digital* [COM(2021) 118 final], o la más reciente *Declaración Europea sobre los Derechos y Principios Digitales para la Década Digital*, proclamada por el Parlamento Europeo, el Consejo y la Comisión [COM(2022) 28 final], de 26 de enero de 2022.

El primero de tales documentos asienta la estrategia *Brújula Digital 2030* sobre cuatro puntos cardinales. Y, a nuestros efectos, es importante el primero de ellos, que se enuncia del siguiente modo: *Ciudadanos con capacidades digitales y profesionales del sector digital muy cualificados.* Este primer eje de actuación pretende contar con una ciudadanía cualificada digitalmente, tanto en lo que afecta al mundo del trabajo como a la disponibilidad de incrementar el número de expertos. Pero mucho más importante es a nuestros efectos la meta que se pretende alcanzar en 2030 por lo que afecta a competencias digitales: «El Plan de acción del pilar europeo de derechos sociales prevé que el objetivo de porcentaje de adultos con al menos capacidades digitales básicas sea del 80 % en 2030», según prevé el *Plan de acción del pilar europeo de derechos sociales* [COM(2021) 102]. Sin duda, esa base de una alta capacitación digital, al menos en competencias básicas, es una premisa necesaria para alcanzar el reto de que la ciudadanía interaccione con las Administraciones Públicas sin riesgo alguno ni dificultades adicionales tanto en la demanda de servicios como en la realización de trámites. Pero adviértase que el objetivo es del 80 % a cumplir en 2030, año hasta el cual queda aún un largo trecho temporal y, por consiguiente, un amplio período de tiempo en el que las medidas transitorias para evitar los desajustes que se puedan dar son, más que necesarias, imprescindibles, sobre todo si se quieren paliar los efectos de una digitalización excluyente. Y aun así, en el hipotético caso que se alcanzaran esos porcentajes de competencias digitales básicas en 2030, cabe constatar que, al menos, un 20 % de la población quedaría extramuros de esas capacidades digitales básicas y, por consiguiente, no podría interactuar digitalmente con garantías con la Administración Pública correspondiente. Ni que decir tiene que los poderes públicos no pueden dejar a la intemperie a esas personas, menos aún cuando con toda probabilidad serán las más vulnerables socialmente.

En ese sentido, la estrategia europea *Brújula Digital 2030* resulta un tanto decepcionante, pues cuando trata en su punto cardinal cuarto de la *Digitalización de los servicios públicos* presenta de modo retórico la necesidad de que los servicios públicos permitan a los ciudadanos «influir en la dirección y los resultados de las actividades de los Gobiernos de forma más eficiente y mejorar los servicios públicos», estableciendo unos servicios públicos digitales que faciliten un acceso general y fácil a los servicios públicos con una interacción continua de capacidades avanzadas, como el tratamiento de datos, la inteligencia artificial y la realidad virtual»; aunque rápidamente, en un ejercicio de realismo, se admite en el mismo documento que, «sin embargo, falta bastante para

materializar esta visión». Si bien el objetivo final es muy loable, que en el espacio digital todos los ciudadanos tengan los mismos derechos que se aplican fuera de línea y puedan ejercerse plenamente por medios telemáticos, el camino a recorrer no será fácil y menos aún sino se adoptan desde el inicio medidas efectivas de acompañamiento a las personas y colectivos más vulnerables (discapacitados, personas de edad avanzada, migrantes, familias monoparentales, especialmente mujeres vulnerables, jóvenes sin recursos, etc.), pero también a aquellos que encuentran serias dificultades para adecuarse a los cambios tecnológicos tan disruptivos que conlleva muchas veces la relación con las diferentes organizaciones del sector público, plurales en su estructura y competencias, pero también en sus medios tecnológicos de acceso y tramitación digital. El objetivo de un «entorno digital centrado en el ser humano», que aparece explicitado en las conclusiones de la propia estrategia *Brújula Digital 2030* requiera, como se viene insistiendo, no solo medidas programáticas o declarativas sino un conjunto de acciones escalonadas que acompañen de forma efectiva en esa compleja transición, aspecto hasta ahora bastante descuidado, por no decir que en algunos casos abandonado.

No obstante, la *Declaración Europea sobre Derechos y Principios Digitales para la Década Digital* ofrece, a pesar de ser un instrumento de *Soft Law*, un arsenal de ideas fuerza y de principios que deberían servir para articular unas medidas normativas de transición digital tanto por lo que afecta a la normativa europea como particularmente a la española, que se encuentra bastante desfasada en este punto y, en especial, tal enfoque tendría que incidir sobre el modo cómo las organizaciones públicas afrontan la transición digital desde parámetros inclusivos y de garantías a los derechos de la ciudadanía más vulnerable o con menores recursos y competencias tecnológicas para interactuar con el sector público por medios digitales.

Comienza la *Declaración* con un preámbulo que pone en valor esa centralidad de la persona en los procesos tan disruptivos que se vivirán en los próximos años con la digitalización, y destaca, así, que «la transformación digital afecta a todos los aspectos de la vida de las personas», destacando el papel que el Parlamento Europeo viene otorgando a la inclusividad, lo que exige en línea con las Declaraciones de Tallín, Berlín y Lisboa, que «el modelo de transformación digital refuerce la dimensión humana del ecosistema digital». Y, por consiguiente, en línea con lo expuesto en la *Brújula Digital 2030*, aunque ahondando en la dimensión personal del proceso de digitalización, se apuesta decididamente por «una transformación digital centrada en los ciudadanos, basada en la solidaridad y la inclusión, y que recuerda la importancia de la libertad de elección». Y este último inciso es muy relevante (aunque en el documento analizado esa libertad de elección se despliegue solo sobre la inteligencia artificial y un entorno digital justo), porque, efectivamente, la inclusión parte de la inevitable premisa de que hay personas y colectivos que, por motivos educativos o sociales, están fuera del entorno digital o con serios problemas para poder moverse adecuadamente y con garantías en tal ecosistema, a quienes se deben ofrecer, por tanto, alternativas viables que exigen de las Administraciones Públicas atención presencial alternativa para que, en ejercicio

de esa libertad de elección, puedan acudir a ella para la realización de trámites, consultas o la recepción de servicios públicos.

Esa Declaración sitúa de forma correcta (Capítulo I) a las personas en el centro de la transformación digital. Pero tal enunciado declarativo se complementa con lo establecido en el Capítulo II que tiene como objeto la *Solidaridad e inclusión*, donde se abordan cuestiones tan relevantes como la garantía de que «las soluciones tecnológicas respeten los derechos de las personas, permitan su ejercicio y promuevan la inclusión», lo que implica «llevar a cabo una transformación digital que no deje a nadie atrás y que debería incluir (aspecto de especial importancia al objeto de este trabajo), «en particular, a las personas mayores, a las personas con discapacidad o a las personas marginalizadas, vulnerables o privadas de derechos, así como a quienes actúen en su nombre». El documento comentado incide asimismo sobre un aspecto relevante como es el de «velar por la transparencia en el uso de los algoritmos u la inteligencia artificial», al efecto de que las personas estén informadas sobre sus posibles afectaciones. En cualquier caso, esa *Declaración* parece dar un paso más en la necesidad de articular una ordenada y efectiva transición digital, aunque tampoco termina por culminar una batería de propuestas y medidas que salvaguarde su efectividad y minimice los riesgos de exclusión digital.

Si esto sucede así en la Unión Europea, la situación en España es aún menos receptiva a un marco de digitalización que sea inclusivo, articulando esas medidas de transición que se tornan imprescindibles, puesto que, como se verá de inmediato, tanto el marco normativo como los documentos que dan pie a los procesos de transformación digital del sector público y de sus relaciones con la ciudadanía, apenas pasan de las meras declaraciones de intenciones. Veamos, por tanto, cuáles son a grandes líneas los ejes del marco normativo y las diferentes estrategias de digitalización que culminan en estos momentos en el Plan de Recuperación, Transformación y Resiliencia, interesando solo en estos momentos cómo tratan tales normas y, sobre todo, los planes e instrumentos estratégicos, la transición digital como medio de facilitar la incorporación de la ciudadanía a esos procesos disruptivos tecnológicamente que están en marcha, con el fin de evitar su afectación a la calidad de los servicios públicos recibidos y a un más que evidente deterioro de la atención ciudadana, dado que ambos ejes deben ser mejorados de forma inmediata para paliar las exclusiones digitales que hoy en día se advierten.

V. LA DIGITALIZACIÓN EN ESPAÑA A IMPULSO DE LA UNIÓN EUROPEA Y SU CONCRECIÓN EN DETERMINADOS DOCUMENTOS DE ESTRATEGIA, INSTRUMENTOS DE *SOFT LAW* Y EN EL PLAN DE RECUPERACIÓN, TRANSFORMACIÓN Y RESILIENCIA

En consecuencia, depende cómo se haga esa digitalización, esto es, de qué manera se articule e implante tal proceso, y sobre todo cómo se gestione la siempre compleja

transición, veremos si realmente mejoran las prestaciones públicas a la ciudadanía o, por el contrario, estas se ven preteridas o empeoradas. Los riesgos, como se viene advirtiendo en estas páginas, son muy tangibles y hoy en día muy evidentes. La brecha digital, especialmente por lo que afecta a España, no se está atenuando si no que, en ciertos aspectos, se está profundizando, «dejando a muchas personas atrás», a pesar de que la Agenda 2030 y los diferentes ODS pretendieran precisamente lo contrario, y de que los mensajes gubernamentales insistan un día sí y otro también machaconamente en esa idea. Esto se ha visto en lo que afecta a muchos colectivos vulnerables (tercera edad, situaciones pobreza, familias monoparentales, menores, etc.) y áreas de actuación de la Administración Pública (educación, servicios sociales, ingreso mínimo vital y renta de garantía de ingresos, sistema de pensiones, sanidad, inmigración, etc.). Bien es cierto que el Informe *DESI 2022* ofrece una ligera mejoría de los indicadores de digitalización, asimismo en lo que afecta a capacidades o competencias digitales de la ciudadanía, en relación con los que ofrecían los Informes anteriores. Pero aun así, el número de ciudadanos de este país que no acreditan disponer de competencias digitales básicas, que serán las necesarias para poder entablar relaciones digitales con las Administraciones Públicas, ronda los veinte millones de personas, lo que sencillamente es una barbaridad. A ello cabe añadir quienes no tienen la suficiente confianza en tales medios telemáticos para llevar a cabo gestiones administrativas de las que se pueden derivar el reconocimiento o pérdida de derechos económicos o patrimoniales. Asimismo, es necesario sumar quienes, aun disponiendo de competencias digitales al efecto, no comprenden adecuadamente los formularios administrativos electrónicos (por su lenguaje opaco) y, por tanto, pueden errar en tales tramitaciones. Al margen de lo ya expuesto en relación con los laberintos digitales que son muchas veces las múltiples y diferenciadas sedes electrónicas de las distintas Administraciones Públicas, muy alejadas —pese a la metáfora siempre empleada de que las sedes electrónicas son, en paralelismo con las físicas, las oficinas «virtuales» de la Administración— de los clásicos pasillos, ventanillas y mesas de los funcionarios de carne y hueso. Las pantallas, más todavía las administrativas, son frías y oscuras.

En todo caso, en el marco normativo europeo citado la transición digital, junto con la transición ecológica, se convierten en los dos pilares más firmes sobre los que se ha de asentar la ansiada recuperación económica. Hasta el punto de que el MRR sitúa unos umbrales mínimos de inversión sobre el total de los recursos transferidos por parte de la Unión Europea que han de alcanzar el porcentaje del 20 por ciento del total de ayudas y préstamos (porcentaje que en el caso de España el Plan de Recuperación sube hasta casi el 30 por ciento del total en lo que a transformación digital respecta). Ese elevadísimo porcentaje en lo que afecta a las contribuciones financieras no reembolsables, se verá ampliado —según los datos ofrecidos recientemente por el Gobierno de España— en la *Adenda al Plan de Recuperación, Transformación y Resiliencia* que se presentará ante la Comisión Europea para tener acceso a los créditos reembolsables que superan la cifra glotal anterior, en cuyo programa inversor también la digi-

talización alcanza un amplio porcentaje de recursos dedicados a la digitalización, en ocasiones vinculada con la sostenibilidad medioambiental.

No deja de ser curioso el afán digitalizador del Gobierno de España, que supera con creces porcentualmente hablando los límites establecidos, por ejemplo, en el caso de la transición ecológica, cuyo porcentaje exigido por el MRR era del 37 por ciento, y el determinado por el Plan de Recuperación presentado por el Gobierno a la Comisión llega al 39 por ciento, dos puntos más de los exigidos, frente a casi 10 puntos más en el caso de la digitalización, al menos por lo que respecta al primer Plan de Recuperación, sin computar la Adenda que actualmente se está preparando para solicitar el segundo tramo de los fondos NGEU por lo que afecta al préstamo. Dicho de otro modo, en digitalización España pretende consumir más del treinta por ciento de los recursos financieros de los fondos NGEU, a los que se deberán sumar los proyectos financiados en el marco de los fondos estructurales y de inversión del Marco Financiero Plurianual 2021-2027, que serán también numerosos.

La gran pregunta es si una digitalización tan intensiva y extensiva fomentará la recuperación y creará realmente empleo (o no lo destruirá inicialmente), así como si realmente servirá para integrar a la población y no dejarla al margen o, en su defecto, como ya anuncian algunos expertos, multiplicará la desigualdad. A tal efecto, las medidas que se incluyan en cada Componente y en los diferentes proyectos, subproyectos y líneas de inversión se convierten así en el eje fundamental de tal transformación digital, sobre todo en si esta será inclusiva o creará, por el contrario, mayor exclusión digital.

Efectivamente, el *Plan de Recuperación, Transformación y Resiliencia*, y en la misma línea camina la *Adenda al Plan* (no se olvide en este punto el papel protagonista como actor institucional que tiene la Vicepresidencia primera del Gobierno, con competencias precisamente sobre este ámbito), sitúa a la Administración Digital y a la digitalización de la sociedad como uno de los grandes retos de futuro. Así, por ejemplo, la digitalización está presente en diferentes políticas palanca de las diez en las que se estructura el citado Plan, pero asimismo en muchos y diferentes Componentes de los treinta en que se subdividen las distintas políticas palanca. La digitalización está, por tanto, vinculada nada más y nada menos que con 21 de los 30 Componentes del Plan de Recuperación. Se ha de tener en cuenta que cada Componente desglosa —como es sabido— las reformas que se proponen y los diferentes proyectos de inversión en los que se gastarán los recursos recibidos de la Unión Europea (en este primer Plan de Recuperación son todos ellos contribuciones financieras no reembolsables por una cuantía un poco inferior inicialmente a los 70.000 millones de euros). La digitalización afectará, así, al segundo pilar del Mecanismo de Recuperación y Resiliencia en ámbitos tales como movilidad sostenible, infraestructuras eléctricas, modernización de las Administraciones Públicas, política industrial y apoyo a las PYMEs, conectividad digital, estrategia de inteligencia artificial, ciencia y tecnología, sistema nacional de salud, competencias digitales, formación profesional y sistema educativo, y un largo etcétera.

De los presupuestos de este *Plan de Recuperación* bien se puede concluir que se han abierto un sinfín de expectativas y una suerte de alocada carrera por diseñar y promover proyectos de digitalización tanto internos como externos por parte de las Administraciones Públicas. Da la impresión de que, si tales exigencias se cumplen, España en 2026 (fecha en la que se debería ultimar la ejecución de los fondos NGEU, según está previsto y si no se aplaza ese término) tendría que ofrecer un panorama institucional, empresarial, social y ciudadano radicalmente distinto al actual en lo que a digitalización respecta. Al menos, eso es lo que se pretende, otra cosa es que se consiga. Los retos son enormes y, hasta la fecha, la ejecución camina con paso muy lento, con una digestión pesada tanto en el nivel central de gobierno como en los autonómicos y locales, con una capilaridad muy atenuada en lo que afecta al mundo empresarial y profesional, también en este ámbito, centrando el esfuerzo principal hasta ahora en la dotación de infraestructuras y recursos tecnológicos (la mayor parte de las veces bienes de equipos) a las Administraciones Públicas y entes del sector público, y algo menos al tejido empresarial y profesional (autónomos), quienes —como se decía— están recibiendo con mayor lentitud esos recursos financieros procedentes de los fondos europeos para mejorar sus infraestructuras tecnológicas y apostar por una digitalización más disruptiva en su ámbito de actuación

En verdad, en lo que afectan a las Administraciones Públicas, los componentes que más inciden en el plano de la digitalización de esas organizaciones y de las personas que en ellas trabajan son el 11 (*Modernización de las Administraciones Públicas*) y el 19 (*Plan Nacional de Capacidades Digitales*), que ambos tienen su inspiración y origen tanto en la *Agenda Digital España 2025* y en los documentos tales —que ahora no procede analizar— como la *Estrategia Nacional de Inteligencia Artificial* (2020), inspirada en buena medida en el Libro Blanco europeo sobre la materia, el *Plan de Digitalización de las Administraciones Públicas 2021-2024* (2021) y el *Plan Nacional de Competencias Digitales* (2021), ambos con una innegable huella en la confección del PRTR, especialmente de los distintos componentes en los que la digitalización está presente y, en particular, en las medidas de inversión.

Asimismo, también se consiguió aprobar en julio de 2021, después de un largo proceso de elaboración, la *Carta de Derechos Digitales*, un documento también de *Soft Law* que, como su propio nombre indica, muestra alguna sensibilidad adicional o marginal al aspecto que aquí se está tratando, cuando lacónicamente, en el epígrafe de «Derechos digitales de la ciudadanía en sus relaciones con las Administraciones Públicas», establece lo siguiente: «Se ofrecerán alternativas en el mundo físico que garanticen los derechos de aquellas personas que opten por no utilizar recursos digitales» (XVI). No añade mucho a lo que ya prevé la Ley (Ley 39/2015, en su artículo 14), aunque parece invertir los términos del problema, ya que parece ser la voluntad del sujeto quien determina el derecho de opción, mientras que en el marco regulatorio vigente es la Administración quien lo hace, de conformidad con una serie de exigencias formales y materiales allí establecidas (artículo 14.2 y 14.3 LPAC).

Por su parte, la Ley Orgánica 3/2018, de protección de datos personales y garantía de los derechos digitales, tal como expone la última parte de su enunciado, trata de los derechos digitales de la ciudadanía, pero apenas se refiere a las relaciones entre ciudadanía y Administración Pública, un importante aspecto que queda limitado a una serie de derechos declarativos o meras invocaciones para que las Administraciones Públicas apuesten por la inclusión digital. Así, el artículo 81 de la LOPDGDD reconoce un genérico derecho de acceso universal a Internet, donde persigue, en términos de objetivos políticos declarativos, la reducción de la brecha de genero, generacional y la producida en entornos rurales. Y, por su parte, el artículo 97 se limita asimismo a esbozar unas líneas de actuación de los Ejecutivos central y autonómico, cuyas acciones irán encaminadas a superar las brechas digitales. Pero, nada se concreta; por lo que tales enunciados normativos tienen un sesgo predominante de naturaleza declarativa e, incluso, de principios sin aportar ningún tipo de medidas ni tampoco de definir cuál es el contenido efectivo de esos derechos.

No se puede aquí tratar, por razones de espacio y porque excede el objeto de este trabajo, el papel de la Inteligencia Artificial en sus posibles afectaciones a los derechos de la ciudadanía cuando sea la Administración Pública quien utilice tal tecnología disruptiva en el ámbito de sus procesos de decisión o administrativos (tramitación y resolución de expedientes). Alguna referencia puntual a esta materia se halla también en la citada *Carta de Derechos Digitales* (XVI).

VI. FINAL

En todo caso, el marco normativo español en lo que afecta al derecho de la ciudadanía a ser atendido físicamente es, ciertamente, muy frágil, a pesar de la regulación prevista en la LPAC, que ha puesto el foco de forma determinante también en los derechos digitales, en tanto en cuanto la pretensión de ese texto normativo es, conjuntamente con lo previsto en la Ley 40/2015 y en el Real Decreto 203/2021, acelerar la digitalización del sector público y, por consiguiente, «empujar» (por medios unas veces sutiles, otras fácticos y en ocasiones normativos) a que los ciudadanos se relacionen cada vez más intensamente con las Administraciones Públicas a través de medios electrónicos, superando, así, el funcionamiento dual que el sector público ahora tiene que seguir, en la medida en que los procedimientos administrativos deben ser siempre telemáticos, pero si la ciudadanía opta (o, mejor dicho le dejan optar) por la atención presencial (y, por tanto, a relacionarse a través de la oralidad y del papel), las organizaciones públicas deben digitalizar tales documentos (tarea, por lo demás, no compleja) y, asimismo, deben crear los entornos y medidas organizativas adecuadas (también en el ámbito de los recursos humanos) para hacer efectivo ese derecho a la atención presencial, hoy en día en franco declive por el desinterés acusado de los poderes públicos a garantizarlo de forma apropiada.

Se echa de menos, por tanto, un marco normativo básico y autonómico que establezca un sistema de relaciones entre ciudadanía y Administración Pública, dando respuesta efectiva a todos los problemas aquí expuestos. No es objeto de este trabajo el análisis del marco normativo vigente; pero conviene llamar la atención sobre el *déficit regulatorio* que sobre las relaciones entre Administración Pública y ciudadanos existe en estos momentos en España. Hay vacíos normativos que son oceánicos, y que deberían ser corregidos de forma inmediata. La LPAC, aquella norma que pretendía —según se dijo— tener una visión exógena o *ad extra*, apenas cita al ciudadano en su parte dispositiva, pues solo recoge unos genéricos derechos establecidos en el artículo 13, que hoy por hoy se muestran insuficientes para encarar ese largo y complejo proceso de transición digital que deberá emprender cuanto antes mejor el sector público español, sino quiere que los estándares de deslegitimación de las Administraciones Públicas caigan más aún de lo que ya están en estos momentos. El desafío es inmenso y el tiempo corre en contra.

En general, en todos esos documentos analizados en el presente trabajo la presencia de la brecha digital o de la exclusión digital tiene escaso o nulo protagonismo. Un poco más de atención parece prestarse a estos temas en los últimos documentos analizados; pero tampoco demasiada. Las referencias a la brecha digital se enmarcan (al menos en el caso español) en el ámbito de la brecha de género, que es solo una manifestación del problema; mientras que en Europa comienza a advertirse qué, en efecto, en esta cuestión pude haber un problema. Dicho de otro modo: la clave está en que se diseñe y ejecute correctamente una adecuada transición digital, un proceso que, además, será largo en el tiempo y plagado de dificultades en su ejecución. Los problemas de las transiciones, tanto la digital como la verde, son los verdaderos desafíos de los próximos años para las instituciones públicas.

No se puede ocultar que el proceso de digitalización que está viviendo la sociedad cada día es más acelerado. Pero, ello no implica que la propia Administración deba ahogarse en una suerte de *ansiedad administrativo-burocrática* que no sabemos muy bien hacia dónde va. Se necesita sosiego y capacidad de visión estratégica de lo que implica la digitalización en términos de atención a la ciudadanía, que es, al fin y a la postre, el ADN existencial de la Administración Pública. Sin embargo, el foco de atención se sigue prestando en digitalizar aceleradamente y, en la medida de lo posible, emplazar directa o indirectamente a que los ciudadanos opten ya de forma definitiva y sin retorno por unas relaciones electrónicas con la Administración Pública; es decir, siempre mediadas con pantallas, donde la presencia física del funcionario se diluye hasta incluso desaparecer, ya que no hay interlocución con personas, sino con formularios, manuales, instrucciones de uso, o todo lo más con consultas telemáticas. No hay caras, no hay voces, no hay ojos, no hay manos, ni hay gestualidad alguna que muestre empatía o comprensión. La Administración se impersonaliza a ritmos frenéticos. Su razón existencial se pierde o desvanece. ¿Eso es, realmente, la Administración que queremos para el futuro de España y de las relaciones con sus ciudadanos? ¿Realmente

queremos una Administración de robots *anonimizada,* en la que las personas apenas aporten valor añadido? ¿Buscamos, ciertamente, que todas las relaciones Administración Pública y ciudadanía se canalicen exclusiva o preferentemente a través de medios electrónicos, erradicando (casi) totalmente la atención personalizada? Si es así, llegará un día en que esa pésima inteligencia de la idea de *Gobierno abierto* no solo se transforme, paradójicamente, en *Administración cerrada*, sino que sin apenas darnos cuenta quizás lleguemos a comprobar que, en verdad, la Administración Pública, tal como la conocimos, ya no existe. Emergerá, así, una *Administración muerta,* al menos en su sentido existencial tal como la hemos conocido en los últimos siglos. En una correcta transición digital está la clave para que ello no suceda.

VII. BIBLIOGRAFÍA

Ararteko: Administración digital y relaciones con la ciudadanía. Su aplicación a las administraciones públicas vascas: https://www.ararteko.eus/es/administracion-digital-y-relaciones-con-la-ciudadania-su-aplicacion-las-administraciones-publicas-vascas

Arateko: Recomendación general 4/2020, *Necesidad de reforzar la atención ciudadana para evitar perjuicios en el ejercicio de los derechos de las personas en sus relaciones con las administraciones públicas y de adoptar medidas para luchar contra la exclusión digital en situaciones de emergencia como las derivadas de la pandemia de la Covid-19.* https://www.ararteko.eus/es/recomendacion-general-del-ararteko-42020.

AEPD, *Tecnologías y Protección de Datos en las Administraciones Públicas*, Madrid, noviembre 2020.

Baricco, A. (2019): *The* game, Anagrama.

Chaves, J. R. (2020): «la cita previa ante la Administración. Un virus jurídico». https://delajusticia.com/2020/07/10/la-cita-previa-ante-la-administracion-un-virus-juridico-que-se-extiende/

COMISIÓN EUROPEA (2010): *Una Agenda Digital Europea,* Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, COM (2010) 245 final/2

COMISIÓN EUROPEA (2020): *Shaping Europe's Digital Futur*, 2020. Se puede consultar en: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/shaping-europe-digital-future_es

COMISIÓN EUROPEA (2019): *Generar confianza en la inteligencia artificial centrada en el ser humano* (COM (2019) 168 final)

COMISIÓN EUROPEA: *Libro Blanco sobre la inteligencia artificial - un enfoque europeo orientado a la excelencia y la confianza* Bruselas, 19.2.2020 COM(2020) 65 final.

COMISIÓN EUROPEA: *Brújula Digital 2030: el enfoque de Europa para el Decenio Digital* [COM(2021) 118 final].

COMISIÓN EUROPEA: *Declaración Europea sobre los Derechos y Principios Digitales para la Década Digital*, proclamada por el Parlamento Europeo, el Consejo y la Comisión [COM(2022) 28 final], de 26 de enero de 2022.

COMISIÓN EUROPEA (2022): Comunicación de la Comisión de 8 de marzo de 2022 «REPowerEU: Acción conjunta para una energía más asequible, segura y sostenible».

Colom, C. (2020), «Las brechas digitales que deben preocuparnos y ocuparnos», *Ekonomiaz 98*, cit., pp. 351-352.

Cotino, L. (2008): «Derechos del ciudadano», en *La Ley de Administración electrónica. Comentarios a la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos»,* E. Gamero y J. Valero, coordinadores.

Fondevila Antolín, J. (2020): *La gestión de los procesos selectivos en un entorno digital,* CEMCI, Granada.

García-Álvarez, G. (2016): «Derecho de los interesados en el procedimiento», en Eduardo Gamero, *Tratado de Procedimiento Administrativo Común y Régimen Jurídico Básico del Sector Público*, Tirant lo Blanch, pp. 1403 y ss.

Gamero Casado; E. y Valero Torrijos J. (coordinadores) (2008): *La Ley de Administración electrónica. Comentario sistemático a la Ley 11/2017, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos,* Thompson/Aranzadi.

GOBIERNO DE ESPAÑA (2019): Gobierno de España, *Estrategia Nacional de Inteligencia Artificial,* noviembre de 2020.

GOBIERNO DE ESPAÑA (2021): *Agenda España Digital 2025*, julio.

GOBIERNO DE ESPAÑA (2021): *Plan Nacional de Competencias Digitales.*

GOBIERNO DE ESPAÑA (2021): *Plan de Digitalización de las Administraciones Públicas*.

GOBIERNO DE ESPAÑA (2021): *Plan de Recuperación, Transformación y Resiliencia*.

GOBIERNO DE ESPAÑA (2021): *Carta de Derechos Digitales.*

Gómez, D. (2019): «Administración electrónica en la Ley 39/2015: «¿Un nuevo despotismo ilustrado?», *Revista #DIRECTUM,* Colegio de Abogados de Barcelona

——(2023): «Obligatoriedad de la cita previa y los plazos administrativos» https://www.derechoadministrativoyurbanismo.es/post/la-obligatoriedad-de-la-cita-previa-y-los-plazos-administrativos

Lassalle, J. M. (2019): *Ciberleviatán. El colapso de la democracia liberal frente a la revolución digital*, Arpa.

Martín Delgado, I. (2017): *La reforma de la Administración electrónica. Una oportunidad para la innovación desde el Derecho*, INAP.

Martínez Gutiérrez, R. (2009): *Administración Pública electrónica,* Civitas/Thompson Reuters.

Rodríguez Zapatero, J. (2020): *Por una España Digital. Una Hoja de Ruta para que Estado y Empresa den el salto a la economía digital,* Deusto.

Valero Torrijos, J. (2007): *El régimen jurídico de la e-Administración: el uso de medios informáticos y telemáticos en el procedimiento administrativo.*

CAPÍTULO 2

LOS DERECHOS DIGITALES Y LA BUENA ADMINISTRACIÓN DIGITAL

Mónica Arenas Ramiro

Universidad de Alcalá
monica.arenas@uah.es

SUMARIO

I. INTRODUCCIÓN

Hablar de una buena Administración en el marco del proceso de digitalización como el que viven nuestras sociedades hace imprescindible ponerlo en conexión con los llamados derechos digitales de los ciudadanos a los que va a prestar sus servicios.

No obstante, hay algo que queremos dejar señalado en relación con el llamado derecho a una buena Administración, y es el convencimiento de que estamos ante un verdadero derecho fundamental,[1] lo que será la premisa sobre la que analizaremos el juego con el resto de derechos digitales reconocidos. A pesar de su no reconocimiento expreso como derecho fundamental a nivel nacional —sí a nivel europeo en el art. 41 de la Carta de Derechos Fundamentales de la Unión Europea (CDFUE)—, sino como principio, analizaremos lo que ello implica para la estructura social y democrática de

[1] Por todos, destaca la brillante monografía de una de las primeras personas que sostuvo la tesis de la existencia de un derecho fundamental a una buena Administración pública. Vid. Tomás Mallén, B., *El derecho fundamental a una buena Administración*, INAP, Madrid, 2004. Vid., también, Rodríguez-Arana, J., «La buena Administración como principio y como derecho fundamental en Europa», en *Revista Misión Jurídica*, Vol. 6, Núm. 6, 2013, pp. 23-56; y Moreno Molina, J.A., «El derecho a una buena Administración», *Lección inaugural del solemne acto de apertura del Curso Académico 2022/2023 de la Universidad de Castilla-La Mancha*, Ediciones de la Universidad de Castilla La Mancha, Cuenca, 2022.

nuestros Estados. Sobre esta idea construiremos la necesidad de identificar los derechos de los ciudadanos frente a la Administración y hacerlo en clave digital.

La Administración pública es quien se encarga, esencialmente, de prestar un servicio a los ciudadanos, por lo que una buena Administración pública está dirigida a servir al interés general de forma eficiente, eficaz, equitativa, transparente y abierta a la participación ciudadana, entre otros valores.[2] Por ello una buena Administración se hace esencial en una democracia moderna.[3]

Pero para entender y ver esta conexión, se hace necesario comenzar analizando el reconocimiento actual de los derechos digitales, así como el proceso de digitalización de la Administración pública, para pasar a continuación a identificar cuáles son los derechos digitales de los ciudadanos frente a la misma en ese proceso de modernización.

Vivimos un proceso de digitalización innegable e imparable y que se ha visto acelerado no sólo por los numerosos avances tecnológicos de los últimos años, sino por los acontecimientos provocados por la pandemia a nivel mundial,[4] y que nos obligaron a mantener medidas de distanciamiento social para combatir el virus, pero nos han conducido también a inventar y poner en marcha herramientas tecnológicas no sólo para proteger nuestra salud,[5] sino para no cerrar negocios, poder ofrecer servicios públicos, continuar con los procesos educativos o estar en contacto con la gente querida.

Es más que evidente que todo ello ha supuesto un cambio de paradigma en nuestras sociedades, en la forma de entender y aplicar el Derecho y de ejercer los derechos

---

[2] Rodríguez-Arana define una buena Administración pública como «aquella que cumple con las funciones que le son propias en democracia. Es decir, una Administración pública que sirve objetivamente a la ciudadanía, que realiza su trabajo con racionalidad, justificando sus actuaciones y que se orienta continuamente al interés general. Un interés general que en el Estado social y democrático de Derecho reside en la mejora permanente e integral de las condiciones de vida de las personas» (Rodríguez-Arana, J., «La buena Administración…», *op. cit.*, p. 26). Sobre su definición tanto en clave positiva como en clave negativa frente a una «mala Administración», vid. Tomás Mallén, B., *El derecho fundamental… op. cit.,* pp. 68-96.

[3] Novales, A. (Coord.), *La modernización de la Administración pública*, Fedea Policy Paper 2022/01, enero 2022, p. 1.

[4] La declaración de pandemia se llevó a cabo el 11 de marzo de 2020 por la Organización Mundial de la Salud (OMS). Vid. Declaración de pandemia internacional de la OMS, aprobada el 11 de marzo de 2020, así como la alocución del Director General de la OMS en la rueda de prensa (Disponible en: https://www.who.int/es/director-general/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing-on-covid-19---11-march-2020).

[5] Todos recordaremos, a nivel nacional, el fallido caso de la conocida RadarCOVID. Vid., «La aplicación dejó de estar disponible el 9 de octubre de 2022, tras dos años de funcionamiento y de haber infringido la normativa de protección de datos», como resolvió la AEPD en su procedimiento sancionador de 18 de febrero de 2022 (Expdte. Nº PS/00222/2021. Publicado el 9 de junio de 2022. Disponible en: https://www.aepd.es/es/documento/ps-00222-2021.pdf). Vid. «Radar Covid muere definitivamente después de fracasar en la lucha contra la pandemia», en *Diario ABC*, de 8 de octubre de 2022 (Disponible en: https://www.abc.es/tecnologia/moviles/aplicaciones/radar-covid-muere-definitivamente-despues-fracasar-lucha-20221008093003-nt.html). Sobre estas aplicaciones, *vid.* Arenas Ramiro, M., «¿Rastrear o no rastrear? He ahí la cuestión. Las apps de rastreo de contactos y la protección de datos», en *La Ley Privacidad*, nº 5, julio-septiembre 2020.

y libertades por parte de los ciudadanos. Y como no podía ser de otra forma, esto también ha supuesto un cambio en la forma de ejercer estos derechos y de relacionarnos con la Administración pública y ha supuesto también un cambio y una modernización de la propia Administración.

La modernización de la Administración se ha convertido en una prioridad de los Gobiernos. De hecho, la Agenda España Digital 2026, presentada por el Gobierno el 8 de julio de 2022, recoge entre sus medidas un Plan de Digitalización de las Administraciones Públicas con el fin de mejorar su eficacia y eficiencia, especialmente en ámbitos como el empleo, la justicia o las políticas sociales mediante la actualización de las infraestructuras tecnológicas.[6] Según la citada Agenda, el objetivo es que en 2025 el 50 % de los servicios públicos estén disponibles a través de apps móviles, simplificando y personalizando la relación de los ciudadanos con las Administraciones.[7] Y en esta línea se encuentra también el Plan de Recuperación, Transformación y Resiliencia presentado igualmente por el Gobierno y en conexión con los Fondos *Next Generation*, y en cuyo Componente 11 incluía una propuesta de modernización de las Administraciones públicas.[8]

Vemos pues que esta transformación digital lo impregna todo, generando nuevas oportunidades a la vez que incorpora amenazas y riesgos significativos. Afecta al conjunto de nuestras realidades y a todos los aspectos de nuestra vida, desde la política a la sociedad y a la economía, desde el individuo a la comunidad, y traspasando fronteras, no se queda en los Estados. Y, como hemos dicho, la Administración pública no es una excepción en este proceso.

En esta línea, resulta indispensable entender que los efectos positivos y negativos de esta transformación digital afectan prácticamente a todos los derechos fundamen-

---

[6] Vid. *España Digital 2026*, julio 2022, especialmente Apartado sobre «Transformación digital del sector público», pp. 64-78. Disponible en https://espanadigital.gob.es/sites/espanadigital/files/2022-07/Espa%C3%B1aDigital_2026.pdf.

[7] Vid. *España Digital 2026*, p. 68; y, también, *Estrategia Nacional de Inteligencia Artificial (ENIA)*, noviembre de 2020, cuyo quinto Eje estratégico está destinado a «Potenciar el uso de la IA en la administración pública y en las misiones estratégicas nacionales», pp. 56-64. Disponible en: https://www.lamoncloa.gob.es/presidente/actividades/Documents/2020/ENIA2B.pdf. Aquí se hace referencia al uso de la Inteligencia Artificial se señala que «la IA permitirá una reducción de trámites y una automatización de tareas obteniéndose servicios más adaptados, de mayor usabilidad, accesibilidad y personalizados a la ciudadanía y empresas» (p. 62).

[8] Presentado por el Gobierno el 7 de octubre de 2021. Sobre el mismo, vid. https://planderecuperacion.gob.es/, y disponible en https://www.lamoncloa.gob.es/temas/fondos-recuperacion/Documents/160621-Plan_Recuperacion_Transformacion_Resiliencia.pdf. Hay que tener en cuenta también su Adenda, presentada en diciembre de 2022 (Disponible en https://portal.mineco.gob.es/RecursosNoticia/mineco/prensa/noticias/2022/20221221_Adenda.pdf). Vid. también el RDL 36/2020, por el que se aprueban medidas urgentes para la modernización de la Administración Pública y para la ejecución del Plan de Recuperación, Transformación y Resiliencia; y sobre dicha norma y sus desafíos, vid. Rivero Ortega, R. (Dir.), *Modernización de la Administración pública para la ejecución del Plan de Recuperación, Transformación y Resiliencia. Comentarios de urgencia al RDL 36/2020, de 30 de diciembre*, Ratio Legis, Salamanca, 2021.

tales. Las nuevas tecnologías o los entornos digitales no se convierten en fuentes del Derecho, sino que, entendemos, son los poderes públicos los que, tomando como punto de partida la esencia y fundamento de los derechos fundamentales, esto es, la dignidad y desarrollo personal, deben definir las normas y políticas públicas destinadas a garantizar los derechos fundamentales en este nuevo marco o entorno digital. Por ello, los derechos fundamentales deben perfilarse en los entornos y espacios digitales y, además, deben, especialmente, ser garantizados en el nuevo entorno digital. Y es en este contexto cuando podemos hablar de derechos digitales.

Más allá de estas consideraciones, nos gustaría recordar aquí que no sólo los derechos fundamentales se van a ver afectados por esta transformación digital, sino que está en juego la propia estructura social y democrática de nuestros Estados. Si no hacemos frente de forma correcta —o no protegemos de forma correcta— el impacto de los avances tecnológicos en los derechos y adaptamos nuestros poderes públicos para que puedan dar respuesta en este proceso de transformación digital, contribuiremos a un proceso de desafectación mayor del existente y los ciudadanos ya no sólo dejarán de sentirse representados, sino que dejarán de confiar en los poderes públicos, con el pernicioso efecto que esto supone para la propia estructura democrática de nuestros Estados.

Esto es, la forma en la que se vean afectados nuestros derechos en los entornos digitales, pero, sobre todo, la forma de garantizarlos y protegerlos por los poderes públicos será lo que marcará la forma de nuestros Estados.

II. LOS DERECHOS DIGITALES

Antes de analizar brevemente si estamos o no ante nuevos derechos en este proceso de transformación digital y cuáles son los que disfrutan los ciudadanos en sus relaciones con la Administración, como documentos de referencia que regulan los llamados derechos digitales a nivel estatal encontramos tanto la LO 3/2018 de Protección de Datos Personales y Garantía de Derechos Digitales (LOPDGDD) y la conocida Carta de Derechos Digitales, presentada por el Gobierno dos años y medio más tarde, en julio de 2021.

Por un lado, la LOPDGDD regula la garantía de los derechos digitales en su Tít. X (arts. 79 a 97). En concreto, en su art. 79 se refiere a los derechos en la Era digital. Destacamos aquí no sólo que la LOPDGDD no considera que estemos ante nuevos derechos —pues señala que los derechos reconocidos en la CE y en resto de normas internacionales «son plenamente aplicables en Internet»—, sino que hace partícipes y garantes de su aplicación a los prestadores y proveedores de servicios de Internet.

Por otro lado, aunque sin carácter vinculante porque no es una norma jurídica, el texto nacional de referencia en el terreno de los derechos digitales lo representa la ya citada Carta de Derechos Digitales presentada por el Gobierno. Como se recoge en las

Consideraciones Previas de dicho documento, la Carta es un marco de identificación de los conflictos que se plantan en el entorno digital, así como una llamada a la regulación y a la adopción de las políticas públicas adecuadas.

II.1. Los derechos digitales

Antes de plantearnos el papel de los poderes públicos y los mecanismos de garantía de los derechos en este proceso de transformación digital, lo primero que tenemos que analizar es si estamos ante derechos ya existentes —para conocer de qué garantías gozan y si son, o no, suficientes—, o bien, si estamos ante nuevos derechos, derechos digitales —y que requieren garantías digitales—.[9]

Así pues, el reto que se plantea al Derecho es si estamos ante nuevos derechos que requieran de un desarrollo legislativo o de un reconocimiento constitucional que les dote de las máximas garantías; o si bien estamos ante los «tradicionales» derechos ya reconocidos en nuestros textos constitucionales y lo que demandan es sólo (que no es poco) una actualización o una reinterpretación de sus garantías adaptándolas al entorno digital.

Recordamos llegados a este punto (aunque sin detenernos) que, tradicionalmente, los derechos se han ido reconociendo a lo largo de la historia, hablándose de generaciones de derechos o de declaraciones de derechos, que han ido ampliándose e internacionalizándose.[10] Las generaciones de derechos han ido de la mano de la evolución del Estado social y democrático de Derecho tal y como lo conocemos hoy en día, pasando de ser derechos humanos a ser considerados fundamentales, con carácter general, cuando éstos son reconocidos y garantizados por un texto constitucional.[11] Y, en este punto, la revolución tecnológica ha llevado a plantearnos si estamos ante el nacimiento de nuevos derechos y de una nueva generación de derechos, de «derechos del futuro», a falta de una «construcción dogmática».[12]

La pregunta debería ser, por lo tanto, si no son suficientes los derechos ya reconocidos en Tratados y textos constitucionales. Y para dar respuesta debemos fijarnos no sólo en las nuevas demandas sociales, sino en el objeto y en el contenido de los nuevos derechos que proponen ser reconocidos. Mientras que el objeto de un derecho hace

---

[9] Rallo Lombarte, A., «Una nueva generación de derechos digitales», en *Revista de Estudios Políticos*, nº 187, 2020, pp. 101-135.

[10] Sobre las generaciones de derechos, por todos, Pérez Luño, A.-E., «Las generaciones de derechos humanos», en *Revista del Centro de Estudios Constitucionales*, nº 10, 1991, pp. 203-217; y Díez-Picazo, L.M., *Sistema de Derechos Fundamentales*, 3ª ed., Thomson/Civitas, Madrid, 2008, pp. 35-37, 40 y 42-44.

[11] Entre otros, vid., Gutiérrez Gutiérrez, I. (Coord.), *Elementos de Derecho constitucional español*, Marcial Pons, Madrid, 2014, pp. 268-270.

[12] Fernández Rodríguez, J. J., «Derechos y progreso tecnológico. Pasado, presente y futuro», en Engelmann, W. (Coord.), *Sistema do Direio, novas tecnologías, globalizaçao e o constitucionalismo contemporáneo,* Universidad Santiago de Compostela, A Coruña, 2020, pp. 259-277 (pp. 271-272).

referencia al ámbito vital que éste protege, que puede ser un ámbito material, una esfera vital o una espacio excluido de la acción del poder público, el contenido de los derechos hace referencia al conjunto de facultades o posibilidades de actuación y garantías en defensa de los propios intereses, y puede ser determinado por el legislador o por los Tribunales.[13]

Así las cosas, si analizamos los ahora denominados derechos digitales, para conocer su objeto y contenido debemos fijarnos dónde y cómo se reconocen.

Sin detenernos en normas y declaraciones internacionales, europeas, o de otros países,[14] por lo que a España se refiere, y como ha quedado dicho, no existen derechos digitales constitucionalmente reconocidos de forma expresa, pero nuestro Estado sí que ha querido reconocerles cierta entidad y desarrollarlos legalmente y así lo ha hecho en normas y en declaraciones no vinculantes. Nos referimos, en primer lugar, a la citada LOPDGDD, esto es, LO 3/2018, de Protección de Datos Personales y Garantía de Derechos Digitales. Esta norma, destinada a regular básicamente el tratamiento de datos personales, incluye en su Título X (artículos 79 a 97), de forma novedosa en nuestro ordenamiento jurídico, los llamados derechos digitales. Entre los derechos que la LOPDGDD reconoce en su Título X, se encuentran los derechos a la neutralidad de la Red así como el del acceso universal a Internet; los relacionados con la seguridad digital; los vinculados a los menores e Internet; los relacionados con los medios de comunicación digital; los relativos al ámbito laboral como el conocido derecho a la desconexión digital; o los vinculados con el tratamiento de la información personal y las facultades que otorga a sus titulares como el derecho al olvido en Internet o el testamento digital. Todos estos «nuevos derechos» reconocidos como objeto de la LOP-

[13] Gutiérrez Gutiérrez, Ignacio (Coord.), *Elementos de Derecho…*, *op. cit.*, pp. 273-247. Fue el Tribunal Constitucional español el que en su Sentencia 11/1981 indicó (FJ 8º) que determinar el contenido de un derecho fundamental se puede hacer, por un lado, a través de lo que disponga la doctrina dominante y la jurisprudencia que identifique las facultades sin las cuales el derecho quedaría desnaturalizado, y, por otro lado, identificando los intereses a los que sirve garantizar el derecho concreto y por los que fue constitucionalizado.

[14] Dejamos aquí solamente citadas: a nivel internacional, la Resolución de la ONU, de 13 de julio de 2021, sobre la *Promoción, protección y disfrute de los derechos humanos en Internet*. A nivel europeo, la *Declaración sobre los Derechos y Principios Digitales para la Década Digital,* de febrero de 2023. En Italia, ya en 2015 —lo que fue una de las primeras iniciativas nacionales sobre la materia, aunque sin carácter vinculante—, se aprobó la *Declaración de Derechos en Internet* (*Dichiarazione dei Diritti in Internet*). Un año más tarde, en 2016, y todo un referente en tanto que fue la primera norma con carácter vinculante, Francia aprobó su *Ley para una República digital* (*Loi pour une République numérique*). Años más tarde, en abril de 2021, en Portugal se aprobó la *Carta portuguesa de Derechos Humanos en la Era Digital* (*Carta Portuguesa de Direitos Humanos na Era Digital*), que en realidad era una Ley de carácter vinculante. Y en Iberoamérica, con carácter general, vid. la *Carta Iberoamericana de Principios y Derechos en Entornos Digitales,* aprobado durante la XXVIII Cumbre Iberoamericana de Jefes de Estado y de Gobierno, 25 de marzo de 2023, bajo el lema «Juntos hacia una Iberoamérica justa y Sostenible». Además, en línea con el proceso de la Carta portuguesa, aunque muchos años antes, en 2014, en Brasil se aprobó la que fue llamada la «primera Constitución de Internet del mundo» o «Marco civil de Internet», aunque en realidad era una Ley; y en Chile debemos destacar el reciente y novedoso ejemplo del reconocimiento de los derechos neurológicos de la Constitución chilena tras su reforma en 2021.

DGDD deberán ser garantizados conforme al mandato establecido en el art. 18.4 CE, esto es, limitando el uso de la informática con el fin de «evitar la traición de la tecnología».[15] No obstante, la mayoría de los derechos reconocidos en esta norma requieren de un desarrollo legislativo o reglamentario posterior, lo que casi a mediados de 2023, año de elecciones autonómicas, municipales y generales, todavía no se ha producido ni hay previsión de que así sea.

En segundo lugar, en España, más allá del citado reconocimiento formal a nivel legislativo, encontramos, como también hemos citado, la Carta de Derechos Digitales, aprobada por el Gobierno el 14 de julio de 2021 que, aunque no tiene valor vinculante porque no es una norma jurídica, es todo un referente interpretativo. Esta Carta reconoce, entre otros, los siguientes bloques de derechos: derechos de libertad como la identidad digital o el derecho al no perfilado; derecho de igualdad como el derecho de acceso y no discriminación; los derechos de participación y conformación del espacio público como la exigencia de información veraz; y los derechos del entorno laboral y empresarial.

Si nos fijamos en los citados documentos españoles —como ocurre con otros textos normativos o declarativos—, más que referirse a nuevos derechos, la Carta indica que «no se trata necesariamente de descubrir derechos digitales pretendiendo que sean algo distinto de los derechos fundamentales ya reconocidos o de que las nuevas tecnologías y el ecosistema digital se erijan por definición en fuente de nuevos derechos».[16] O añade expresiones indicando que no se trata «de crear nuevos derechos fundamentales, sino de perfilar los más relevantes en el entorno y los espacios digitales o describir derechos instrumentales o auxiliares de los primeros»;[17] mientras que la LOPDGDD indica que «los derechos y libertades consagrados en la Constitución y en los tratados y convenios internacionales en que España sea parte son plenamente aplicables en Internet»,[18] no como algo diferente de los derechos ya existentes.

Por último, a mayor abundamiento, si observamos los llamados derechos digitales, vemos que su fundamento último no difiere de la esencia de los que podríamos llamar «derechos tradicionales», ya que según indica, por ejemplo, la Carta de Derechos Digitales española, «la persona y su dignidad son la fuente permanente y única de los

---

[15] Rallo Lombarte, A., «De la «libertad informática» a la constitucionalización de nuevos derechos digitales (1978-2018)», en *Revista de Derecho Político*, nº 100, 2017, pp. 646-647, con referencia a los debates constitucionales que se produjeron a la hora de redactar el art. 18.4 Constitución Española plasmados en la obra publicada por las Cortes Generales y editada por Sainz Moreno, F. (Ed.), *Constitución española. Trabajos parlamentarios*. Tomo I, Cortes Generales, Madrid, 1980, pp. 1068 y ss.

[16] Carta de Derechos Digitales española de 2021, Consideraciones previas.

[17] Carta de Derechos Digitales española de 2021, Consideraciones previas.

[18] Art. 79 LOPDGDD. De la misma forma que lo hiciera la ya citada Resolución de la Asamblea General de las Naciones Unidas sobre la *Promoción, protección y disfrute de los derechos humanos en Internet*, aprobada por el Consejo de Derechos Humanos el 13 de julio de 2021 (A/HRC/RES/47/16. Distribuida el 26 de julio de 2021), Pto. 1, al señalar que «los mismos derechos que asisten a las personas fuera de Internet también deben protegerse en línea».

mismos y la clave de bóveda tanto para proyectar el Ordenamiento vigente sobre la realidad tecnológica, como para que los poderes públicos definan normas y políticas públicas ordenadas a su garantía y promoción».[19]

Por todo ello, entendemos —personalmente y a riesgo de equivocarnos— que la tecnología no pone de manifiesto nuevos derechos con nuevos objetos o ámbitos dignos de protección, sino nuevos escenarios que obligan a reflexionar sobre el alcance de los derechos tradicionales y sus garantías, que obligan a determinar su contenido. Si las nuevas demandas sociales no tuvieran su reflejo en los derechos ya reconocidos constitucionalmente, sólo entonces podríamos hablar de la necesidad de reconocer nuevos derechos.[20] El objeto de estos supuestos nuevos derechos no difiere del objeto de los tradicionales derechos ya reconocidos en los textos constitucionales y en Tratados o Declaraciones internacionales.

Así pues, entendemos que más que nuevos derechos digitales, lo que se produce es una impregnación del carácter digital en los derechos ya existentes, en su ejercicio, y que lo que se requiere es un proceso de reinterpretación o desarrollo de los tradicionales derechos adaptándolos y protegiéndolos en un entorno digital. Además, lo determinante no será reconocerlos, sino hacerlos efectivos y protegerlos,[21] y las Declaraciones no son suficiente.

Por todo ello, es esencial tener en cuenta que el reconocimiento de nuevos derechos debe suponer un «triunfo» frente al Estado, que será, en último término, quien los tenga que hacer efectivos y proteger, y frente a quien podrán ser exigidos. Y esto se debe trasladar al ámbito de la Administración pública.

II.2. El papel de los poderes públicos

Más allá de la discusión doctrinal analizada, tenemos que señalar que las clasificaciones de generaciones de derechos tienen un valor más académico que práctico, pues lo realmente relevante a la hora de reconocer derechos es garantizarlos, dotarles de protección.

Si bien la LOPDGDD garantiza legalmente el conjunto de derechos a los que denomina digitales, no han faltado las voces que han evidenciado que si bien dicho reconocimiento es «loable», la propia norma rebaja las expectativas de protección al no otorgarles el rango de ley orgánica y, por lo tanto, la máxima protección que nuestro ordenamiento

---

[19] Carta Derechos Digitales española de 2021, Consideraciones previas.

[20] Cotino Hueso, L., «Nuevo paradigma en las garantías de los derechos fundamentales y una nueva protección de datos frente al impacto social y colectivo de la inteligencia artificial», en Bauzá, M. (Coord.) / Cotino, L. (Dir.), *Derechos y garantías ante la Inteligencia Artificial y las decisiones automatizadas*, Aranzadi, Pamplona, 2022, pp. 69-105 (p. 72); y Escobar Roca, G., *Nuevos derechos y garantías de los derechos*, Marcial Pons, Madrid, 2018, pp. 99 y ss..

[21] Fernández Rodríguez, J. J., «Derechos y progreso tecnológico…», *op. cit.*, p. 272.

jurídico garantiza a los derechos fundamentales. Se evidencia así que, a pesar de que pueda existir una demanda social, existen dificultades de «materialización jurídica».[22]

En este sentido, recordamos que, ya sea para hablar de nuevos derechos o para reinterpretarlos, para garantizar su ejercicio y su eficacia, se requiere de un reconocimiento formal y vinculante, no una mera declaración de intenciones. Y ello requiere, en último término, un altísimo nivel de consenso político y social, que puede verse fuertemente condicionado en razón del escenario parlamentario del momento que se viva en el Estado correspondiente.

La garantía de nuevos derechos requiere de voluntad política, lo que nos lleva a plantearnos —por desgracia, por encima de cualquier demanda social— si habrá voluntad para un desarrollo legal o, por el contrario, si se alcanzará el necesario consenso para un reconocimiento constitucional —esto último si queremos dotar a los derechos digitales (o a los tradicionales digitalizados) del rango de derechos fundamentales, considerando en este punto que son aquéllos que la comunidad política considera tan importantes como para excluir la posibilidad de que las leyes ordinarias puedan limitar o afectar a su contenido esencial y dotados de una tutela jurisdiccional reforzada—.[23] Hay autores que, aunque no hablan tanto de nuevos derechos, sino de nuevos mecanismos de garantía, consideran necesaria una reforma constitucional en clave digital, no tanto para reconocer nuevos derechos, sino para reconocer una nueva faceta a los ya tradicionales en el entorno digital y asegurar nuevos mecanismos de garantía para los mismos.[24] De esta forma, hay que redefinir o actualizar la interpretación de los «derechos del pasado» para «mantener su protección operativa»,[25] pero para satisfacer las situaciones que van surgiendo se van a requerir las correspondientes reformas normativas, ya sea mediante la aprobación de leyes (aunque no recibiendo la consideración de derechos fundamentales), ya sea a través de su constitucionalización.[26]

No podemos olvidar que todo reconocimiento de derechos implica su garantía efectiva y que esta garantía en este proceso de digitalización impone todo un conjunto de obligaciones a los poderes públicos para que, por un lado, hagan posible el acceso universal a la tecnología e Internet, y, por otro lado, y gracias a ese acceso universal, permitan el desarrollo personal en este entorno digital.[27]

---

[22] Rebollo Delgado, L./Zapatero Martin, P., *Derechos digitales*, UNED/Dykinson, Madrid, 2019, pp. 13-14.

[23] Gutiérrez Gutiérrez, I. (Coord.), *Elementos de Derecho…, op. cit.,* p. 268.

[24] Sobre el procedimiento de reforma constitucional, puede verse, por ejemplo, el artículo de Aláez Corral, B., «Capítulo 27. El procedimiento de reforma constitucional cuarenta años después», en Punset Blanco, R. / Álvarez Álvarez, L. (Coords.), *Cuatro décadas de una constitución normativa (1978-2018). Estudios sobre el desarrollo de la Constitución española*, Civitas / Thomson Reuters, Pamplona, 2019, pp. 639-667.

[25] Fernández Rodríguez, J. J., «Derechos y progreso tecnológico…», *op. cit.*, pp. 263-264.

[26] Fernández Rodríguez, J. J., «Derechos y progreso tecnológico…», *op. cit.*, pp. 267-268; y Rallo Lombarte, A., «Una nueva generación…», *op. cit.*, p. 107.

[27] Rallo Lombarte, A., «Una nueva generación…», *op. cit.*, p. 131.

Así pues, es el legislador el que debe establecer las leyes que permitan que los derechos desplieguen su plena eficacia; o bien, proceder a su constitucionalización. Esto es, el legislador está obligado a adoptar las medidas adecuadas, necesarias y suficientes para proteger los derechos. Así, todos los derechos pueden ampliar su alcance y proyección a través de dicho desarrollo legislativo.[28]Además, en este proceso de demandas sociales y reconocimiento de derechos en un entorno digital, hay que asumir una perspectiva global sobre los derechos porque la tecnología es un fenómeno global. No podemos olvidar el contexto geopolítico en el que nos encontramos y la deriva hacia Asia y el riesgo de que asumiendo sus avances tecnológicos y haciéndonos dependientes de los mismos, acabemos por asumir y adoptar tecnologías desarrolladas sin ningún tipo de respeto hacia los derechos de los ciudadanos.[29]

Pero junto al desarrollo legal, o incluso al margen del mismo, una forma de garantizar los derechos en el proceso de transformación digital es, como se ha dicho, su constitucionalización y así, sus garantías. La solución ya nos la adelantó la LOPDGDD. La misma norma indica en su Preámbulo que los derechos digitales que reconoce en su Título X deberían incluirse en la deseable reforma de nuestro texto constitucional, una reforma que «debería incluir entre sus prioridades la actualización de la Constitución a la era digital y, específicamente, elevar a rango constitucional una nueva generación de derechos digitales».

Si bien las afirmaciones de la LOPDGDD pueden parecer contradictorias (al no reconocer nuevos derechos en su art. 79, pero luego hablar de una nueva generación de derechos), entendemos que más que reconocer nuevos derechos digitales, la esencia debería ser dotar a los derechos tradicionalmente reconocidos en nuestro texto constitucional de una mayor protección y seguridad jurídica adaptándolos al imparable proceso de digitalización y de Internet, «a las nuevas realidades producidas por la ciencia y la tecnología».[30] El proceso sería pues digitalizar nuestro texto constitucional y reorientar los mecanismos de protección de nuestros derechos fundamentales teniendo en cuenta el nuevo entorno digital y sus amenazas.[31]

Y en este proceso de reconocimiento de «nuevos» derechos, sería el momento oportuno para replantearnos la construcción del derecho a una buena Administración como un derecho fundamental vinculándolo a la transformación digital y a los derechos digitales ya reconocidos legalmente o en la Carta de Derechos Digitales. No

---

[28] Gutiérrez Gutiérrez, I. (Coord.), Elementos de Derecho…, *op. cit.*, pp. 285-286.

[29] Martínez Martínez, R., «¿Un año de derechos digitales», en *Eldiario.es*, de 12 de julio de 2022.

[30] Piñar Mañas, J. L., «Identidad y persona en la sociedad digital», en de la Quadra-Salcedeo, T. / Piñar Mañas, J.L. (Dirs.), *Sociedad digital y Derecho*, BOE, Madrid, 2018, p. 105; y Rodotà, S., *La vida y las reglas. Entre el derecho y el no derecho*, Trotta, Madrid, 2010, p. 12.

[31] Cotino Hueso, L., «Nuevo paradigma en…», *op. cit.*, p. 70; y Balaguer Callejón, F., «La Constitución del algoritmo», en Gomes, A. C. y otros (Coords.), *Direito Constitucional: diálogos em homenagem ao 80º aniversário de J. J. Gomes Canotilho*. Belo Horizonte, Fórum, Brasil, 2021. Y, con más detalle, del mismo autor, *La Constitución del algoritmo*, FMGA, Aragón, 2022. Vid., también, Celeste, E., *Digital Constitutionalism. The Role of Internet Bill of Rights*, Routledge, Nueva York, 2023.

obstante, no podemos perder de vista que, como luego recalcaremos, el derecho a una buena Administración ya es un derecho fundamental a nivel europeo.

Así las cosas, a falta de reconocimiento constitucional, y de ausencia de desarrollo legal o reglamentario, hasta que una u otra vía se produzcan, creemos que la solución durante esta transformación digital puede venir por otra vía. Teniendo en cuenta que la mayoría de tecnologías disruptivas «beben» de información personal, de datos personales —o si no identifican directamente, lo pueden (y desean) llegar a hacer para personalizar los servicios ofrecidos—, creemos que la solución ya la tenemos en nuestras manos, sin perjuicio de los matices correspondientes. Entendemos que si lo que hay en juego, en último término, son datos personales, la normativa y criterios o principios generales a aplicar serían los previstos en el terreno de la protección de datos, y más específicamente los previstos en el Reglamentos europeo 2016/679 de Protección de Datos Personales (RGPD).[32]

La solución tendría que venir de reforzar los principios tradicionalmente reconocidos en las normas vigentes en materia de protección de datos personales, al mismo tiempo que juridificar principios éticos, una perspectiva ética, haciéndolos jurídicamente exigibles y situando a la persona en el centro de la transformación digital. En esta línea, más allá de la LOPDGDD y la citada Carta de Derechos Digitales, también a nivel europeo, aunque sin carácter vinculante debemos citar en primer lugar la *Declaración Europea sobre los Derechos y Principios Digitales para la Década Digital*, proclamada conjuntamente el 7 de febrero de 2023, por el Parlamento Europeo, el Consejo y la Comisión.[33] Esta Declaración establece la necesidad de dar prioridad a las personas, situar a la persona en el centro de la transformación digital, debiendo la tecnología proteger los derechos de las personas, esto es, estar al servicio y beneficio de todos los ciudadanos europeos. Y, en segundo lugar y en la misma línea, y con carácter vinculante, la Propuesta de Reglamento sobre Inteligencia Artificial, presentada el 21 de abril de 2021.[34]

Pero más allá de normas claras y precisas —y éticas— y un estricto cumplimiento del test de proporcionalidad, se requiere de forma previa a la puesta en marcha de cualquier nueva invención una evaluación del impacto en la vida de los sujetos atendiendo a valores éticos y no discriminatorios. En esta línea se dirigen los esfuerzos

[32] Más allá de las indispensables bases de legitimación para poder tratar datos personales, previstas en el art. 6 RGPD), el RGPD recoge como principios esenciales para poder tratar los datos personales los siguientes principios relativos al tratamiento (art. 5 RGPD): principio de licitud, lealtad y transparencia; principio de limitación de la finalidad; principio de minimización de datos; principio de exactitud; principio de limitación del plazo de conservación; principio de integridad y confidencialidad; y principio de responsabilidad proactiva.

[33] La *Declaración sobre los Derechos y Principios Digitales* presenta el compromiso de la UE con una transformación digital protegida, segura y sostenible que sitúe a las personas en el centro, en consonancia con los valores fundamentales de la UE y los derechos fundamentales Declaración disponible en https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32023C0123(01)&from=ES.

[34] Disponible en https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A52021PC0206.

europeos y no solo con la propuesta de Reglamento sobre Inteligencia Artificial citado, sino con las conocidas «Directrices éticas para una IA fiable» («Ethics guidelines for trustworthy AI»), del Grupo de Expertos de Alto nivel de la UE para IA, publicadas ya en abril de 2019,[35] y que se centran en tres componentes: que la Inteligencia Artificial sea licita, que sea ética y que sea robusta desde el punto de vista técnico y social. Estas orientaciones pivotan alrededor de la transparencia con las exigencias de facilitar la trazabilidad y la auditabilidad de los sistemas de Inteligencia Artificial, o la promoción y formación y la educación con el fin de conocer una Inteligencia Artificial fiable. Todo ello se puede trasladar a cualquier nuevo desarrollo o avance tecnológico.

Por último, debemos añadir que la labor de garantizar los derechos en el terreno digital no se puede dejar sólo en manos del legislador o de los Tribunales en su labor interpretativa. Debemos dotar de mayores facultades de control y de sanción a las Autoridades de control independientes, ya sea en materia de protección de datos o en materia de Inteligencia artificial, para que nos ayuden en este proceso complejo. Nos referimos, en el caso español, a la Agencia Española de Protección de Datos (AEPD) o sus homólogas autonómicas, o, en su caso, a la futura Agencia Estatal de Supervisión de la Inteligencia Artificial (AESIA), prevista en la *Estrategia Nacional de Inteligencia Artificial* (como uno de los ejes de la citada *Agenda España Digital* 2026),[36] y en los Presupuestos Generales de 2022.

Y, finalmente, sólo queremos dejar aquí apuntado la necesidad de que los poderes públicos limiten el poder de actuación y de intervención en los derechos fundamentales de los llamados gigantes tecnológicos porque la digitalización no se trata de una cuestión que afecte exclusivamente al sector público.[37] La propia naturaleza de la transformación digital ha convertido a los operadores privados en un agente de primer orden en la garantía, o posible lesión, de los derechos fundamentales, con independencia de su tamaño o localización. Asimismo, debemos entender que los derechos no son sólo límites al poder público y que no podemos hablar sólo de las obligaciones positivas de los poderes públicos para garantizar nuestros derechos, sino que ante las amenazas del sector privado, especialmente en este terreno de estas grandes compañías que lo saben todo de nosotros, debemos acabar hablando de una eficacia horizontal (*Drit-*

[35] Disponible en https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai.

[36] Vid. la ya citada *Estrategia Nacional de Inteligencia Artificial (ENIA)*, noviembre de 2020, y su quinto Eje estratégico destinado a «Potenciar el uso de la IA en la administración pública y en las misiones estratégicas nacionales», pp. 56-64.

[37] Al respecto, vid. Novales, A. (Coord.), *La modernización…, op. cit.,* pp. 13-16, quien hace hincapié en el consenso en la colaboración entre sector público y privado y señala que «Definir mecanismos adecuados de colaboración público-privada requiere también tener presente cuál es nuestra estructura empresarial. En las numerosas empresas pequeñas y microempresas españolas que, incluyendo los autónomos sin asalariados, constituyen un 94% de las empresas dadas de alta en la Seguridad Social, la propiedad está muy concentrada y el capital apenas tiene liquidez. Con esta realidad de nuestra estructura empresarial, es claro que la colaboración público-privada no debe limitarse a las empresas grandes, teniendo además en cuenta que muchas iniciativas prometedoras en innovación se llevan a cabo en empresas que nacen con un tamaño lógicamente reducido».

twirkung) entre particulares. Por todo ello, esto implica exigir responsabilidades a los gigantes tecnológicos, por su responsabilidad cívica o ética y democrática, y limitar su actuación frente a posibles riesgos generados por su actuación porque es a través de su tecnología y de las herramientas que generan cómo condicionan el ejercicio de nuestros derechos, requiriéndose, por lo tanto, la intervención política de los Estados y no dejándose nuestros derechos y la estructura de nuestros Estados, en manos de la «buena voluntad» de estos gigantes digitales. Sin detenernos aquí en este tema, más allá de la necesaria colaboración público-privada,[38] dejamos señalado que en esta línea de regular la actuación de los gigantes tecnológicos en el proceso de digitalización de nuestras sociedades y de nuestros derechos en julio de 2022 se aprobó el Reglamento europeo conocido como la Ley de Servicios Digitales (*Digital Services Act*, DSA), que será aplicable a partir del 17 de febrero de 2024.[39]

III. LA DIGITALIZACIÓN DE LA ADMINISTRACIÓN

En los últimos años, como hemos dejado señalado, hemos asistido a importantes cambios: por un lado, en el terreno tecnológico, cambios que permiten un fácil y rápido acceso a la información, su análisis, intercambio, combinación, almacenamiento ilimitado y recuperación con las más variadas finalidades, y las muestras más evidentes nos

[38] Así se recoge, por ejemplo, también en el RDL 36/2020, por el que se aprueban medidas urgentes para la modernización de la Administración Pública y para la ejecución del Plan de Recuperación, Transformación y Resiliencia, arts. 8-11, donde se regulan nuevas formas de colaboración público-privadas, donde señala además en el Apdo. I de su Exposición de Motivos: «La Administración Pública debe responder de modo ágil y eficaz, como sobradamente ha demostrado en otras ocasiones, y sin disminuir sus obligaciones de control, salvaguardando el interés general. Para ello, es preciso acometer un proceso de modernización que le proporcione las herramientas necesarias para acometer la ejecución del Plan y la mejor gestión de fondos, contando con el sector público y el sector privado».

[39] Vázquez Alonso, V. J., «La censura «privada» de las grandes corporaciones digitales y el nuevo sistema de la libertad de expresión», en *Teoría & Derecho. Revista de Pensamiento jurídico*, nº 32, pp. 108-129 (pp. 121-122 y 111 y 114), quien hace referencia a normas como la Sección 230 de la Ley estadounidense de Decencia en las Comunicaciones de 1996 (*Communications Decency Act*), que garantiza la irresponsabilidad de los intermediarios de Internet por lo que compartan a través de sus canales como por lo que decidan eliminar a través de las facultades de moderación que tienen (47 U.S. Code § 230 - *Protection for private blocking and screening of offensive material*); la Directiva 2000/31/CE sobre el Comercio electrónico del año 2000 la que también, de forma ingenua, considera la presunción de inocencia de estas Plataformas, y sólo las hace responsables si tienen conocimiento efectivo de las actividades ilícitas o control de los contenidos publicados o almacenados, además de no exigirles una obligación general de supervisión (arts. 14 y 15); o a las Leyes de Francia y Alemania, que aunque centradas en el ámbito de las libertades de expresión e información y la lucha contra los contenidos de odio en Internet o en las redes sociales, redefinen el régimen de responsabilidad de estas grandes corporaciones digitales en cuanto que prestadoras de servicios de Internet (*Loi núm. 2020-766, du 24 juin 2020, visant à lutter contre les contenus haineux sur Internet*; y *Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz - NetzDG)* vom 1. September 2017 (Netzwerkdurchsetzungsgesetz - NetzDG). Sin embargo, curiosa y polémicamente, en España, la STS 747/2022, de 3 de noviembre, condenó a un usuario de redes sociales por los comentarios vertidos en su perfil por terceros, obviando toda la responsabilidad de la red social.

las están mostrando las herramientas de Inteligencia artificial. Y, por otro lado, se ha producido un cambio en la mentalidad de los ciudadanos, que cada vez son más conscientes del valor de la información pública, pero también de la importancia de su información personal y demandan mayor conocimiento de lo que hacen los poderes públicos, a la vez que también exigen un mayor control respecto de lo que los mismos hacen.

Es obvio que todo este proceso de automatización supondrá una simplificación administrativa, la reducción de trámites innecesarios y, por lo tanto, la reducción de costes; y también conllevará un mayor acceso a la información, mejorando la transparencia administrativa y contribuyendo a un mejor control de la misma, que es la finalidad que se está persiguiendo con todo este proceso.[40] Estos cambios implican que los poderes públicos tienen que cambiar su mentalidad a la hora de trabajar y tratar la información personal. Los procedimientos se van a establecer de forma digitalizada o informatizada, pero antes de esto, el mayor problema será rediseñar los procedimientos existentes y adaptarlos a las nuevas tecnologías, haciéndolos respetuosos con los derechos fundamentales de los ciudadanos a los que van dirigidos.

Se cumple así con el mandato constitucional de eficacia y de servicio al interés general previstos en el artículo 103.1 CE,[41] y desarrollado en el artículo 3 de la Ley 40/2015 de Régimen Jurídico del Sector público,[42] a la vez que se refuerza el principio de responsabilidad de los poderes públicos —reconocido también constitucionalmen-

---

[40] Troncoso Reigada, A., «La Administración electrónica y la protección de datos personales», en *Revista Jurídica de Castilla y León.*, nº 16, 2008, pp. 31-112 (p. 38).

[41] Señala el art. 103.1 CE: «La Administración Pública sirve con objetividad los intereses generales y actúa de acuerdo con los principios de eficacia, jerarquía, descentralización, desconcentración y coordinación, con sometimiento pleno a la ley y al Derecho». Al respecto, vid. Troncoso Reigada, A., «La Administración electrónica…», *op. cit.*, pp. 35-36.

[42] El art. 3 Ley 40/2015 recoge los principios generales que deben regir el funcionamiento y actuación de las Administraciones públicas e indica: «1. Las Administraciones Públicas sirven con objetividad los intereses generales y actúan de acuerdo con los principios de eficacia, jerarquía, descentralización, desconcentración y coordinación, con sometimiento pleno a la Constitución, a la Ley y al Derecho. Deberán respetar en su actuación y relaciones los siguientes principios: a) Servicio efectivo a los ciudadanos. b) Simplicidad, claridad y proximidad a los ciudadanos. c) Participación, objetividad y transparencia de la actuación administrativa. d) Racionalización y agilidad de los procedimientos administrativos y de las actividades materiales de gestión. e) Buena fe, confianza legítima y lealtad institucional. f) Responsabilidad por la gestión pública. g) Planificación y dirección por objetivos y control de la gestión y evaluación de los resultados de las políticas públicas. h) Eficacia en el cumplimiento de los objetivos fijados. i) Economía, suficiencia y adecuación estricta de los medios a los fines institucionales. j) Eficiencia en la asignación y utilización de los recursos públicos. k) Cooperación, colaboración y coordinación entre las Administraciones Públicas. 2. Las Administraciones Públicas se relacionarán entre sí y con sus órganos, organismos públicos y entidades vinculados o dependientes a través de medios electrónicos, que aseguren la interoperabilidad y seguridad de los sistemas y soluciones adoptadas por cada una de ellas, garantizarán la protección de los datos de carácter personal, y facilitarán preferentemente la prestación conjunta de servicios a los interesados. 3. Bajo la dirección del Gobierno de la Nación, de los órganos de gobierno de las Comunidades Autónomas y de los correspondientes de las Entidades Locales, la actuación de la Administración Pública respectiva se desarrolla para alcanzar los objetivos que establecen las leyes y el resto del ordenamiento jurídico. 4. Cada una de las Administraciones Públicas del artículo 2 actúa para el cumplimiento de sus fines con personalidad jurídica única».

te en el art. 9.3 CE como uno de los pilares del Estado de Derecho—,[43] que deben rendir cuentas a los ciudadanos, pues son éstos los que les han legitimado, a través de largas cadenas de legitimación, para ejercer sus funciones.[44]

Pero la modernización de la Administración pública no se deriva sólo de la respuesta a los principios de eficiencia o transparencia de las Administraciones públicas que hemos citado y constitucionalmente consagrados. Podríamos decir que el proceso de modernización de la Administración pública se reflejó por primera vez con la Ley 30/1992 del Régimen jurídico de las Administraciones públicas y del Procedimiento administrativo común, introduciendo (en su art. 45) el uso de medios electrónicos, lo que poco a poco fue desarrollándose y completándose con normas posteriores, especialmente de rango reglamentario o sectoriales, como las relacionadas con el sector y la Administración tributaria. Pero fue con la Ley 11/2007, de Acceso electrónico de los ciudadanos a los Servicios públicos con la que se dio un salto cualitativo en la modernización de la Administración pública, pasando el cambio de ser una mera potestad facultativa en manos de las Administraciones públicas, a ser una verdadera obligación de las mismas.[45]

Así pues, normas como la pionera Ley 11/2007, de Acceso electrónico de los ciudadanos a los Servicios públicos actualmente derogada por la Ley 39/2015, del Procedimiento Administrativo Común de las Administraciones Públicas, la Ley 40/2015 del Régimen jurídico del Sector público, o el Reglamento de actuación y funcionamiento del Sector público por medios electrónicos (aprobado por Real Decreto 203/2021), establecieron los procedimientos para actuar tanto dentro de las Administraciones públicas como en la relación entre ellas y con los ciudadanos y empresas. Asimismo, las normas relativas a los llamados Esquema Nacional de Seguridad (aprobado por Real Decreto 311/2022) y el Esquema Nacional de Interoperabilidad (aprobado por el Real Decreto 4/2010) establecen las medidas de seguridad para hacer dichos procedimientos interoperables y seguros informáticamente.[46]

---

[43] Señala el art. 9.3 CE: «La Constitución garantiza el principio de legalidad, la jerarquía normativa, la publicidad de las normas, la irretroactividad de las disposiciones sancionadoras no favorables o restrictivas de derechos individuales, la seguridad jurídica, la responsabilidad y la interdicción de la arbitrariedad de los poderes públicos».

[44] García García, J., «Gobierno abierto: transparencia, participación y colaboración en las Administraciones Públicas», en *Innovar*, 24 (54), 2014, pp. 75-88 (p. 79).

[45] Vid. Cotino Hueso, L., «El nuevo reglamento de Administración electrónica, que no innova en tiempos de transformación digital», en *Revista Catalana de Dret Públic*, nº 63, 2021, pp. 120-121; con referencia a Gamero Casado, E. (Dir.), *Tratado de procedimiento administrativo común y régimen jurídico básico del sector público*, Tirant lo Blanch, Valencia, 2017. Un excelente análisis de la evolución del proceso de modernización de la Administración pública lo encontramos en Valero Torrijos, J., «De la digitalización a la innovación tecnológica. Valoración jurídica del proceso de modernización de las administraciones públicas españolas en la última década (2004-2014)», en *IDP: Revista de Internet, Derecho y Política*, nº 19, 2014, pp. 117-129.

[46] Sobre las mismas y el proceso de digitalización de las Administraciones públicas, vid. Cerrillo I Martínez, A. (Coord.), *A las puertas de la Administración digital. Una guía detallada para la aplicación de las Leyes 39/2015 y 40/2015*, INAP, Madrid, 2016, pp. 17-22 y 37-60.

En este sentido, que la Administración pública se digitalice y se adapte a la evolución tecnológica de la sociedad a la que presta sus servicios se ha convertido no sólo en una reivindicación legislativa. Aunque para ser sinceros, como ya hemos comentado, esa modernización no es algo nuevo, sino que es un proceso que lleva fraguándose desde los años noventa y que tiene como objetivo esencial acercarse a los ciudadanos, prestándoles mejores servicios, mejorando la calidad de los mismos, y facilitando su participación en los asuntos públicos.[47] Pero es cierto que el uso de las nuevas tecnologías potencia que sea más fácil su consecución.[48] Podríamos decir que una consecuencia de la evolución tecnológica y del desarrollo de la Administración electrónica es el llamado «Gobierno abierto» («*Open Government*»), y que cuando se supera la idea de la Administración electrónica como herramienta que facilita los servicios públicos, se ofrece algo más que un servicio unidireccional hacia el ciudadano: la tecnología pasa a formar parte de la vida diaria y de la propia Administración, y se centra en la idea de la rendición de cuentas y en la participación ciudadana. La verdadera ventaja del uso de las nuevas tecnologías en la Administración será la forma en que dichos instrumentos se empleen y su objetivo y finalidad.[49]

De esta forma se consigue también que la Administración pública cumpla con los principios constitucionales de eficacia y de servicio al interés general previstos en el ya citado artículo 103.1 CE;[50] y, de la misma forma, se consigue que haciendo efectiva la máxima de la transparencia, se cumpla con el principio de responsabilidad de los poderes públicos, rindiendo cuentas a los ciudadanos.[51]

---

[47] Bañon y Martínez, R., «La modernización de la Administración Pública española. Balance y perspectivas», en *Revista Política y Sociedad*, 13 (1993), pp. 9-20, quien recuerda que ya en 1992 el Gobierno anunció la aplicación de 204 medidas de modernización administrativa, consecuencia del Plan de modernización para la Administración del Estado, publicado oficialmente en 1990 (p. 9). Asimismo, Novales nos recuerda que «Posteriormente, en 1997, el Gobierno formado tras las elecciones de marzo de 1996, puso en marcha una nueva comisión de reforma de la Administración, cuyos trabajos tampoco fructificaron. En el año 2013 se constituyó la Comisión para la Reforma de la Administración pública, que elaboró un completo informe con más de 200 medidas para la modernización y reforma de las AA.PP. (CORA, 2013). Algunas de estas medidas se llevaron a cabo y se realizaron informes trimestrales para evaluar su ejecución. No obstante, el último informe data del segundo trimestre de 2016 y muchas de las medidas quedaron pendientes» (Novales, A. (Coord.), *La modernización…, op. cit.,* pp. 2-3). Vid., también, Gómez Manresa, M. F., «Innovación tecnológica y jurisdicción contencioso-administrativa», en *Revista Española de Derecho Administrativo*, nº 205, 2020, pp. 97-124.

[48] Gutiérrez David, E., «Derecho de acceso a la información pública», en *Eunomía*, nº 6, 2014, pp. 190-193.

[49] García García, J. (2014). «Gobierno abierto…», *op. cit.*, p. 78.

[50] Vid. Troncoso Reigada, A., «La Administración electrónica…», *op. cit.*, pp. 35-36, quien se refiere a las Cartas de Servicios de las Administraciones Públicas como un ejemplo de la voluntad por mejorar los servicios ofrecidos a los ciudadanos. En detalle, vid. Troncoso Reigada, A., «Las Cartas de Servicio: un compromiso con el ciudadano», en *Jornadas sobre La mejora de la calidad de los servicios públicos en la Administración de la Comunidad Autónoma de La Rioja celebradas el 17 de abril de 2002*, Gobierno de La Rioja, La Rioja, 2004, pp. 109-116.

[51] García García, J. (2014). «Gobierno abierto…», *op. cit.*, p. 79.

Así, por ejemplo, la utilización de las nuevas tecnologías permite mejorar la participación de los ciudadanos a la hora de diseñar y gestionar los servicios públicos.[52] Si los ciudadanos se sienten bien informados y «escuchados», el nivel de participación y compromiso con la institución será mayor. Los servicios se tienen que diseñar no sólo conforme a las expectativas de los ciudadanos sino también con su colaboración, para que se impliquen y con la idea de que cualquier institución pública lo único que hace es gestionar, hacer de intermediaria «*exigiendo retornos de lo público a lo público*».[53]

La Administración debe saber qué servicios son los más valorados por los ciudadanos, así como los que más demandan o necesitan con el fin de poder organizarlos y ofrecérselos. Y la mejor herramienta en la actualidad para esta interacción la proporciona Internet. A través de los servicios que ofrece la Red los ciudadanos pueden mandar sus opiniones y hacer sus reclamaciones y, en consecuencia, la Administración podrá desarrollar y diseñar los servicios mejorando su calidad.[54]

La confianza en los servicios públicos recibidos, la implicación en los mismos a través de las vías de participación facilitadas por las nuevas tecnologías y la existencia de mecanismos de rendición de cuentas son los elementos indispensables para un correcto funcionamiento democrático de la gestión pública.[55] De esta forma, y sólo de esta forma, se reforzará el principio democrático: «*el saber implicaría ya una incitación psicológica a participar*».[56] Más aún, la calidad democrática de nuestra sociedad se medirá por la implicación de sus ciudadanos en la misma porque lo importante no es tanto el poder ejercido sino en cómo se ejerce.[57]

En consecuencia, el concepto de modernización vigente incluye tres planos conectados pero independientes: la flexibilización organizativa y la agilización de las relaciones con los ciudadanos/clientes; la redefinición de la distribución territorial del poder, tanto en el plano nacional como en el espacio europeo; y la adaptación a las directrices y acuerdos comunitarios. Precisamente en esta complejidad de objetivos radica la importancia que se concede en este momento a la modernización administrativa. En

---

[52] Cotino Hueso, L., «La regulación de la participación y de la transparencia a través de Internet y medios electrónicos. propuestas concretas», en *P3T, Journal of public policies and territories. Participation, citizen control, governance*, nº 2, 2012, p. 29, quien además critica la falta de normas que se centren en regular la participación (pp. 29-31); y con cita de Tur Ausina, R., «Participación ciudadana. Oportunidad, necesidad y esencia de su regulación legal», en *Deliberación. Revista para la mejora de la calidad democrática*, nº 1, 2010.

[53] Sánchez González, M. y otros, «Innovación y Open Government como claves para una Universidad abierta y participativa. Estrategias y resultados en la UNIA», en *Telos*, 2014, pp. 2.

[54] Troncoso Reigada, A., «La Administración electrónica…», *op. cit.*, p. 39.

[55] García García, J. (2014). «Gobierno abierto…», *op. cit.*, p. 76.

[56] Silva García, F., «El derecho a la información pública en la jurisprudencia constitucional: ¿un derecho fundamental incómodo?», en *Cuestiones constitucionales. Revista Mexicana de Derecho Constitucional*, nº 24, 2011, p. 285.

[57] Sobre esta idea, vid. Cabo, D. / Magallón, R., «Nuevos retos para las Administraciones Públicas. Datos, cultura cuantitativa y calidad democrática», en *Telos*, 2013, pp. 1-2.

efecto, la modernización administrativa es un aspecto subordinado de la modernización de la sociedad española.[58]

Por ello, si bien debe quedar claro que la infraestructura tecnológica, la digitalización de la Administración debe mejorar, este proceso debe ir de la mano de un cambio cultural y organizativo, pero no sólo respecto de los ciudadanos, sino de los funcionarios públicos y de los propios gobernantes, facilitándose la prestación de servicios y sus procesos, así como el acceso a los mismos, contribuyendo a una mejor transparencia de la gestión pública. Las mejoras deben englobar todo el proceso de vida de tratamiento de la información, desde su recogida, pasando por su procesamiento y tratamiento, hasta su conservación o destrucción. Y ello va a requerir no sólo de una ciudadanía preparada, sino de personal que tenga las competencias adecuadas.

No podemos quedarnos sólo en la tramitación y notificación electrónica de los procedimientos, previstos en las normas anteriormente citadas. Hay que aprovechar las ventajas que ofrecen herramientas como la Inteligencia Artificial, el Blockchain o el BigData para aprovechar los avances tecnológicos e innovar en los procedimientos administrativos, poniendo la Administración al servicio de los ciudadanos. Queda mucho por hacer y hay que hacerlo bien desde el principio, sentando las bases de lo que queda por venir.[59] No podemos obviar el hecho de que «la modernización de los procesos del sector público tiene un elevado poder tractor sobre el conjunto de la economía y de la sociedad».[60]

Por todo ello, la digitalización de la Administración pública española es urgente, adaptándose a los cambios que ha sufrido la sociedad española en estos últimos tiempos. El ya citado Plan de Recuperación, en el marco de la Agenda España Digital 2026, prevé un presupuesto de más de cuatro mil millones de euros destinados a adaptar la Administración pública a los retos de la sociedad contemporánea, impulsando los servicios públicos digitales que se prestan a ciudadanos y a empresas, mejorando la eficiencia interna de las Administraciones públicas, con procedimientos automatizados, simplificando trámites, trabajando en un modelo de identidad digital y empleando herramientas de inteligencia artificial que ayuden a reducir tiempos y costes.

Esto es, la idea de Administración electrónica se ha superado (en teoría) y estamos en un proceso de modernización e innovación. Así, mientras que la Administración electrónica consiste básicamente en una herramienta para hacer más cómodo y rápido el servicio prestado, una vez superado ese inicial momento, y haciéndonos conscientes de las posibilidades que las nuevas tecnologías nos ofrecen, el objetivo no será sólo ofrecer un servicio público de más calidad, sino ofrecer más información a los ciudadanos para que éstos puedan ejercer un mayor y mejor control de los poderes públicos y puedan

[58] Bañon y Martínez, R., «La modernización…», *op. cit.*, 13 (1993), p. 10.
[59] Novales, A. (Coord.), *La modernización…, op. cit.*, pp. 9-11.
[60] Vid. *Estrategia Nacional de Inteligencia Artificial (ENIA)*, p. 57.

participan con mayor conciencia en los asuntos públicos;[61] y, más aún, el objetivo debería ser innovar en este proceso de transición, aprovechando los beneficios que herramientas como la Inteligencia Artificial pueden ofrecer al sector público.[62] Si esto lo unimos al hecho de que su actuación debe ser siempre desde el respeto de los derechos fundamentales, podemos concluir que la modernización o digitalización de la Administración pública no debería concebirse como una concesión que hacen los Estados, sino como una obligación de los poderes públicos para con la sociedad a la que deben servir.

En conclusión, podemos decir que si la dinámica inevitable a la que está abocada la Administración pública es ser una Administración digital y más transparente —en democracia no podría ser de otra forma— y, por lo tanto, más abierta a los ciudadanos a los que sirve, éstos deben tener una serie de derechos reconocidos a la hora de relacionarse con la misma.

IV. LA BUENA ADMINISTRACIÓN DIGITAL Y LOS DERECHOS DIGITALES

El proceso de digitalización y modernización de la Administración pública, como hemos visto, surge con la finalidad de ofrecer un servicio más eficiente y eficaz a los ciudadanos, acercar la Administración a los ciudadanos con el fin de aumentar, en último término, la calidad democrática de nuestros Estados. De esta forma los avances tecnológicos se convierten en un elemento indispensable para hablar de una buena Administración.[63] De la misma forma que afirmamos que ha-

---

[61] Para esta cuestión vid., también, Ley 37/2007, sobre Reutilización de la Información del Sector Público (modificada por la Ley 18/2015), que en su art. 3 define la reutilización de la información como: «*el uso de documentos que obran en poder de las Administraciones y organismos del sector público, por personas físicas o jurídicas, con fines comerciales o no comerciales, siempre que dicho uso no constituya una actividad administrativa pública. Queda excluido de este concepto el intercambio de documentos entre Administraciones y organismos del sector público en el ejercicio de las funciones públicas que tengan atribuidas*».

[62] Esta necesidad, y beneficio, se ha visto tanto a nivel internacional como europeo. Así, por ejemplo, podemos citar en el marco de la OCDE: Berryhill, J. / Kok Heang, K. / Clogher, R. / McBride, K., *Hola, mundo: la Inteligencia Artificial y su uso en el sector público*, Documentos de trabajo de la OCDE sobre Gobernanza pública, nº 36, OCDE, 2019 (ed. en español 2020) (Disponible en https://www.oecd.org/gov/innovative-government/working-paper-hello-world-artificial-intelligence-and-its-use-in-the-public-sector.htm), donde se reconoce el potencial de la IA «como una herramienta para incrementar la productividad del servicio público, servir mejor a sus ciudadanos y potenciar la innovación en sus empresas» (p. 3). Y en el marco de la Unión Europea: Misuraca, G / Van Noordt, C, *AI Watch, Artificial Intelligence in public services. Overview of the use and impact of AI in public services in the EU*, Oficina de publicaciones de la Unión Europea, Luxemburgo, 2020 (Disponible en https://op.europa.eu/es/publication-detail/-/publication/4c72dd88-bcda-11ea-811c-01aa75ed71a1).

[63] Con esta afirmación, vid. STSJ de Castilla y León 126/2019, de 6 de febrero de 2019 (Rec. 486/2018). Y, en el mismo sentido, Martínez Soria, J., «Gobierno electrónico en Alemania y en Europa», en Cotino Hueso, L., *Democracia, participación y voto a través de las nuevas tecnologías*, Colección Sociedad de la Información 13, Comares, Granada, pp. 245-262 (en concreto, p. 250).

blar de buena Administración es hablar de una Administración transparente, hablar de una buena Administración pasa por hablar en nuestros días de una Administración digitalizada.

Y es en el contexto de esa Administración digitalizada donde debemos establecer los derechos digitales que los ciudadanos tienen a la hora de relacionarse con la misma.

La Carta de Derechos Digitales se estructura en seis grandes bloques. A saber: Libertad, Igualdad, Participación y conformación del espacio público, Entorno laboral y empresarial, Entornos específicos (como, por ejemplo, los derechos ante la IA o el empleo de la neurotecnologías) y, por último, el bloque relativo a las Garantías y eficacia de la Carta. Para el caso que aquí nos interesa, nos centraremos en el Bloque relativo a los Derechos de participación y conformación del espacio público (Apdos. XIII a XVIII).

El contenido de la Carta de Derechos Digitales se proyecta en el conjunto de la sociedad, pero también de la gestión pública, siendo necesario que las distintas Administraciones públicas interioricen su contenido y ajusten su actuación y funcionamiento a sus previsiones, garantizando la protección y ejercicio de los derechos de las personas también en un entorno digital. Y es aquí, como hemos dicho, donde cobra sentido la exigencia de la garantía del derecho a una buena Administración. No podemos olvidar que esta exigencia va a ser el fundamento de la regulación de los derechos digitales de los ciudadanos en este terreno.

Partimos del derecho a una buena Administración como derecho fundamental a nivel europeo reconocido en la CDFUE, en su art. 41, que señala:

> «1. *Toda persona tiene derecho a que las instituciones, órganos y organismos de la Unión traten sus asuntos imparcial y equitativamente y dentro de un plazo razonable.*
>
> 2. *Este derecho incluye en particular: a) el derecho de toda persona a ser oída antes de que se tome en contra suya una medida individual que la afecte desfavorablemente; b) el derecho de toda persona a acceder al expediente que le concierna, dentro del respeto de los intereses legítimos de la confidencialidad y del secreto profesional y comercial; c) la obligación que incumbe a la Administración de motivar sus decisiones.*
>
> 3. *Toda persona tiene derecho a la reparación por la Unión de los daños causados por sus instituciones o sus agentes en el ejercicio de sus funciones, de conformidad con los principios generales comunes a los Derechos de los Estados miembros.*
>
> 4. *Toda persona podrá dirigirse a las instituciones de la Unión en una de las lenguas de los Tratados y deberá recibir una contestación en esa misma lengua»*

Este derecho fundamental europeo, exigible frente a las instituciones, órganos y organismos de la Unión Europea, no se reconoce a nivel nacional de forma expresa como derecho fundamental, derivándose su exigencia de dar cumplimiento al principio constitucional de eficacia del art. 103.1 CE, entendiéndose que una buena Administración es aquélla que cumple con los principios aquí reconocidos. En este sentido,

como nos recuerdan desde el Consejo de Europa, «*la buena Administración depende de la calidad de la organización y gestión que debe cumplir con requisitos de eficacia, eficiencia y relevancia a las necesidades de la sociedad*».[64] Señala el art. 103.1 CE:

> «1. *La Administración Pública sirve con objetividad los intereses generales y actúa de acuerdo con los principios de eficacia, jerarquía, descentralización, desconcentración y coordinación, con sometimiento pleno a la ley y al Derecho*»

Hoy día a través del reconocimiento de la buena Administración se persigue dar una respuesta adecuada a las necesidades de la ciudadanía ante los nuevos retos a los que deben hacer frente las Administraciones públicas. Está ampliamente aceptado que, gracias al uso de los medios electrónicos, las Administraciones públicas son más eficaces y eficientes, más abiertas y transparentes, más cercanas a los ciudadanos y facilitan la comunicación y la participación de éstos en la Administración pública. De este modo, los medios electrónicos constituyen un instrumento idóneo para lograr un buena Administración.

Lograr una buena Administración no se trata simplemente de utilizar ordenadores para facilitar la eficacia y eficiencia de la actividad administrativa, sino, por el contrario, de la posibilidad de implantar sistemas automatizados con una gran capacidad de procesamiento que puede llegar a adoptar decisiones que afectan a sujetos concretos, lo que obliga a diseñar procedimientos, a regularlos y a redefinir las garantías jurídicas.

La cuestión es que en este proceso de transformación digital, en las relaciones que los ciudadanos tengan con la Administración, no sean éstos los que se vean perjudicados con el cambio ni vean disminuidas las garantías jurídicas de las que hasta ahora venían disfrutando. Las garantías que tradicionalmente se han venido consagrando por el Derecho Administrativo se deben adaptar al cambio digital que vivimos y que viven nuestras Administraciones, buscándose una compatibilidad, no sólo con el fin de facilitar el ejercicio de derechos, sino el cumplimiento de obligaciones.[65] Y para ello, en esta transición, se hace necesario en este proceso la aplicación de un principio de «*favor civis*», donde el ciudadano no puede salir perjudicado con el cambio.[66]

---

[64] Vid. Recomendación del Consejo de Europa sobre la Buena Administración, de 20 de junio de 2007 (CM/Rec(2007)7). Disponible en https://rm.coe.int/16807096b9.

[65] Valero Torrijos, J., «Administración pública, ciudadanos y nuevas tecnologías», en Wagner, S. (Coord.), *El Derecho Administrativo en el umbral del siglo XXI: Homenaje al Profesor Dr. D. Ramón Martín Mateo*, Tirant lo Blanch, Valencia, 2000, pp. 2943-2968 (p. 2955); con referencia, entre otros, a Torres López, M.ªA., «El documento electrónico en las relaciones jurídico-administrativas: especial referencia a los actos de comunicación», en *Revista Vasca de Administración Pública*, n.º 55, 1999, pp. 273 y 255-256, respectivamente, quien insiste en el choque entre inseguridad y eficacia, a lo que deberían dirigirse todos los esfuerzos legislativos; y Chico de la Cámara, P., «Notificaciones electrónicas y principios constitucionales», en Bosch Cholbi, J. L. (Coord.), *Comentarios a la Ley general tributaria al hilo de su reforma*, Wolters Kluwer, Madrid, 2016, pp. 183-196.

[66] En este sentido, con esta exigencia durante este proceso de modernización de la Administración pública, especialmente en lo relacionado con las notificaciones electrónicas, vid. Cotino Hueso, L., «La

El problema llegados a este punto es que si bien la citada, y derogada, Ley 11/2007 de Acceso electrónico de los ciudadanos a los Servicios públicos sí que reconocía derechos a los ciudadanos en este proceso de modernización, innovando y configurando así un verdadero «estatuto del ciudadano administrado electrónicamente», las normas aprobadas posteriormente destinadas a regular esa modernización —las citadas Leyes 39 y 40/2015 o el RD 203/2021—, no parecen seguir esta dinámica y «tienen escasa creatividad e innovación al respecto de los derechos» que reconocen, algo completamente criticable.[67]

De ahí la necesidad de analizar si podemos retomar ese estatus del administrado electrónicamente de la actual Carta de Derechos Digitales, que si bien no tiene carácter vinculante, sí un importante valor interpretativo. Se hace imprescindible, por lo tanto, analizar cuáles son los derechos digitales que la Carta de Derechos Digitales reconoce a los ciudadanos en sus relaciones con las Administración públicas, para ver si ésta es la línea a seguir en futuras propuestas legislativas o, incluso, constitucionales para consagrar así el derecho fundamental a una buena Administración.

IV.1. Las obligaciones de las Administraciones públicas en los entornos digitales

Por todo lo visto hasta ahora, se hace indispensable analizar los derechos digitales de la ciudadanía en sus relaciones con las Administraciones Públicas como la esencia del derecho a una buena Administración en el entorno digital, especialmente cuando la tendencia es a un uso o contacto exclusivo con las mismas a través de medios electrónicos o digitales, con los peligros de exclusión que esto puede implicar para una gran parte de la población, la falta de garantías actualmente existente,[68] y con el peligro

preocupante falta de garantías constitucionales y administrativas en las notificaciones electrónica», en *Revista General de Derecho Administrativo*, nº 57, mayo 2021, haciendo referencia a la citada STSJ de Castilla y León 126/2019, de 6 de febrero de 2019 (Rec. 486/2018).

[67] Vid. Cotino Hueso, L., «La preocupante falta…», *op. cit.*, con referencia a Valero Torrijos, J., «La reforma de la Administración electrónica, ¿una oportunidad perdida?», en *Revista Española de Derecho Administrativo*, nº 172, 2015, pp. 13-24. Y destacando esa falta de «un sistema integral de relaciones entre Administración y ciudadanía que aglutine una visión holística del problema incorporando sistemáticamente tanto la perspectiva presencial como la digital en tales relaciones, al efecto de situar al ciudadano en el frontispicio de la actividad esencial de la Administración y codificar adecuadamente sus derechos en ese modelo relacional dual físico/virtual que ya está inserto en las formas de actuar de las administraciones públicas sin aparente vuelta atrás», vid. Ararteko, *Administración digital y relaciones con la ciudadanía. Su aplicación a las administraciones públicas vascas*, Ararteko, País Vasco, octubre 2021, p. 43. Sobre los «subderechos» que deberían integrar este derecho a una buena Administración, vid. Tomás Mallén, B., *El derecho fundamental… op. cit.,* pp. 110-149.

[68] Vid. Cotino Hueso, L. «La obligación de relacionarse electrónicamente con la Administración y sus escasas garantías», en *IDP. Revista de Internet, Derecho y Política*, nº 26, 2018, pp. 7-8, quien se refiere a la discrecionalidad de la Administración para establecer la relación electrónica y los requisitos materiales.

de perder de vista el verdadero objetivo de digitalizar a las Administraciones y quiénes son sus destinatarios.

De hecho, el Tribunal Europeo de Derechos Humanos (TEDH) en su Sentencia de 16 de febrero de 2021, asunto *Stichting Landgoed Steenbergen y otros contra Holanda*,[69] lo ha puesto de manifiesto al analizar el uso exclusivo y excluyente de medios electrónicos a la hora de relacionarse con la Administración pública, concluyendo que, en todo caso, debe buscarse siempre el necesario y justo equilibrio.[70] En este caso el TEDH concluyó que no se había lesionado el derecho de los demandantes porque si bien el TEDH consideró que la Administración pública holandesa podía exigir una tramitación exclusivamente electrónica, lo puso en conexión con el hecho de que los demandante no eran analfabetos digitales,[71] hecho que, por ejemplo, en el asunto *Zavodnik contra Eslovenia* propició que el TEDH concluyera la lesión del derecho de los demandantes al considerar desproporcionada la decisión de la Administración eslovena de un procedimiento exclusivamente digital dada la edad y la falta de accesibilidad electrónica de los demandantes.[72]

Así lo reconoció también nuestro Tribunal Supremo en su Sentencia de 6 de mayo de 2021, donde el Tribunal Supremo matiza que la exigencia y obligatoriedad de una relación exclusivamente electrónica debe recogerse en una norma con rango de ley, no siendo suficiente cualquier tipo de Reglamento.[73] O la STS de 31 de mayo de 2021, donde ante la falta de firma digital para la presentación telemática en un procedimien-

---

[69] STEDH de 16 de febrero de 2021, asunto *Stichting Landgoed Steenbergen y otros contra Holanda*, §§ 47 y 50, que señalan, respectivamente: «§ 47. Si bien no le corresponde al Tribunal determinar la forma en que deben publicarse las notificaciones del tipo de que se trata, de los principios antes mencionados se desprende que cuando se interpone un recurso contra una decisión de una autoridad administrativa que puede ser perjudicial de terceros directamente afectados, es necesario que exista un sistema que permita a esas partes tomar conocimiento de dicha decisión en el momento oportuno. Esto requiere que la decisión, o la información relevante al respecto, esté disponible de una manera predeterminada y publicitada que sea fácilmente accesible para todos los terceros potencialmente afectados directamente. Siempre que existan suficientes salvaguardias para lograr dicha accesibilidad, en principio entra dentro del margen de apreciación del Estado optar por un sistema de publicación únicamente por medios electrónicos (*…)*»; y «§ 50. El Tribunal acepta la afirmación del Gobierno de que la comunicación electrónica entre las autoridades administrativas y los ciudadanos puede contribuir al objetivo de una administración más accesible y que funcione mejor (véase el párrafo 38 supra). Debe comprobar si, dados los hechos del caso, se logró un justo equilibrio entre, por un lado, el interés de la comunidad en su conjunto por tener una administración más moderna y eficiente y, por otro lado, los intereses de los solicitantes»**.**

[70] Analizando dichas Sentencias, vid. Castillo Blanco, F. A., «¿Disminuyen los derechos de la ciudadanía en la era digital? A propósito de la subsanación en el procedimiento administrativo», en *Sociedad Digital*, de 14 de junio de 2021, donde el autor señala que: «Las consecuencias para los obligados a relacionarse electrónicamente con las Administraciones públicas, como ya dejamos apuntado, no son menores y, en este caso, a salvo de que la jurisprudencia del Tribunal Supremo diga otra cosa, o el legislador lo remedie que no parece que vayan por ahí los tiros, resulta evidente que se produce un retroceso en los derechos de los ciudadanos en su relación con la Administración».

[71] STEDH de 16 de febrero de 2021, asunto *Stichting Landgoed Steenbergen y otros contra Holanda*, § 52.

[72] STEDH de 21 de mayo de 2015, asunto *Zavodnik contra Eslovenia*.

[73] STS 1587/2021, de 6 de mayo (Rec. 150/2020), FJ 7º.

to selectivo y su exclusión del mismo, el Tribunal Supremo concluyó que la Administración debería haber dado la posibilidad de subsanar dicho trámite y no escudarse en lo técnicamente posible y en el programa informático.[74]

Pero veamos qué es lo que establecen las normas actualmente vigentes sobre las obligaciones de las Administraciones públicas en los entornos digitales, por poco innovadoras que las mismas sean. Así, dejando de lado lo previsto en su día en la Ley 30/1992, de Régimen Jurídico de las Administraciones públicas y del Procedimiento administrativo común, sobre la incorporación de la tecnología en la actuación de las Administraciones Públicas,[75] o en la «transgresora» Ley 11/2007 de Acceso electrónico a los Servicios públicos,[76] nos centraremos en las vigentes Leyes 39 y 40/2015, así como en el más reciente Reglamento de actuación y funcionamiento del Sector público por medios electrónicos (RD 203/2021). No nos detendremos en las mismas, pues no son las previsiones contenidas en las mismas el objeto de nuestro estudio,[77] pero sí que haremos mención a las obligaciones que las mismas reconocen, así como a las deficiencias de las mismas.

La Ley 39/2015 recoge, básicamente, en sus arts. 12 a 14 los derechos de los ciudadanos a la relación electrónica con la Administración y la correspondiente asistencia en dicho proceso, lo que se completa con el art. 43 relativo a las notificaciones electrónicas; y con el art. 53 en relación con las garantías de los interesados en el procedimiento administrativo, o con el art. 98 en relación con los medios electrónicos de pago cuando se establecen como forma de finalización de los procedimientos.[78]

---

[74] STS 762/2021, de 31 de mayo (Rec. 6119/2019), FJ 6º.

[75] En el art. 45 de la Ley 30/1992 se establecía la validez de los documentos electrónicos y el impulso al empleo y aplicación de las técnicas y medios electrónicos, informáticos y telemáticos, por parte de la Administración al regular la incorporación de los medios técnicos. Asimismo, y también de forma facultativa para las Administraciones en función de su capacidad técnica, en los arts. 38 y 59 (especialmente tras la reforma operada por la Ley 24/2011) se regulaba, respectivamente, la informatización de registros y archivos, y la notificación por medios telemáticos, pero aquí siempre que el interesado lo hubiera señalado como medio preferente o consentido expresamente.

[76] La Ley 11/2007 da el paso de la apuesta voluntaria por la modernización en manos de los Administraciones, al establecimiento de una obligación de las mismas. Es la propia Ley la que, en su Exposición de Motivos, reconoce la obligación de la Administración pública de transformarse en una Administración electrónica regida por el principio de eficacia: «Esa es una de las grandes novedades de la Ley: pasar de la declaración de impulso de los medios electrónicos e informáticos —que se concretan en la práctica en la simple posibilidad de que algunas Administraciones, o algunos de sus órganos, permitan las comunicaciones por medios electrónicos— a que estén obligadas a hacerlo porque la Ley reconoce el derecho de los ciudadanos a establecer relaciones electrónicas».

[77] Para una mayor profundización sobre el tema, recomendamos la lectura de las Notas técnicas elaboradas por el Observatorio de Administración Electrónica (OBSAE) sobre aspectos concretos del desarrollo de la Administración electrónica. Disponibles en https://administracionelectronica.gob.es/pae_Home/pae_OBSAE/pae_NotasTecnicas.html.

[78] El art. 12 Ley 39/2015 se refiere a la «Asistencia en el uso de medios electrónicos a los interesados»; el art. 13 Ley 39/2015 a los «Derechos de las personas en sus relaciones con las Administraciones Públicas», cuyo apartado 13.b) reitera el derecho a la citada asistencia en el uso de medios electrónicos en sus relaciones con las Administraciones, aunque referido a todos los ciudadanos; el art. 14 Ley 39/2015 regula el «Derecho y obligación de relacionarse electrónicamente con las Administraciones Públicas»; el art. 43 Ley

Por su parte, la Ley 40/2015 recoge principios de actuación de las Administraciones públicas, pero hace poco hincapié en los necesarios para el ámbito electrónico, y se refiere al funcionamiento electrónico del sector público en sus arts. 38 a 46 bis, regulando cuestiones como las sedes electrónicas, los portales de Internet, o los sistemas de identificación de las Administraciones públicas; o se refiere a las relaciones electrónicas interadministrativas en los arts. 155 a 158.[79]

Finalmente el RD 203/2021 retoma y hace hincapié en algunos de los principios olvidados en las anteriores normas, como los de neutralidad, accesibilidad o interoperabilidad.[80] Asimismo, como ya hicieran los arts. 12 y 14 Ley 39/2015, se refiere al derecho y obligación de relacionarse electrónicamente con las Administraciones públicas en su art. 3, y a canales de asistencia para el acceso a los servicios electrónicos en su art. 4. No obstante, esta norma, como ya se ha dicho «no mejora los problemas de la obligatoriedad de la relación electrónica», manteniéndose los problemas de indefensión en los casos de las notificaciones electrónicas y los desajustes ante los avances tecnológicos que van dejando obsoleta la norma ante el uso de la automatización y de herramientas como la Inteligencia Artificial en los procedimientos administrativos.[81] Además, esta norma, como también se ha puesto de manifiesto por la doctrina, no atiende a los problemas de brecha digital que la modernización de la Administración puede producir en la ciudadanía, siendo una norma que se ocupa básicamente de modernizar la Administración sin tener en cuenta cómo este proceso afectará a la ciudadanía a la que, en principio, debería servir.[82] Se ha perdido, como también ha mantenido la doctrina más reputada que ha escrito sobre la materia, una gran oportunidad de adaptar a la imparable realidad de la transformación digital las Administraciones públicas y, sobre todo, de situar en el centro de dichas relaciones a los ciudadanos con las garantías adecuadas.[83]

En términos generales, lo que sucede con estas normas es que la falta de concreción de las mismas,[84] y el no situar al ciudadano en el centro de la regulación, deja

39/2015 regula la «Práctica de las notificaciones a través de medios electrónicos»; y la Disp. Transit. Segunda Ley 39/2015 se refiere al régimen transitorio del «Registro electrónico y archivo electrónico único».

[79] Asimismo, el art. 3.2 Ley 40/2015 recupera, como ha quedado dicho alguno de los principios necesarios para el funcionamiento electrónico de la Administración y señala: «2. Las Administraciones Públicas se relacionarán entre sí y con sus órganos, organismos públicos y entidades vinculados o dependientes a través de medios electrónicos, que aseguren la interoperabilidad y seguridad de los sistemas y soluciones adoptadas por cada una de ellas, garantizarán la protección de los datos de carácter personal, y facilitarán preferentemente la prestación conjunta de servicios a los interesados». Más allá de este artículo y los ya citados, la Disposición adicional 17ª Ley 40/2015 se refiere al «Registro electrónico estatal de los órganos e instrumentos de cooperación».

[80] Art. 2 RD 203/2021.

[81] Cotino Hueso, L., «El nuevo reglamento…», *op. cit.*, pp. 118-136.

[82] Cotino Hueso, L., «El nuevo reglamento…», *op. cit.*, p. 124, con referencia a Jiménez Asensio, R., «Administración y ciudadanía en el reglamento de actuación del sector público por medios electrónicos», en el *Blog La Mirada Institucional*, de 25 de abril de 2021.

[83] Cotino Hueso, L., «El nuevo reglamento…», *op. cit.*, p. 131.

[84] A pesar de que la STC 55/2018 indica que «la Ley 39/2015 constituye uno de «los pilares sobre los que se asentará el Derecho administrativo español'» (FJ 2º), y que pretende conseguir «una Adminis-

a la ciudadanía en una clara situación de inseguridad, siendo esto uno de los principales problemas de las relaciones de la ciudadanía con la Administración. Gran parte de los ciudadanos se sienten frustrados, no se sienten seguros en las relaciones electrónicas con la Administración pública, no confían en realizar bien los trámites, que se cierren los procedimientos de forma adecuada y, menos, el poder reclamar ante la Administración cuando exista un fallo técnico. Esto provoca que la ciudadanía se aleje de la Administración.

Por ello, las relaciones electrónicas deben estar marcadas por una exigencia de seguridad, situando al ciudadano en el centro de la modernización del servicio, tal y como en su día estableció y señaló la Ley 11/2007.[85] Se han propuesto medidas como la exigencia a la Administración de servicios al estilo de «botón antipánico» de asistencia al ciudadano,[86] o de medidas innovadoras como la introducción en el modelo administrativo de medidas ya previstas en la normativa de protección de datos como la privacidad desde el diseño y por defecto.[87]

---

tración sin papel basada en un funcionamiento íntegramente electrónico» (FJ 11º.b)), creemos que las normas vigentes no son tan detalladas como se requiere, obviando muchos aspectos necesarios para ofrecer las garantías suficientes a los ciudadanos en esta transición digital en su relación con las Administraciones públicas. Si bien somos conscientes de que en un mundo en continuo cambio y de cambio tecnológico es incoherente hablar de descender al detalle, creemos que los requisitos mínimos que permitan la adaptación al cambio, como podría ser lo relacionado con herramientas de Inteligencia Artificial, tampoco se ha contemplado.

[85] Señalaba la Exposición de Motivos de la Ley 11/2007: «Una Administración a la altura de los tiempos en que actúa tiene que acompañar y promover en beneficio de los ciudadanos el uso de las comunicaciones electrónicas. Estos han de ser los primeros y principales beneficiarios del salto, impensable hace sólo unas décadas, que se ha producido en el campo de la tecnología de la información y las comunicaciones electrónicas. Al servicio, pues, del ciudadano la Administración queda obligada a transformarse en una administración electrónica regida por el principio de eficacia que proclama el artículo 103 de nuestra Constitución. Es en ese contexto en el que las Administraciones deben comprometerse con su época y ofrecer a sus ciudadanos las ventajas y posibilidades que la sociedad de la información tiene, asumiendo su responsabilidad de contribuir a hacer realidad la sociedad de la información. Los técnicos y los científicos han puesto en pie los instrumentos de esta sociedad, pero su generalización depende, en buena medida, del impulso que reciba de las Administraciones Públicas. Depende de la confianza y seguridad que genere en los ciudadanos y depende también de los servicios que ofrezca. El mejor servicio al ciudadano constituye la razón de la reformas que tras la aprobación de la Constitución se han ido realizando en España para configurar una Administración moderna que haga del principio de eficacia y eficiencia su eje vertebrador siempre con la mira puesta en los ciudadanos». Sobre esta cuestión, vid. Cotino Hueso, L., «La preocupante falta…», *op. cit.*, con referencia a López Tallón, A., *Manual práctico de supervivencia en la Administración electrónic@*,, MetaBiblioteca. Biblioteca virtual de Libros en abierto, 2010; y a Gamero Casado, E. (Dir.), *Tratado de procedimiento administrativo…, op. cit.,* quien destaca «el plano de irrealidad en el que se han movido los redactores de la Ley» al imponer la obligatoriedad casi por defecto, sin pensar en los ciudadanos y sí en la necesidad de la Administración de modernizarse, lo que Cotino ha calificado como un «*agárrate como puedas*», esto es, que los administrados obligados resuelvan sus problemas como puedan.

[86] Vid. Cotino Hueso, L., «La preocupante falta…», *op. cit.*.

[87] Art. 25 RGDP; y, también, Cotino Hueso, L., «El nuevo reglamento…», *op. cit.*, p. 123.

IV.2. Las derechos digitales en las relaciones con las Administraciones públicas

Hemos visto cómo normas de Derecho Administrativo regulaban las obligaciones de las Administraciones públicas en las relaciones de los ciudadanos y los derechos de los mismos, pero vamos a centrarnos ahora en cuáles son los derechos digitales que van a contribuir a consolidar la existencia de una buena Administración digital.

Así, la LOPDGDD impone algunas obligaciones concretas a los poderes públicos relacionadas, sobre todo, con el fomento de las competencias digitales y el impulso de políticas públicas destinadas a fortalecer dichas competencias, o sobre la forma de identificar a los interesados en las notificaciones y publicaciones de actos administrativos; o, por otro lado, reconoce a las Administraciones públicas una potestad de verificación de los datos aportados en las solicitudes.[88]

No obstante, la Carta, a pesar de su falta de vinculatoriedad, es mucho más precisa que el resto de normas vinculantes sobre las relaciones de los ciudadanos con la Administración y se va a referir de forma expresa a los derechos digitales de los ciudadanos en dichas relaciones.

La Carta dedica su Apartado XVIII al reconocimiento de los derechos digitales de la ciudadanía en sus relaciones con las Administraciones Públicas, que, en gran medida vienen marcados por el marco normativo sobre funcionamiento electrónico del sector público.

Entre los derechos digitales de la ciudadanía en sus relaciones con las Administraciones públicas, en primer lugar la Carta se refiere a un derecho a la igualdad de las personas.

> «1. *El derecho a la igualdad de las personas se extiende al acceso a los servicios públicos y en las relaciones digitales con las Administraciones públicas. A tal fin se promoverán políticas públicas activas que garanticen el acceso a los servicios públicos, a los sistemas y los procedimientos a todos los sujetos y la asistencia en tales procedimientos»*

Este derecho implica la igualdad en el acceso a los servicios públicos y en las relaciones digitales con las Administraciones públicas. En línea con la LOPDGDD, la Carta se refiere a la promoción de políticas públicas activas que garanticen el acceso tanto a los servicios públicos, como a los sistemas y a los procedimientos a todos los sujetos y, al mismo tiempo, en línea también con las normas administrativas anteriormente citadas, reconoce también la promoción de políticas públicas orientadas a la asistencia a los ciudadanos en tales procedimientos.

[88] Arts. 83 (derecho a la educación), 97 (políticas de impulso de los derechos digitales), medidas de seguridad en el ámbito del sector público (Disp. Adic. Primera), identificación de los interesados en las notificaciones por medio de anuncios y publicaciones de actos administrativos (Disp. Adic. Séptima), potestad de verificación de las Administraciones públicas (Disp. Adic. Octava) LOPDGDD.

Directamente conectados con este primer derecho a la igualdad centrado en el acceso se encontrarían los Derechos de Igualdad reconocidos en la Carta de Derechos Digitales (Apdos. VIII a XII) que comprenden el derecho a la igualdad y a la no discriminación en el entorno digital, al disponer que el derecho y el principio a la igualdad inherente a las personas será aplicable en los entornos digitales, incluyendo la no discriminación y la no exclusión.

Con el fin de materializar las previsiones contenidas en la Carta, podemos acogernos a lo previsto, con carácter general, en la LOPDGDD, en las Leyes 39 y 40/2015 y en el RD 203/2021, y a lo dispuesto en el Esquema Nacional de Seguridad y en el de Interoperabilidad con el fin de conseguir sistemas más accesibles e interoperables. Pero, de forma más concreta con la igualdad, no sólo nos tendremos que fijar en la LO 3/2007 para la Igualdad efectiva de mujeres y hombres —cuyo Tit. V recoge el desarrollo del principio de igualdad en el empleo público y donde se recogen, entre otras cuestiones, las acciones administrativas para la igualdad (arts. 23 a 35) y los criterios de actuación de las Administraciones públicas (art. 51)—, sino también en normas que promuevan aplicar una perspectiva de género en los procesos de transformación digital, para garantizar la ausencia de sesgos en los datos y en los algoritmos usados, sesgos como los de género. Nos referimos a la Ley 15/2022 Integral de Igualdad de Trato y Prohibición de discriminación, donde se reconoce y exige, por primera vez en el ordenamiento jurídico español, la igualdad de los algoritmos.[89] Esta perspectiva de género cobra especial importancia en un entorno de un futuro fuertemente marcado por los avances tecnológicos y la utilización de herramientas como la inteligencia artificial, en un entorno dominado mayoritariamente por la presencia masculina, donde los sesgos y condicionantes existentes pueden contribuir a agravar la brecha de género en el entorno digital.

No podemos olvidar que si tenemos sociedades racistas u homófobas, nuestro futuro digital, si no lo cambiamos, será racista u homófobo. El problema aquí es evitar o corregir dichos estereotipos y su plasmación en las herramientas tecnológicas que sirvan a la Administración pública para tomar decisiones.

[89] Art. 23 Ley 15/2022: «Artículo 23. Inteligencia Artificial y mecanismos de toma de decisión automatizados. 1. En el marco de la Estrategia Nacional de Inteligencia Artificial, de la Carta de Derechos Digitales y de las iniciativas europeas en torno a la Inteligencia Artificial, las administraciones públicas favorecerán la puesta en marcha de mecanismos para que los algoritmos involucrados en la toma de decisiones que se utilicen en las administraciones públicas tengan en cuenta criterios de minimización de sesgos, transparencia y rendición de cuentas, siempre que sea factible técnicamente. En estos mecanismos se incluirán su diseño y datos de entrenamiento, y abordarán su potencial impacto discriminatorio. Para lograr este fin, se promoverá la realización de evaluaciones de impacto que determinen el posible sesgo discriminatorio. 2. Las administraciones públicas, en el marco de sus competencias en el ámbito de los algoritmos involucrados en procesos de toma de decisiones, priorizarán la transparencia en el diseño y la implementación y la capacidad de interpretación de las decisiones adoptadas por los mismos. 3. Las administraciones públicas y las empresas promoverán el uso de una Inteligencia Artificial ética, confiable y respetuosa con los derechos fundamentales, siguiendo especialmente las recomendaciones de la Unión Europea en este sentido. 4. Se promoverá un sello de calidad de los algoritmos».

En segundo lugar, entre los derechos digitales de la ciudadanía en sus relaciones con las Administraciones públicas, se indica que los principios de transparencia y de reutilización de datos las orientarán.

> «2. *El principio de transparencia y de reutilización de datos de las Administraciones públicas guiará la actuación de la Administración digital, de conformidad con la normativa sectorial. En particular, se garantizará el derecho de acceso a la información pública, se promoverá la publicidad activa y la rendición de cuentas y se velará por la portabilidad de los datos y la interoperabilidad de los formatos, sistemas y aplicaciones, en los términos que prevea el ordenamiento jurídico vigente*»

La idea es que estos principios guíen la actuación de la Administración digital, de conformidad con la normativa sectorial. Por ello se hace necesario tener en cuenta lo previsto en la Ley 19/2013, de Transparencia, Acceso a la Información Pública y Buen Gobierno, así como en sus homólogas autonómicas; y en la Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público. En esta línea, la Carta exige que los poderes públicos garanticen derechos que ya se reconocen en las citadas normas como son el derecho de acceso a la información pública, y solicita a los poderes públicos que promuevan la publicidad activa y la rendición de cuentas, y que velen por cuestiones técnicas que facilitan el tratamiento de la información por parte de los poderes públicos como son la portabilidad de los datos y la interoperabilidad de los formatos, sistemas y aplicaciones.

En este punto la Carta no hace aquí nada más que recordar y remitirse a la necesidad de cumplir los principios ya recogidos en la legislación vigente, por lo que los problemas que tienen las normas de puesta en práctica y cumplimiento de principios como la interoperabilidad es algo que sigue presente en la Carta. La cuestión es que debemos entender el proceso de digitalización como un proceso de innovación, como una apuesta por la innovación, lo que en el sector público supone una apuesta por el uso de datos abiertos y la reutilización de la información.[90]

En tercer lugar, entre los derechos digitales reconocidos a los ciudadanos en su relación con las Administraciones públicas la Carta indica que se promoverá la universalidad, la neutralidad y la no discriminación de las tecnologías usadas por las Administraciones públicas.

> «3. *Se promoverá la universalidad, la neutralidad y la no discriminación, en particular por razón de sexo, de las tecnologías usadas por las Administraciones públi-*

[90] En este sentido, vid. Valero Torrijos, J. / Cerdá Meseguer, I., «Transparencia, acceso y reutilización de la información ante la transformación digital del sector público: enseñanzas y desafíos en tiempos del COVID-19», en *Eunomía. Revista en Cultura de la Legalidad*, nº 19, 2020, pp. 103-126, quien destaca el hecho de que la transformación digital «requiere de una apuesta decidida por la innovación y, en particular, por la efectiva integración de los sistemas de información a partir de los planteamientos de los datos abiertos y la transparencia basada en la reutilización de la información del sector público» (p. 103).

cas, y se impulsará la puesta a disposición entre Administraciones de aplicaciones de cuyos derechos de propiedad intelectual sean titulares, salvo supuestos de especial protección por una norma. Las Administraciones públicas promoverán que la provisión de servicios por medios digitales respete los principios de esta Carta»

La Carta señala que la no discriminación lo será en particular por razón de sexo. Nuevamente vuelve a hacerse hincapié en la aplicación de la perspectiva de género, con lo que ello implica de cumplir la legislación vigente, y ya citada, sobre la materia.

Más allá de reiterar la necesidad de la igualdad, en este caso, destaca el hecho de que se exige el cumplimiento del principio de igualdad no sólo respecto del diseño o desarrollo de aplicaciones por parte de las Administraciones públicas, sino respecto de las tecnologías por ellas usadas, lo que indirectamente está afectando a las aplicaciones desarrolladas por el sector privado.

Asimismo, la Carta exige impulsar el intercambio de aplicaciones que hayan sido diseñadas por las Administraciones públicas, respecto de las cuales tengan los derechos de propiedad intelectual, dejando de lado las que sean de titularidad privada o, como la propia Carta indica, respecto de las que exista una especial protección por una norma que exija un deber de confidencialidad o secreto. El problema aquí será nuevamente la interoperabilidad de las aplicaciones desarrolladas. Y nuevamente encontramos un problema recurrente en el ámbito de los avances tecnológicos y es la dicotomía entre sector público y sector privado. No tiene sentido, hoy en día, seguir separando ambos ámbitos. La digitalización no se trata de una cuestión que afecte exclusivamente al sector público. La propia naturaleza de la transformación digital ha convertido a los operadores privados en un agente de primer orden en la garantía, o posible lesión, de los derechos fundamentales, con independencia de su tamaño o localización.

Ello obliga a innovar el ordenamiento jurídico tanto desde el punto de vista del entendimiento tradicional de los derechos como límites al poder público, como desde la óptica de las garantías. Los derechos no son sólo límites al poder público.

Asimismo, son estos gigantes tecnológicos los que están creando y tienen el potencial económico para crear las ya citadas herramientas disruptivas y diseñar, por ejemplo, algoritmos, que, como se ha dicho , perseguirán un objetivo puramente comercial, más allá de cualquier tipo de interés público. Por ello, debemos entender que el sector privado es protagonista, pero que también tiene cierta responsabilidad, no tanto por los contenidos porque no son editores en sentido estricto, pero sí porque interfieren en el ejercicio de los derechos.[91] Esto exige contar con un sector privado que opere como

[91] Sobre el papel de los gigantes tecnológicos y su responsabilidad, vid. Arenas Ramiro, M. / Díaz Lima, D. «Privacidad y derechos digitales», en Balaguer Callejón, F. y Cotino Hueso, L. (Coords.), *Derecho público de la Inteligencia Artificial,* FMGA, Zaragoza, 2023, pp. 304-313. Asimismo, vid. las Conclusiones del Abogado General del TJUE, Szpunar, de 8 de junio de 2023 (C-376/22) al hilo de analizar la normativa austriaca por la que se obligaba a los prestadores de plataformas digitales a establecer un procedimiento de control de contenidos presuntamente ilícitos.

un protagonista comprometido y proactivo a la hora de investigar, innovar y emprender, y que lo haga desde la ética de la garantía de los derechos fundamentales. Pero también implica exigir responsabilidades, por su responsabilidad cívica o ética y democrática, y limitar su actuación frente a posibles riesgos generados por su actuación porque es a través de su tecnología y de las herramientas que generan cómo condicionan el ejercicio de nuestros derechos, requiriéndose, por lo tanto, la intervención política de los Estados y no dejándose nuestros derechos y la estructura de nuestros Estados, en manos de la buena voluntad de estos gigantes digitales.[92]

Se hacen necesarias normas que regulen esta transformación digital y que los Estados asuman que una regulación es necesaria porque todo mercado necesita de una regulación, no teniendo sentido la eterna dicotomía entre Estado y mercado.[93] No puede dejarse la cuestión totalmente a lo que ellas decidan ni en clave estratégica e internacional, ni respecto del ámbito electoral, ni en general. Sus intereses privados en modo alguno tienen por qué alinearse con los intereses nacionales ni con los intereses públicos y derechos fundamentales de la ciudadanía en juego. De ahí que es necesario ver qué fórmulas de regulación emplear para hacer prevalecer tales intereses y derechos en juego.

Por otro lado, se garantiza la accesibilidad universal en el entorno digital, promoviendo las condiciones necesarias para garantizar la accesibilidad universal de los entornos digitales, en particular a las personas con discapacidad, tanto desde el punto de vista del diseño tecnológico como respecto de sus contenidos, asegurando especialmente que la información relativa a las condiciones legales del servicio resulte accesible y comprensible. En este sentido, la accesibilidad universal se reconoce también en la Carta de Derechos Digitales en su Apdo. XI;[94] y se solicita la promoción de políticas públicas destinadas a romper la brecha digital de acceso en su Apdo. XII.[95] Así pues, en

---

[92] Vázquez Alonso, Víctor Javier, «La censura «privada…», *op. cit.,* pp. 121-122.

[93] Así lo manifestó el Prof. Amunátegui en la entrevista realizada por Reche reflexionando sobre el desarrollo de la IA, los problemas jurídicos que plantea, y cómo cambiará nuestra aproximación al Derecho en el futuro. Vid. Reche Tello, N., «Protegiendo la privacidad mental a través de la regulación de las neurotecnologías. El modelo médico de Chile», en *Revista La Ley Privacidad*, núm. 12, 2022.

[94] El Apdo. XI Carta de Derechos Digitales dispone: «Accesibilidad universal en el entorno digital. 1. Se promoverán las condiciones necesarias para garantizar la accesibilidad universal de los entornos digitales, en particular a las personas con discapacidad, tanto desde el punto de vista del diseño tecnológico como respecto de sus contenidos, asegurando especialmente que la información relativa a las condiciones legales del servicio resulte accesible y comprensible. 2. Los entornos digitales, en particular los que tengan por finalidad la participación en los asuntos públicos, incorporarán medidas que aseguren la participación efectiva, en particular de las personas con discapacidad. 3. Se fija el objetivo de garantizar el derecho a la alfabetización y a la educación digital, en particular de las personas con discapacidad».

[95] El Apdo. XII Carta de Derechos Digitales sobre las «Brechas de acceso al entorno digital» dispone: «1. Se fomentará y facilitará el acceso de todos los colectivos a los entornos digitales y su uso y la capacitación para el mismo. 2. Se promoverán políticas públicas específicas dirigidas a abordar las brechas de acceso atendiendo a posibles sesgos discriminatorios basados en las diferencias existentes por franjas de edad, nivel de autonomía, grado de capacitación digital o cualquier otra circunstancia personal o social para garantizar la plena ciudadanía digital y participación en los asuntos públicos de todos los colectivos en mayor riesgo de exclusión social, en particular el de personas mayores, así como la utilización del entorno digital en los

los procesos de transformación digital se velará, con arreglo a la normativa aplicable, por la accesibilidad de toda clase, incluso de las personas mayores, lo que en el caso de las Administraciones públicas implicará tener en cuenta lo previsto en otras normas, específicamente, en el Real Decreto 1112/2018, sobre Accesibilidad de los sitios web y aplicaciones para dispositivos móviles del sector público.[96] En el citado RD se recogen los principios y requisitos para la accesibilidad de los sitios web y de las aplicaciones para dispositivos móviles, entre los que se indica la obligación para las Administraciones públicas de dar cumplimiento a la citada accesibilidad de modo que «sus contenidos sean perceptibles, operables, comprensibles y robustos», a la vez que señala, algo muy destacable, que la accesibilidad «se tendrá presente de forma integral» en todo el proceso de vida de la web o aplicación diseñadas.[97]

Se pretende así no sólo llegar al mayor número de ciudadanos, sino poner fin a la fragmentación del mercado y a la diferenciación técnica, no sólo a nivel nacional, sino a nivel europeo, con el fin de evitar el uso de aplicaciones con versiones diferentes que, en último término, las hagan no interoperables y con ello, no operables ni útiles para la ciudadanía a la que van dirigidas a dar servicio.

En cuarto lugar, la Carta añade entre los derechos digitales de los ciudadanos en sus relaciones con las Administraciones públicas la exigencia de que se ofrecerán alternativas en el mundo físico que garanticen los derechos de aquellas personas que no quieran o no puedan utilizar recursos digitales y no resulten obligadas a ello, en las mismas condiciones de igualdad.

> «4. *Se ofrecerán alternativas en el mundo físico que garanticen los derechos de aquellas personas que no quieran o no puedan utilizar recursos digitales y no resulten obligadas a ello, en las mismas condiciones de igualdad*»

Esta cuestión está directamente relacionada con la brecha digital de acceso —que ya hemos señalado tenía su reconocimiento también en el Apdo. XII Carta Derechos Digitales—, pero también con la libre elección, reconocida en las normas administra-

procesos de envejecimiento activo. Los asuntos públicos de todos los colectivos, en particular el de personas mayores, así como la utilización del entorno digital en los procesos de envejecimiento activo».

[96] Entre las normas que completan lo previsto en el citado RD de 2018 debemos citar: la Ley 34/2002, de Servicios de la sociedad de la información y de comercio electrónico; la Ley 9/2017, de Contratos del Sector Público; la Ley 19/2013, Transparencia, Acceso a la información pública y Buen Gobierno; y la Ley 40/2015, de Régimen Jurídico del Sector Público. De forma específica para la Administración de Justicia, la Ley 18/2011, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia. O, de forma más concreta para determinados tipos de minusvalías o personas con discapacidad, la Ley 27/2007, por la que se reconocen las lenguas de signos españolas y se regulan los medios de apoyo a la comunicación oral de las personas sordas, con discapacidad auditiva y sordociegas; el Reglamento sobre las condiciones básicas para el acceso de las personas con discapacidad a las tecnologías, productos y servicios relacionados con la sociedad de la información y medios de comunicación social (RD 1494/2007); o la Ley General de derechos de las personas con discapacidad y de su inclusión social (aprobada por RDLeg. 1/2013).

[97] Art. 5 RD 1112/2018.

tivas citadas que hablan de un derecho de los ciudadanos y de una obligación de la Administración, reconociéndose así el derecho de las personas a relacionarse también por medios no electrónicos con las Administraciones públicas.[98]

Recordamos en este punto las Sentencias del Tribunal Supremo de 2021 citadas anteriormente, así como las del TEDH especialmente a partir el año 2021 y el debate surgido al respecto sobre la obligatoriedad o no de realizar una transición digital cuando las normas vigentes, ni las más recientes como el RD 203/2021, afrontan los retos que dicha transformación digital va a implicar para la ciudadanía más allá de los cambios necesarios a nivel técnico en la Administración.

En quinto lugar, se indica que el poder público autor de una actividad en el entorno digital deberá identificar a los órganos responsables de la misma.

> «5. *El poder público autor de una actividad en el entorno digital deberá identificar a los órganos responsables de la misma*»

Esto en realidad no es más que una obligación derivada del derecho a identificar a autoridades y personal responsable en las actuaciones administrativas, siendo además los responsables en la tramitación.[99]

En sexto lugar, se indica en la Carta de Derechos Digitales que en las relaciones con las Administraciones públicas, como parte de los derechos de los ciudadanos, se promoverán los derechos de la ciudadanía en relación con la Inteligencia Artificial reconocidos en la propia Carta en el marco de la actuación administrativa, que luego veremos que se reconocen en el Apdo. XXV.[100] En este sentido en la Carta se reconocen cuatro derechos.

Un primer derecho a que las decisiones y actividades en el entorno digital respeten los principios de buen Gobierno y el derecho a una buena Administración digital, así como los principios éticos que guían el diseño y los usos de la Inteligencia artificial.

> «6. *Se promoverán los derechos de la ciudadanía en relación con la inteligencia artificial reconocidos en esta Carta en el marco de la actuación administrativa reconociéndose en todo caso los derechos a:*
>
> a) *Que las decisiones y actividades en el entorno digital respeten los principios de buen gobierno y el derecho a una buena Administración digital, así como los principios éticos que guían el diseño y los usos de la inteligencia artificial*»

Es la primera vez que se hace referencia al derecho a una buena Administración digital, contribuyéndose así a consolidar su necesidad. Asimismo, se afronta uno de los

[98] Vid., en este sentido, art. 14 Ley 39/2015 y art. 3 RD 203/2021.

[99] Así, por ejemplo, art. 20 Ley 39/2015, o art. 40 Ley 40/2015 sobre los sistemas de identificación de las Administraciones públicas.

[100] Se reconoce este derecho en el Apdo. XVIII.6 Carta de Derechos Digitales.

graves riesgos, y que genera mayor desconfianza en la utilización de las tecnologías disruptivas, la falta de ética y la dificultad de encajar los códigos de valores que deben presidir las actuaciones de las Administraciones públicas. Se dispone pues el cumplimiento de los principios de buen Gobierno, reconocidos, entre otras, en la Ley 19/2013 de Transparencia.[101] Y respecto al cumplimiento de valores éticos, nos remitimos a las ya citadas «Directrices éticas para una IA fiable» de 2019, así como a lo previsto en la *Estrategia Nacional de Inteligencia Artificial* que recoge la previsión de elaboración de una *Guía de uso de la Inteligencia Artificial en el sector público* —en colaboración con las Comunidades Autónomas y las entidades locales, a través de una Conferencia Sectorial—[102] para incluir esta herramienta no sólo de manera interoperable, sino con pleno respeto a los principios éticos.[103]

---

[101] Art. 26 Ley 19/2013, que diferencia entre principios generales y principios de actuación: «1. Las personas comprendidas en el ámbito de aplicación de este título observarán en el ejercicio de sus funciones lo dispuesto en la Constitución Española y en el resto del ordenamiento jurídico y promoverán el respeto a los derechos fundamentales y a las libertades públicas. 2. Asimismo, adecuarán su actividad a los siguientes: a) Principios generales: 1.º Actuarán con transparencia en la gestión de los asuntos públicos, de acuerdo con los principios de eficacia, economía y eficiencia y con el objetivo de satisfacer el interés general. 2.º Ejercerán sus funciones con dedicación al servicio público, absteniéndose de cualquier conducta que sea contraria a estos principios. 3.º Respetarán el principio de imparcialidad, de modo que mantengan un criterio independiente y ajeno a todo interés particular. 4.º Asegurarán un trato igual y sin discriminaciones de ningún tipo en el ejercicio de sus funciones. 5.º Actuarán con la diligencia debida en el cumplimiento de sus obligaciones y fomentarán la calidad en la prestación de servicios públicos. 6.º Mantendrán una conducta digna y tratarán a los ciudadanos con esmerada corrección. 7.º Asumirán la responsabilidad de las decisiones y actuaciones propias y de los organismos que dirigen, sin perjuicio de otras que fueran exigibles legalmente. b) Principios de actuación: 1.º Desempeñarán su actividad con plena dedicación y con pleno respeto a la normativa reguladora de las incompatibilidades y los conflictos de intereses. 2.º Guardarán la debida reserva respecto a los hechos o informaciones conocidos con motivo u ocasión del ejercicio de sus competencias. 3.º Pondrán en conocimiento de los órganos competentes cualquier actuación irregular de la cual tengan conocimiento. 4.º Ejercerán los poderes que les atribuye la normativa vigente con la finalidad exclusiva para la que fueron otorgados y evitarán toda acción que pueda poner en riesgo el interés público o el patrimonio de las Administraciones. 5.º No se implicarán en situaciones, actividades o intereses incompatibles con sus funciones y se abstendrán de intervenir en los asuntos en que concurra alguna causa que pueda afectar a su objetividad. 6.º No aceptarán para sí regalos que superen los usos habituales, sociales o de cortesía, ni favores o servicios en condiciones ventajosas que puedan condicionar el desarrollo de sus funciones. En el caso de obsequios de una mayor relevancia institucional se procederá a su incorporación al patrimonio de la Administración Pública correspondiente. 7.º Desempeñarán sus funciones con transparencia. 8.º Gestionarán, protegerán y conservarán adecuadamente los recursos públicos, que no podrán ser utilizados para actividades que no sean las permitidas por la normativa que sea de aplicación. 9.º No se valdrán de su posición en la Administración para obtener ventajas personales o materiales. 3. Los principios establecidos en este artículo informarán la interpretación y aplicación del régimen sancionador regulado en este título». Y sobre estos principios adaptados al ámbito digital, vid. Cerrillo I Martínez, A. (Coord.), *A las puertas de…, op. cit.,* pp. 61-76.

[102] Según información publicada en el Portal de Transparencia de la Administración General del Estado, «Actualmente se están llevando a cabo diversos trabajos orientados a culminar el proceso de elaboración y la publicación de la Guía. Se espera que los resultados sean patentes entre 2023 y 2024».

[103] Vid. *Estrategia Nacional de Inteligencia Artificial, ENIA*, *op. cit.,* p. 59, tomando como ejemplo la Guía aprobada en el Reino Unido (*A Guide to using artificial intelligence in the public sector*, Central Digital and Data Office / Office for Artificial Intelligence, 2019. Disponible en https://www.gov.uk/government/collections/a-guide-to-using-artificial-intelligence-in-the-public-sector.

También en relación con el uso de la Inteligencia Artificial, se reconoce el derecho a la transparencia en el uso de instrumentos de Inteligencia Artificial y sobre su funcionamiento y alcance en cada procedimiento concreto y, en particular, acerca de los datos utilizados, su margen de error, su ámbito de aplicación y su carácter decisorio o no decisorio.

> «6. *Se promoverán los derechos de la ciudadanía en relación con la inteligencia artificial reconocidos en esta Carta en el marco de la actuación administrativa reconociéndose en todo caso los derechos a:*
>
> b) *La transparencia sobre el uso de instrumentos de inteligencia artificial y sobre su funcionamiento y alcance en cada procedimiento concreto y, en particular, acerca de los datos utilizados, su margen de error, su ámbito de aplicación y su carácter decisorio o no decisorio. La ley podrá regular las condiciones de transparencia y el acceso al código fuente, especialmente con objeto de verificar que no produce resultados discriminatorios»*

Así pues, la ley podrá regular las condiciones de transparencia y el acceso al código fuente, especialmente con objeto de verificar que no produce resultados discriminatorios. Destaca el conocido caso BOSCO, que era un programa informático empleado por el Gobierno español para ayudar en la concesión del bono social para obtener descuentos en la factura de la luz. Ante la comprobación de que el algoritmo arrojaba resultados discriminatorios, excluyendo a determinados colectivos vulnerables, se solicitó acceso a su código fuente. Aquí el Juzgado de lo Central de los Contencioso Administrativo nº 8, mediante Sentencia de 30 de diciembre de 2021, denegó el acceso al Código fuente por considerar que éste formaba parte de la propiedad intelectual.[104]

En tercer lugar, se reconoce el derecho a obtener una motivación comprensible en lenguaje natural de las decisiones que se adopten en el entorno digital, con justificación de las normas jurídicas relevantes, tecnología empleada, así como de los criterios de aplicación de las mismas al caso. El interesado tendrá derecho a que se motive o se explique la decisión administrativa cuando ésta se separe del criterio propuesto por un sistema automatizado o inteligente.

> «6. *Se promoverán los derechos de la ciudadanía en relación con la inteligencia artificial reconocidos en esta Carta en el marco de la actuación administrativa reconociéndose en todo caso los derechos a:*

[104] Esta Sentencia tiene su antecedente más cercano en la Sentencia del TS de Wisconsin de 2016, asunto *Estado de Wisconsin contra Loomis*. Vid. State v. Loomis, 881 N.W.2d 749 (Wis. 2016) (Disponible en https://law.justia.com/cases/wisconsin/supreme-court/2016/2015ap000157-cr.html). Sobre este asunto, vid. el excelente análisis realizado por Presno Linera, M. A., «La insoportable opacidad del algoritmo. A propósito, aunque no sólo, del caso BOSCO», en el Blog *El derecho y el revés*, publicado el 23 de abril de 2022. Vid., también el interesante estudio, en perspectiva penal, de Martínez Garay, L., «Peligrosidad, algoritmos y *due process*: el caso State v. Loomis», en *UNED. Revista de Derecho Penal y Criminología*, nº 20 (2018), pp. 485-502.

> c) *Obtener una motivación comprensible en lenguaje natural de las decisiones que se adopten en el entorno digital, con justificación de las normas jurídicas relevantes, tecnología empleada, así como de los criterios de aplicación de las mismas al caso. El interesado tendrá derecho a que se motive o se explique la decisión administrativa cuando esta se separe del criterio propuesto por un sistema automatizado o inteligente»*

La cuestión es la vuelta a la necesidad de la intervención humana en estos procesos automatizados, y, sobre todo, la explicabilidad de las decisiones tomadas.[105]

Y, en cuarto y último lugar, se reconoce que la adopción de decisiones discrecionales quede reservada a personas, salvo que normativamente se prevea la adopción de decisiones automatizadas con garantías adecuadas.

> «6. *Se promoverán los derechos de la ciudadanía en relación con la inteligencia artificial reconocidos en esta Carta en el marco de la actuación administrativa reconociéndose en todo caso los derechos a:*
>
> d) *Que la adopción de decisiones discrecionales quede reservada a personas, salvo que normativamente se prevea la adopción de decisiones automatizadas con garantías adecuadas»*

Recordamos en este punto que la necesidad de incluir garantías adecuadas en normas con el fin de garantizar el tratamiento de la información personal realizado ya

[105] Sobre esta cuestión Presno Linera nos recuerda que sobre la explicabilidad ya se pronunció la UNESCO con su *Recomendación sobre la Ética de la Inteligencia Artificial*, aprobada en la reunión del 9 al 24 de noviembre de 2021 (Código del documento SHS/BIO/REC-AIETHICS/2021). Vid. Presno Linera, M. A., «La insoportable opacidad del algoritmo. A propósito, aunque no sólo, del caso BOSCO», en el Blog *El derecho y el revés*, publicado el 23 de abril de 2022. Así en su Apdo. 40 la Recomendación declara: «La explicabilidad supone hacer inteligibles los resultados de los sistemas de IA y facilitar información sobre ellos. La explicabilidad de los sistemas de IA también se refiere a la inteligibilidad de la entrada, salida y funcionamiento de cada componente algorítmico y la forma en que contribuye a los resultados de los sistemas. Así pues, la explicabilidad está estrechamente relacionada con la transparencia, ya que los resultados y los subprocesos que conducen a ellos deberían aspirar a ser comprensibles y trazables, apropiados al contexto. Los actores de la IA deberían comprometerse a velar por que los algoritmos desarrollados sean explicables. En el caso de las aplicaciones de IA cuyo impacto en el usuario final no es temporal, fácilmente reversible o de bajo riesgo, debería garantizarse que se proporcione una explicación satisfactoria con toda decisión que haya dado lugar a la acción tomada, a fin de que el resultado se considere transparente». Y en su Apdo. 38 la Recomendación señala: «Las personas deberían estar plenamente informadas cuando una decisión se basa en algoritmos de IA o se toma a partir de ellos, en particular cuando afecta a su seguridad o a sus derechos humanos; en esas circunstancias, deberían tener la oportunidad de solicitar explicaciones e información al actor de la IA o a las instituciones del sector público correspondientes. Además, las personas deberían poder conocer los motivos por los que se ha tomado una decisión que afecta a sus derechos y libertades y tener la posibilidad de presentar alegaciones a un miembro del personal de la empresa del sector privado o de la institución del sector público habilitado para revisar y enmendar la decisión. Los actores de la IA deberían informar a los usuarios cuando un producto o servicio se proporcione directamente o con la ayuda de sistemas de IA de manera adecuada y oportuna».

la llevó a cabo el Tribunal Constitucional en su Sentencia 76/2019. En esta Sentencia, al hilo de analizar la constitucionalidad del art. 58.bis) LOREG, el TC indica que la exigencia de medidas adecuadas debe contenerse en la norma que regule el tratamiento. En este caso, la norma que regule la adopción de decisiones automatizadas en el terreno administrativo deberá contener las garantías adecuadas, no limitándose simplemente a señalar su necesidad.[106]

En este mismo sentido, el Tribunal de Justicia de la Unión Europea ha indicado que cuando las normas (es cierto que aquí se habla de normas, no de documentos sin valor vinculante) se refieran a desarrollos posteriores por «normas más específicas», estas «normas más específicas» no pueden limitarse a reiterar las disposiciones generales de las normas de las que derivan, sino que deben incluir las medidas adecuadas y específicas destinadas, en último término a proteger la dignidad humana, los intereses legítimos y los derechos fundamentales de los interesados.[107] Así pues, en las relaciones de los ciudadanos con las Administraciones públicas, hacen falta normas que recojan y regulen de forma específica y con las garantías adecuadas reflejadas expresamente en las mismas cuándo la Administración podrá tomar una decisión discrecional de forma automatizada sin intervención humana alguna.

Estos cuatro derechos, como ha indicado la propia Carta, deben ponerse en conexión con los derechos reconocidos por la misma Carta, en este caso, en su Apdo. XXV,[108] haciéndose hincapié en la no discriminación y en principios como el de transparencia o auditabilidad, así como en el hecho de la supervisión e intervención humana y a la posibilidad de impugnar las decisiones automatizadas, derecho que también se reconoce en el art. 22 RGDP.[109]

---

[106] STC 76/2019, FJ 8º. Sobre esta cuestión, vid. Arenas Ramiro, M., «Partidos políticos, opiniones políticas e Internet», en *Teoría y Realidad Constitucional*, nº 44, 2019, pp. 363-364.

[107] Vid., por ejemplo, STJUE de 30 de marzo de 2023, asunto *Hauptpersonalrat der Lehrerinnen und Lehrer* (C-34/21).

[108] La Carta reconoce en su Apdo. XXV los Derechos ante la Inteligencia artificial: «1. La inteligencia artificial deberá asegurar un enfoque centrado en la persona y su inalienable dignidad, perseguirá el bien común y asegurará cumplir con el principio de no maleficencia. 2. En el desarrollo y ciclo de vida de los sistemas de inteligencia artificial: a) Se deberá garantizar el derecho a la no discriminación cualquiera que fuera su origen, causa o naturaleza, en relación con las decisiones, uso de datos y procesos basados en inteligencia artificial. b) Se establecerán condiciones de transparencia, auditabilidad, explicabilidad, trazabilidad, supervisión humana y gobernanza. En todo caso, la información facilitada deberá ser accesible y comprensible. c) Deberán garantizarse la accesibilidad, usabilidad y fiabilidad. 3. Las personas tienen derecho a solicitar una supervisión e intervención humana y a impugnar las decisiones automatizadas tomadas por sistemas de inteligencia artificial que produzcan efectos en su esfera personal y patrimonial».

[109] Art. 22 RGPD que señala: «1. Todo interesado tendrá derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar. 2. El apartado 1 no se aplicará si la decisión: a) es necesaria para la celebración o la ejecución de un contrato entre el interesado y un responsable del tratamiento; b) está autorizada por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento y que establezca asimismo medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, o c) se basa en el consentimiento explícito del interesado. 3. En los casos a que se refiere el apartado 2, letras a) y c), el responsable del tratamiento adop-

Para finalizar, la Carta de Derechos Digitales reconoce un séptimo y último derecho digital a los ciudadanos en las relaciones que éstos mantienen con las Administraciones públicas. Así, la Carta exige a los poderes públicos que, a la hora de diseñar los algoritmos en el caso de adopción de decisiones automatizadas o semiautomatizadas, realicen de forma necesaria una evaluación de impacto en los derechos digitales de los ciudadanos.

> «7. *Será necesaria una evaluación de impacto en los derechos digitales en el diseño de los algoritmos en el caso de adopción de decisiones automatizadas o semiautomatizadas*»

Esto se debe poner en conexión con las obligaciones derivadas del cumplimiento del RGPD respecto de los tratamientos de datos personales, que también exige la necesaria evaluación de impacto en aquellos tratamientos de datos personales que impliquen decisiones automatizadas.[110] Con carácter general, sobre todo en el proceso de transformación digital de las Administraciones públicas, las evaluaciones de impacto, contribuyen especialmente a proteger los derechos de los grupos y colectivos más vulnerables, pues el empleo de la tecnología tendrá en ellos y en sus vidas un mayor impacto en sus relaciones con las Administraciones públicas en tanto que colectivos más necesitados de los servicios prestados por las mismas.[111]

Una vez vistos los derechos digitales en las relaciones con las Administraciones públicas, lo que debe quedarnos claro es que su finalidad no puede ser otra que el cumplimiento y consecución del derecho a una buena Administración. La búsqueda de una Administración eficaz y eficiente, como exige nuestro texto constitucional, que sea respetuosa con los derechos de los ciudadanos a los que debe prestar sus servicios debe materializarse en la garantía de los derechos digitales de éstos cuando se relacionen con la misma.

---

tará las medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, como mínimo el derecho a obtener intervención humana por parte del responsable, a expresar su punto de vista y a impugnar la decisión. 4. Las decisiones a que se refiere el apartado 2 no se basarán en las categorías especiales de datos personales contempladas en el artículo 9, apartado 1, salvo que se aplique el artículo 9, apartado 2, letra a) o g), y se hayan tomado medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado».

[110] Art. 22 RGPD ya citado sobre las decisiones automatizadas y elaboración de perfiles, y el art. 35 RGPD sobre evaluaciones de impacto, cuyo apartado 1 indica: «1. Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales. Una única evaluación podrá abordar una serie de operaciones de tratamiento similares que entrañen altos riesgos similares».

[111] Al respecto, vid. Valero Torrijos, J., «Las garantías jurídicas de la inteligencia artificial en la actividad administrativa desde la perspectiva de la buena administración» en *Revista Catalana de Dret Públic*, nº 58, 2019, pp. 82-96 (p. 88).

Pero la cuestión aquí es que si bien la Carta recoge los citados derechos digitales de los ciudadanos, las normas que desarrollan la organización y funcionamiento de la Administración pública no terminan de reflejar dichos derechos y, mucho menos, de hacerlos efectivos. Las normas no están preparadas, porque omiten, para los grandes cambios tecnológicos que se avecinan y tenemos encima. Nada se dice de *bigdata, machine learning*, algoritmos o Inteligencia Artificial más allá de la citada Ley 15/2022 sobre Igualdad integral de trato (en su art. 23, como ya indicamos).

Por todo ello, la respuesta debe venir orientada a la exigencia de una buena Administración. En este sentido, el planteamiento no puede ser si regular o no la tecnología, sino, por el contrario, determinar qué variables deben tenerse en cuenta en atención de sus propias características, sin que sea admisible limitarse únicamente a adoptar una postura de pasividad ante la incapacidad de gestionar los riesgos frente al avance tecnológico.

Por último, más allá de los derechos digitales reconocidos en las relaciones con las Administraciones públicas que acabamos de analizar, la Carta de Derechos Digitales reconoce en su tercer bloque, como ya ha quedado dicho, un conjunto de derechos digitales destinados a garantizar la participación y la conformación del espacio públicos (Apdos. XIII a XVIII). En primer lugar la Carta se refiere en su Apdo. XIII al Derecho a la neutralidad de Internet, que ya hemos citado. En segundo lugar, la Carta se refiere en su Apdo. XIV a las Libertades de expresión e información en los entornos digitales. En tercer lugar, completando el derecho del Apartado anterior, como una de las cualidades inherentes a la libertad de información, exigida constitucionalmente, en el Apdo. XV de la Carta encontramos el Derecho a recibir libremente información veraz. Esta exigencia es una de las formas de hacer frente a los fenómenos de desinformación y manipulación informativa crecientes en los últimos años y que ocupa uno de las primeras preocupaciones en la Unión Europea. En cuarto lugar, en el Apdo. XVI se reconoce el Derecho a la participación ciudadana por medios digitales. Nada nuevo bajo el sol si tenemos en cuenta que estos derechos se encuentran actualmente reconocidos, y con carácter vinculante, en la normativa administrativa ya señalada. Y, por último, en el Apdo. XVII la Carta se refiere al Derecho a la educación digital.

V. A MODO DE REFLEXIÓN

El verdadero reto de la Revolución digital consiste en conocer la tecnología y para qué sirve o, mejor dicho, lo que se pretende hacer con ella y puede ofrecernos, a la vez que conocer cómo impacta en nuestras vidas, cómo afecta a nuestra dignidad y desarrollo personal. Y esto se debe aplicar a su impacto en todos los derechos y en todos los ámbitos.

El diseño de una Administración digital debe plantearse con una visión de futuro no centrada en exclusiva en los cambios tecnológicos y en el salto del papel, de lo físico, a los entornos virtuales y a lo digital. Además, no basta con transformar, sino que

debemos innovar. La evolución a la hora de prestar los servicios públicos debe venir marcada «por el protagonismo de sus destinatarios».[112]

En el proceso de transformación digital que vivimos, una buena Administración debe ser una Administración modernizada y digitalizada. Es inconcebible lo contrario. La respuesta debe pasar no tanto en quién hace, quién transforma, sino en cómo transformamos, y qué criterios deben cumplirse para contar con una buena Administración digital, centrándose en los sujetos a los que se va a dar servicio.

Ninguna de las normas aprobadas hasta ahora sobre modernización y digitalización de las Administraciones públicas, ni la innovadora, aunque derogada, Ley 11/2007 —por mucho que lo intentó—, han supuesto realmente un cambio de paradigma en el ecosistema administrativo, sino que se han asentado en un modelo burocrático y alejado de las demandas sociales, que siguen reclamando en gran medida reforzar las relaciones de los ciudadanos con las Administraciones públicas, reforzar el principio democrático de nuestras Administraciones.[113]

Así, lo que es más relevante, la nueva buena Administración digital debe incluir nuevos modelos de relación entre el ciudadano y la Administración en términos de igualdad y que incluya una transparencia total sobre la información que maneja la Administración, una rendición de cuentas permanente y un nuevo modelo de participación de los ciudadanos en la vida pública.[114]

La Administración pública debe poner en todo momento a los usuarios de sus servicios, personas y empresas, en el centro de la gestión pública. La Administración debe estar al servicio de los ciudadanos, y no al revés. Y a ello deben contribuir los avances tecnológicos y los procesos de modernización de la Administración.[115] Debemos ser conscientes de que lo relevante no es tanto el contexto, sea éste físico o virtual, sino las personas, porque los avances tecnológicos no transforman la esencia y las características innatas del ser humano.[116] Así las cosas, debemos girar en torno a la idea de que la persona debe estar en el centro de la protección, la tecnología debe estar al servicio de la humanidad, y debemos dejar de concebir a los sujetos como objetos en función de lo que vale su información personal para verlos como sujetos (aunque en el entorno digital se vuelven básicamente consumidores de servicios y herramientas digitales).[117]

---

[112] Valero Torrijos, J., «De la digitalización…», *op. cit.,* p. 125, para quien con este cambio de paradigma «no resulta aventurado afirmar el avance necesario en la personalización de los mismos según el perfil, las necesidades y preferencias de cada individuo o entidad».

[113] En este sentido, vid. Valero Torrijos, J., «De la digitalización…», *op. cit.,* p. 123.

[114] Novales, A. (Coord.), *La modernización…, op. cit.*, p. 23.

[115] Se considera que «El beneficio final de todo este proceso es para la ciudadanía. Es ella quien debe monitorizar la actividad de la Administración, sentirla más cerca y poder usar aplicaciones adaptadas y personalizadas a sus necesidades, para poder mejorar los diferentes aspectos de su vida a través de la tecnología» (Vid. *Estrategia Nacional de Inteligencia Artificial, ENIA*, *op. cit.,* p. 57).

[116] Rebollo Delgado, Lucrecio / Zapatero Martin, Pilar, Derechos digitales, *op. cit.*, p. 18.

[117] En palabras del SEPD en su Opinión 4/2015 indica que se debería crear así un entorno «prosumidor». El término prosumidor fue acuñado por Toffler, A., en *The Third Wave*, 1980, y empleado también por Brown, I. / Marsden, Ch., *Regulating Code*, MIT Press, Cambridge, 2013. En otra línea, la

Desde esta perspectiva, el ciudadano debería tener libertad y capacidad de elección para escoger, en la medida de lo posible, a aquellos prestadores de servicios públicos que mejor se adapten a sus circunstancias, en lugar de ser un mero sujeto pasivo.[118]

Pero esta idea de una buena Administración digital sólo la podemos hacer factible si se cumplen dos condiciones. Por un lado, si se aprueban normas vinculantes «innovadoras» en la transformación digital, impregnadas de criterios y valores éticos, y sólo si lo hacemos evaluando los riesgos y amenazas desde el diseño y por defecto,[119] dotándolas de las garantías necesarias que prevean el principio de *favor civis*, a favor del ciudadano. Es necesario reconfigurar las garantías jurídicas para que, en definitiva, no se sustituya la burocratización por la mera tecnificación en busca de la eficacia y la eficiencia a toda costa, planteando un falso conflicto con la innovación tecnológica. La obligación de modernizar la Administración debe caer en los poderes públicos y no repercutir de forma negativa en los ciudadanos a los que debe prestarles servicio.[120]

Y, por otro lado, sólo podremos tener una buena Administración digital si existe una colaboración con el sector privado y éste, que tiene el potencial para el desarrollo de los avances tecnológicos, se hace también responsable del cambio y se someten a normas más allá de las del mercado y responden por los servicios ofrecidos o herramientas diseñadas sin ocultarse tras los criterios de la libertad de expresión e información y derechos de propiedad intelectual.[121]

Tampoco estaría de más obligar al sector público a cumplir con los derechos digitales de los ciudadanos en sus relaciones con las Administraciones públicas y garantizar un régimen sancionador efectivo, que podría venir desde la óptica del *compliance*, más allá de meros apercibimientos, lo que podría venir de la mano, de auditorías no sólo internas, sino externas, que podrían quedar residenciadas en Autoridades de control

---

opinión de Rodotà, S., *Tecnopolitica: la democrazia e le nuove tecnologie della comunicazione*, Laterza, Roma, 1997, pp. 134 y ss., y 164 y ss, refiriéndose, en lugar de al ciudadano o *citizen* al «*netizen*» como consumidor. Al respecto, vid. Villaverde Menéndez, I., «Ciberconstitucionalismo, las TIC y los espacios virtuales de los derechos fundamentales», en *Revista catalana de Dret Public*, nº 35, 2007, pp. 23 y 30.

[118] Novales, A. (Coord.), *La modernización…, op. cit.,* p. 2.

[119] Interesante el planteamiento de aplicar la normativa de protección de datos a los proyectos de Inteligencia Artificial como forma de evaluar el impacto en la vida privada y dignidad de las personas, desde el diseño y por defecto de estas nuevas herramientas. Al respecto, vid. Martínez Martínez, R., «Inteligencia artificial desde el diseño. Retos y estrategias para el cumplimiento normativo», en *Revista Catalana de Dret Públic*, nº 58, 2019, pp. 64-81.

[120] No podemos olvidar que, como la propia Carta de Derechos Digitales reconoce (Apdo. XXVIII), se deja la eficacia de los derechos digitales reconocidos en la Carta, entre los que se incluyen los citados derechos digitales en las relaciones con las Administraciones públicas, en manos del Gobierno y de su voluntad, para que adopte «las disposiciones oportunas»; o incluso, para que se evalúen «las leyes administrativas y procesales vigentes a fin de examinar su adecuación al entorno digital y la propuesta en su caso de reformas oportunas en garantía de los derechos digitales» (Apdo. XXVII.4 Carta Derechos Digitales).

[121] Quizá sería interesante apostar, como indica la Carta de Derechos Digitales en su Apdo. XXVII, relativo a las garantías de los derechos digitales, por una tutela administrativa de los derechos en los entornos digitales, apostando por la promoción de mecanismos de autorregulación, control propio y procedimientos de resolución alternativa de conflictos.

independientes, como la futura Agencia Estatal de Supervisión de la Inteligencia Artificial (AESIA).[122]

Por último, entendemos que la configuración de un derecho fundamental a una buena Administración, de un derecho fundamental a una buena Administración digital, debe gozar de las correspondientes garantías y mecanismos de control,[123] y no ser reconocido únicamente en un documentos declarativo como es la Carta de Derechos Digitales.[124] Aunque es un gran paso.

Así las cosas, mientras no se plantee la aprobación formal, o la modificación normativa, de un marco jurídico específico, las Administraciones públicas no pueden dejar de asumir su responsabilidad y adoptar para sí mismas políticas exigentes que fomenten un liderazgo del sector público basado en la mejor defensa del interés general y los principios éticos propios de un Estado democrático de derecho y todo ello en clave digital. Y esto implica liderar su proceso de modernización. De ahí la necesidad de impregnar de valores y principios éticos las normas y los avances y descubrimientos tecnológicos, que no serán más que un reflejo de la sociedad que somos. Tenemos la oportunidad de aprovechar las ventajas que nos ofrece la tecnología, construyendo sociedades más justas e igualitarias y participativas.

Consigamos que nuestras Administraciones públicas no reproduzcan la obra de Mariano José de Larra, *Vuelva usted mañana* (1833), porque el mañana ya está aquí y debemos hacerle frente por la buena salud de nuestros Estados.

VI. BIBLIOGRAFÍA

Aláez Corral, B., «Capítulo 27. El procedimiento de reforma constitucional cuarenta años después», en Punset Blanco, R. / Álvarez Álvarez, L. (Coords.), *Cuatro décadas de una constitución normativa (1978-2018). Estudios sobre el desarrollo de la Constitución española*, Civitas / Thomson Reuters, Pamplona, 2019, pp. 639-667.

Arenas Ramiro, M., «¿Rastrear o no rastrear? He ahí la cuestión. Las apps de rastreo de contactos y la protección de datos», en *La Ley Privacidad*, nº 5, julio-septiembre 2020.

[122] Con propuestas sobre las consecuencias del incumplimiento de las garantías por parte de las Administraciones públicas, desde la invalidez de los actos administrativos hasta la responsabilidad patrimonial, vid. Valero Torrijos, J., «Las garantías jurídicas….» *op. cit.*, pp. 91-93.

[123] Vid. sobre sistemas de control idóneo, especialmente cuando se empleen herramientas de Inteligencia Artificial, Valero Torrijos, J., «Las garantías jurídicas….» *op. cit.*, p. 91.

[124] Para Rodríguez-Arana este derecho ya tiene su soporte en la idea de una Administración al servicio del interés general, con suficiente base constitucional y como proyección del Estados social y democrático de Derecho, recogiendo así el concepto del «Derecho Administrativo Constitucional». Vid. Rodrigue-Arana, J., «El derecho fundamental a la buena Administración en la constitución Española y en la Unión Europea», en *Revista A&C de Direito Administratito y Constitucional*, nº 40, 2010, pp. 233-263 (pp. 248-250).

——«Partidos políticos, opiniones políticas e Internet», en *Teoría y Realidad Constitucional*, nº 44, 2019, pp. 341-372.

Arenas Ramiro, M. / Díaz Lima, D. «Privacidad y derechos digitales», en Balaguer Callejón, F. y Cotino Hueso, L. (Coords.), *Derecho público de la Inteligencia Artificial,* FMGA, Zaragoza, 2023, pp. 287-317.

Balaguer Callejón, F., «La Constitución del algoritmo», en Gomes, A. C. y otros (Coords.), *Direito Constitucional: diálogos em homenagem ao 80º aniversário de J. J. Gomes Canotilho*. Belo Horizonte, Fórum, Brasil, 2021.

——*La Constitución del algoritmo*, FMGA, Aragón, 2022.

Bañon Y Martínez, R., «La modernización de la Administración Pública española. Balance y perspectivas», en *Revista Política y Sociedad*, 13 (1993), pp. 9-20.

Berryhill, J. / Kok Heang, K. / Clogher, R. / Mcbride, K., *Hola, mundo: la Inteligencia Artificial y su uso en el sector público*, Documentos de trabajo de la OCDE sobre Gobernanza pública, nº 36, OCDE, 2019 (ed. en español 2020) (Disponible en https://www.oecd.org/gov/innovative-government/working-paper-hello-world-artificial-intelligence-and-its-use-in-the-public-sector.htm).

Brown, I. / Marsden, Ch., *Regulating Code*, MIT Press, Cambridge, 2013.

Cabo, D. / Magallón, R., «Nuevos retos para las Administraciones Públicas. Datos, cultura cuantitativa y calidad democrática», en *Telos*, 2013

Castillo Blanco, F. A., «¿Disminuyen los derechos de la ciudadanía en la era digital? A propósito de la subsanación en el procedimiento administrativo», en *Sociedad Digital*, de 14 de junio de 2021

Celeste, E., *Digital Constitutionalism. The Role of Internet Bill of Rights*, Routledge, Nueva York, 2023.

Cerrillo i Martínez, A. (Coord.), *A las puertas de la Administración digital. Una guía detallada para la aplicación de las Leyes 39/2015 y 40/2015*, INAP, Madrid, 2016.

Chico de la Cámara, P., «Notificaciones electrónicas y principios constitucionales», en Bosch Cholbi, J. L. (Coord.), *Comentarios a la Ley general tributaria al hilo de su reforma*, Wolters Kluwer, Madrid, 2016, pp. 183-196.

COMISIÓN PARA LA REFORMA DE LAS ADMINISTRACIONES PÚBLICAS (CORA), *Reforma de las Administraciones Públicas*, Ministerios de Hacienda y Administraciones Públicas y de Presidencia, Madrid, 2013 (Disponible en https://datos.gob.es/es/catalogo/e05024601-informes-cora).

Cotino Hueso, L., «Nuevo paradigma en las garantías de los derechos fundamentales y una nueva protección de datos frente al impacto social y colectivo de la inteligencia artificial», en Bauzá, M. (Coord.) / Cotino, L. (Dir.), *Derechos y garantías ante la Inteligencia Artificial y las decisiones automatizadas*, Aranzadi, Pamplona, 2022, pp. 69-105.

——«El nuevo reglamento de Administración electrónica, que no innova en tiempos de transformación digital», en *Revista Catalana de Dret Públic*, nº 63, 2021, pp. 118-136.

——«La preocupante falta de garantías constitucionales y administrativas en las notificaciones electrónica», en *Revista General de Derecho Administrativo*, nº 57, mayo 2021.

——«La obligación de relacionarse electrónicamente con la Administración y sus escasas garantías», en *IDP. Revista de Internet, Derecho y Política*, nº 26, 2018.

——«La regulación de la participación y de la transparencia a través de Internet y medios electrónicos. propuestas concretas», en *P3T, Journal of public policies and territories. Participation, citizen control, governance*, nº 2, 2012, pp. 29-31.

Díez-Picazo, L. M., *Sistema de Derechos Fundamentales*, 3ª ed., Thomson/Civitas, Madrid, 2008.

Escobar Roca, G., *Nuevos derechos y garantías de los derechos*, Marcial Pons, Madrid, 2018.

Fernández Rodríguez, J. J., «Derechos y progreso tecnológico. Pasado, presente y futuro», en Engelmann, W. (Coord.), *Sistema do Direio, novas tecnologías, globalizaçao e o constitucionalismo contemporáneo,* Universidad Santiago de Compostela, A Coruña, 2020, pp. 259-277.

Gamero Casado, E. (Dir.), *Tratado de procedimiento administrativo común y régimen jurídico básico del sector público*, Tirant lo Blanch, Valencia, 2017.

García García, J., «Gobierno abierto: transparencia, participación y colaboración en las Administraciones Públicas», en *Innovar*, 24 (54), 2014, pp. 75-88.

Gómez Manresa, M. F., «Innovación tecnológica y jurisdicción contencioso-administrativa», en *Revista Española de Derecho Administrativo*, nº 205, 2020, pp. 97-124.

Gutiérrez David, E., «Derecho de acceso a la información pública», en *Eunomía*, nº 6, 2014.

Gutiérrez Gutiérrez, I. (Coord.), *Elementos de Derecho constitucional español*, Marcial Pons, Madrid, 2014.

Jiménez Asensio, R., «Administración y ciudadanía en el reglamento de actuación del sector público por medios electrónicos», en el *Blog La Mirada Institucional*, de 25 de abril de 2021.

López Tallón, A., *Manual práctico de supervivencia en la Administración electrónic@,*, MetaBiblioteca. Biblioteca virtual de Libros en abierto, 2010.

Martínez Garay, L., «Peligrosidad, algoritmos y *due process*: el caso State v. Loomis», en *UNED. Revista de Derecho Penal y Criminología*, nº 20 (2018), pp. 485-502.

Martínez Martínez, R., «¿Un año de derechos digitales», en *Eldiario.es*, de 12 de julio de 2022.

——«Inteligencia artificial desde el diseño. Retos y estrategias para el cumplimiento normativo», en *Revista Catalana de Dret Públic*, nº 58, 2019, pp. 64-81.

Martínez Soria, J., «Gobierno electrónico en Alemania y en Europa», en Cotino Hueso, L., *Democracia, participación y voto a través de las nuevas tecnologías*, Colección Sociedad de la Información 13, Comares, Granada, pp. 245-262.

Misuraca, G / Van Noordt, C, *AI Watch, Artificial Intelligence in public services. Overview of the use and impact of AI in public services in the EU*, Oficina de publicaciones de la Unión Europea, Luxemburgo, 2020 (Disponible en https://op.europa.eu/es/publication-detail/-/publication/4c72dd88-bcda-11ea-811c-01aa75ed71a1).

Moreno Molina, J. A., «El derecho a una buena Administración», en *Lección inaugural del solemne acto de apertura del Curso Académico 2022/2023 de la Universidad de Castilla-La Mancha*, Ediciones de la Universidad de Castilla La Mancha, Cuenca, 2022.

Novales, A. (Coord.), *La modernización de la Administración pública*, Fedea Policy Paper 2022/01, enero 2022.

OECD, *Recommendation of the Council on Open Government* – OECD, 14 de diciembre de 2017. – C(2017)140 – C/M(2017)22. Paris: OECD (Disponible en https://www.oecd.org/gov/Recommendation-Open-Government-Approved-Council141217.pdf).

Pérez Luño, A.-E., «Las generaciones de derechos humanos», en *Revista del Centro de Estudios Constitucionales*, nº 10, 1991, pp. 203-217.

Piñar Mañas, J. L., «Identidad y persona en la sociedad digital», en de la Quadra-Salcedeo, T. / Piñar Mañas, J. L. (Dirs.), *Sociedad digital y Derecho*, BOE, Madrid, 2018.

Presno Linera, M. A., «La insoportable opacidad del algoritmo. A propósito, aunque no sólo, del caso BOSCO», en el Blog *El derecho y el revés*, publicado el 23 de abril de 2022.

Rallo Lombarte, A., «Una nueva generación de derechos digitales», en *Revista de Estudios Políticos*, nº 187, 2020, pp. 101-135.

——«De la «libertad informática» a la constitucionalización de nuevos derechos digitales (1978-2018)», en *Revista de Derecho Político*, nº 100, 2017.

Rebollo Delgado, L. / Zapatero Martin, P., *Derechos digitales*, UNED/Dykinson, Madrid, 2019.

Reche Tello, N., «Protegiendo la privacidad mental a través de la regulación de las neurotecnologías. El modelo médico de Chile», en *Revista La Ley Privacidad*, núm. 12, 2022.

Rivero Ortega, R. (Dir.), *Modernización de la Administración pública para la ejecución del Plan de Recuperación, Transformación y Resiliencia. Comentarios de urgencia al RDL 36/2020, de 30 de diciembre*, Ratio Legis, Salamanca, 2021.

Rodotà, S., *Tecnopolitica: la democrazia e le nuove tecnologie della comunicazione*, Laterza, Roma, 1997.

——*La vida y las reglas. Entre el derecho y el no derecho*, Trotta, Madrid, 2010.

Rodríguez-Arana, J., «La buena Administración como principio y como derecho fundamental en Europa», en *Revista Misión Jurídica*, Vol. 6, nº 6, 2013, pp. 23-56.

——«El derecho fundamental a la buena Administración en la constitución Española y en la Unión Europea», en *Revista A&C de Direito Administratito y Constitucional*, nº 40, 2010, pp. 233-263.

Sánchez González, M. y otros, «Innovación y Open Government como claves para una Universidad abierta y participativa. Estrategias y resultados en la UNIA», en *Telos*, 2014.

Silva García, F., «El derecho a la información pública en la jurisprudencia constitucional: ¿un derecho fundamental incómodo?», en *Cuestiones constitucionales. Revista Mexicana de Derecho Constitucional*, nº 24, 2011.

Tomás Mallén, B., *El derecho fundamental a una buena Administración*, INAP, Madrid, 2004.

Torres López, M.ªA., «El documento electrónico en las relaciones jurídico-administrativas: especial referencia a los actos de comunicación», en *Revista Vasca de Administración Pública*, n.º 55, 1999.

Troncoso Reigada, A., «Las Cartas de Servicio: un compromiso con el ciudadano», en *Jornadas sobre La mejora de la calidad de los servicios públicos en la Administración de la Comunidad Autónoma de La Rioja celebradas el 17 de abril de 2002*, Gobierno de La Rioja, La Rioja, 2004, pp. 109-116.

——«La Administración electrónica y la protección de datos personales», en *Revista Jurídica de Castilla y León.*, nº 16, 2008, pp. 31-112.

Tur Ausina, R., «Participación ciudadana. Oportunidad, necesidad y esencia de su regulación legal», en *Deliberación. Revista para la mejora de la calidad democrática*, nº 1, 2010.

Valero Torrijos, J., «Las garantías jurídicas de la inteligencia artificial en la actividad administrativa desde la perspectiva de la buena administración» en *Revista Catalana de Dret Públic*, nº 58, 2019, pp. 82-96.

——«La reforma de la Administración electrónica, ¿una oportunidad perdida?», en *Revista Española de Derecho Administrativo*, nº 172, 2015, pp. 13-24.

——«De la digitalización a la innovación tecnológica. Valoración jurídica del proceso de modernización de las administraciones públicas españolas en la última década (2004-2014)», en *IDP: Revista de Internet, Derecho y Política*, nº 19, 2014, pp. 117-129.

——«Administración pública, ciudadanos y nuevas tecnologías», en WAGNER, S. (Coord.), *El Derecho Administrativo en el umbral del siglo XXI: Homenaje al Profesor Dr. D. Ramón Martín Mateo*, Tirant lo Blanch, Valencia, 2000, pp. 2943-2968.

Valero Torrijos, J. / Cerdá Meseguer, I., «Transparencia, acceso y reutilización de la información ante la transformación digital del sector público: enseñanzas y desafíos en tiempos del COVID-19», en *Eunomía. Revista en Cultura de la Legalidad*, nº 19, 2020, pp. 103-126.

Vázquez Alonso, V. J., «La censura «privada» de las grandes corporaciones digitales y el nuevo sistema de la libertad de expresión», en *Teoría & Derecho. Revista de Pensamiento jurídico*, nº 32, pp. 108-129.

Villaverde Menéndez, I., «Ciberconstitucionalismo, las TIC y los espacios virtuales de los derechos fundamentales», en *Revista catalana de Dret Public*, núm. 35, 2007, pp. 19-42.

CAPÍTULO 3

NUEVAS PERSPECTIVAS DE LOS DERECHOS FUNDAMENTALES ANTE LA ADMINISTRACIÓN DIGITAL

Inmaculada Jiménez-Castellanos Ballesteros

Universidad de Sevilla
inmajcb@us.es

SUMARIO

I. INTRODUCCIÓN

Ante el reto de la digitalización, el Derecho debe jugar un papel de extraordinaria importancia y constante evolución. De un lado, debe salvaguardar los derechos humanos en el entorno digital con la misma eficacia que fuera de él frente a los riesgos y las amenazas del impacto de la implementación de las tecnologías de la información y comunicación. De otro, los ordenamientos jurídicos deben amoldarse a los cambios ante una tecnología que avanza vertiginosamente de manera imparable.

En este escenario, los Estados democráticos se ven inmersos en una necesaria adaptación a los avances de la cuarta revolución tecnológica. Esta transformación debe partir de la posición central del ciudadano y asegurar el ejercicio de su libertad individual. Para abordar los retos que depara el progreso tecnológico, el punto de partida no es otro que la dignidad humana y el libre desarrollo de la personalidad y, en consecuencia, de los derechos fundamentales que de ellos se derivan[1]. La dignidad es el límite

[1] Cotino Hueso, L., «Nuevo paradigma en la garantía de los derechos fundamentales y una nueva protección de datos frente al impacto social y colectivo de la inteligencia artificial», en Cotino Hueso,

jurídico claro frente a los peligros estructurales de los derechos o de la propia humanidad. Asimismo, de la dignidad pueden derivarse en su caso nuevos derechos fundamentales o nuevos contenidos y garantías de los ya existentes[2]. Como afirma Rallo Lombarte, la sociedad digital demanda un haz de derechos que garanticen la subordinación de la tecnología al individuo, preserven su dignidad y se proyecten sobre la totalidad de los ámbitos en que actúa en sociedad[3].

En uno de estos ámbitos, concretamente en el sector público, la Administración Pública ha pasado por un proceso continuo de digitalización con dos fases: de la actividad presencial o en papel, a una etapa desarrollada fundamentalmente *on line* por medios electrónicos en las relaciones con los administrados, especialmente tras la pandemia provocada por el Covid-19, lo cual ha desembocado en un impulso a la Administración digital.

A esto hay que añadir un cambio en la gestión pública con la irrupción de nuevas tecnologías disruptivas y con el recurso a los sistemas de inteligencia artificial y los algoritmos en la toma de decisiones que se alimentan de datos. La respuesta del Derecho a estos nuevos desafíos jurídicos demanda que las Administraciones Públicas, en la prestación de servicios públicos a la sociedad, mantengan el justo equilibrio entre las ventajas que reporta la transformación digital y la garantía de los derechos de los ciudadanos en estos nuevos entornos, desarrollando las mejores condiciones posibles para que la libertad y la igualdad del individuo y de los grupos en que se integra sean reales y efectivas como promueve el artículo 9.2 de la Constitución Española (CE).

En este contexto, las soluciones jurídicas son aún incipientes, pues carecemos de un marco jurídico específico, sin olvidar la labor en este campo de la Unión Europea (UE). Entre los derechos de última generación, se van afirmando nuevos derechos digitales. Así, en España se recogen en la Carta de Derechos digitales[4] elaborada en julio de 2021 que, aunque sin valor normativo, viene a ser, en cierto modo, una concreción de nuestro catálogo de derechos fundamentales a la era digital. Como señala en su artículo 25, «la inteligencia artificial deberá asegurar un enfoque centrado en la persona y su inalienable dignidad». De acuerdo con sus consideraciones previas, «no trata de crear nuevos derechos fundamentales sino de perfilar los más relevantes en el entorno y los espacios digitales o describir derechos instrumentales o auxiliares de los primeros». Si bien estos instrumentos de naturaleza declarativa pueden sentar unos principios básicos y vertebradores de la sociedad digital, deben ir necesariamente acompaña-

---

L., (dir.), *Derechos y garantías ante la inteligencia artificial y las decisiones automatizadas*, Aranzadi, Cizur Menor (Navarra), 2022, p.67.

[2] *Ibid.*,p.71.

[3] Rallo Lombarte, A., « Una nueva generación de derechos digitales», en *Revista de Estudios Políticos*, 187, enero-marzo, 2020, p.103.

[4] https://www.lamoncloa.gob.es/presidente/actividades/Documents/2021/140721-Carta_Derechos_Digitales_RedEs.pdf. Fecha de consulta: 19-01-2023.

dos de las oportunas reformas normativas y de políticas proactivas centradas en el ciudadano, ante los nuevos desafíos que son ya una realidad.

II. DERECHOS DIGITALES DE LA CIUDADANÍA EN SUS RELACIONES CON LAS ADMINISTRACIONES PÚBLICAS

Bajo este epígrafe de la Carta de derechos digitales y el titulado derechos ante la inteligencia artificial, se recoge una relación de derechos fundamentales que se ven especialmente afectados en las relaciones Administración-administrado en el medio digital.

Los derechos digitales pueden definirse como un conjunto de facultades de los individuos diseñados específicamente para preservar los intereses, libertades y otros derechos consolidados frente a las transgresiones y vulneraciones que impliquen el avance de las nuevas tecnologías y las relaciones de poder que se están gestando. En consecuencia, los derechos digitales acometerían una doble finalidad: por un lado, la adaptación de los derechos reconocidos frente a los riesgos y amenazas que implica la implementación de la revolución tecnológica; y, por otro, los derechos de nueva creación que se configuren para dar respuesta a necesidades inéditas[5].

En este apartado, vamos a centrarnos en la primera finalidad y en los principales derechos fundamentales que se ven afectados por el avance de la revolución digital, tomando la Carta de derechos digitales como documento de referencia.

II.1. El principio de igualdad en las relaciones digitales con la Administración

En el artículo 18 párrafo 1, 3 y 4 se contempla este principio:

> «1. *El derecho a la igualdad de las personas se extiende al acceso a los servicios públicos y en las relaciones digitales con las Administraciones Públicas. A tal fin se promoverán políticas públicas activas que garanticen el acceso a los servicios públicos, a los sistemas y los procedimientos a todos los sujetos y la asistencia en tales procedimientos».*
>
> «3. *Se promoverá la universalidad, la neutralidad y la no discriminación, en particular por razón de sexo, de las tecnologías usadas por las Administraciones Públicas(…).*
>
> 4. *Se ofrecerán alternativas en el mundo físico que garanticen los derechos de aquellas personas que no quieran o no puedan utilizar recursos digitales y no resulten obligadas a ello, en las mismas condiciones de igualdad.»*

[5] Expósito Gázquez, A., « Los derechos digitales: apertura del debate jurídico para su concreción y desarrollo», en Cerrillo i Martinez, A.(dir.), *La Administración digital*, Dykinson, Madrid, 2022, p. 144.

El propósito de esta proclamación en la Carta es proyectar el principio de igualdad sobre las relaciones digitales con las Administraciones Públicas. La igualdad, como valor superior del ordenamiento jurídico (artículo 1.1 CE), es también un derecho fundamental que vincula a todos los poderes públicos (artículo 14 CE). Por tanto, en el acceso a los servicios públicos y en las relaciones digitales en el sector público, las Administraciones no pueden dispensar ningún trato discriminatorio. A tal fin, y en línea con la igualdad material (artículo 9.2 CE), los poderes públicos deben promover políticas públicas que fomenten y garanticen la condiciones que posibiliten que la igualdad en este sector sea real y efectiva.

La universalidad en el acceso a los servicios públicos y en las relaciones digitales con la Administración Pública exige la superación de la brecha digital. Este es un concepto complejo, que supone la toma de conciencia de los obstáculos en la conexión y acceso, en la formación adecuada en esta herramienta y en sus consecuencias discriminatorias en otros entornos de la sociedad. En este sentido, la edad, el género, las capacidades limitadas, los grupos vulnerables, el medio rural y los problemas económicos son factores a tener en cuenta, porque de ellos se derivan desigualdades no solo en el acceso a Internet sino en el ejercicio de otros derechos sociales (ayudas, prestaciones, subvenciones).

En relación con el derecho de acceso a Internet, su implantación como herramienta de comunicación y de relación con las Administraciones Públicas ha supuesto un elemento esencial en la construcción de nuestras sociedades digitales, pero no ha tenido un reconocimiento jurídico paralelo, lo que ha dificultado la concreción y desarrollo de este derecho. En el ámbito internacional, países como México lo contemplan en sus textos constitucionales[6]. En España, el acceso a la conexión a Internet no es considerado un derecho fundamental (disposición final primera), si bien tiene reconocimiento expreso en el artículo 81 de la Ley 3/2018, de 5 de diciembre de Protección de Datos Personales y garantía de los derechos digitales: «1. Todos tienen derecho a acceder a Internet independientemente de su condición personal, social, económica o geográfica. 2. Se garantizará un acceso universal, asequible, de calidad y no discriminatorio para toda la población.3. El acceso a Internet de hombres y mujeres procurará la superación de la brecha de género tanto en el ámbito personal como laboral. 4. El acceso a Internet procurará la superación de la brecha generacional mediante acciones dirigidas a la formación y el acceso a las personas mayores. 5. La garantía efectiva del derecho de acceso a Internet atenderá la realidad específica de los entornos rurales.6. El acceso a Internet deberá garantizar condiciones de igualdad para las personas que cuenten con necesidades especiales»[7]. El contenido de este de-

[6] Artículo 6 de la Constitución política de los Estados Mexicanos de 1917: «*El Estado garantizará el derecho de acceso a las tecnologías de la información y comunicación, así como a los servicios de radiodifusión y telecomunicaciones, incluido el de banda ancha e Internet. Para tales efectos, el Estado establecerá condiciones de competencia efectiva en la prestación de dichos servicios*».

[7] RD 203/2021 de 30 de marzo por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos.

recho debe conectarse con el mandato del artículo 97 de la LOPDGDD en cuanto a las políticas de impulso de los derechos digitales que deberán llevar a cabo el Gobierno, en colaboración con las Comunidades Autónomas, mediante la elaboración de un plan de acceso a Internet con, entre otros objetivos, superar las brechas digitales y garantizar el acceso a Internet de colectivos vulnerables o con necesidades especiales y de entornos familiares y sociales económicamente desfavorecidos mediante, además de otras medidas, un bono social de acceso a Internet y el impulso de la creación de espacios de conexión de acceso público. En el ámbito de la Administración Pública, el articulo 2 b) del RD 203/2021 de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos, establece como principio el de accesibilidad, entendido como el conjunto de principios y técnicas que se deben respetar al diseñar, construir, mantener y actualizar los servicios electrónicos para garantizar la igualdad y la no discriminación en el acceso de las personas usuarias, en particular de las personas con discapacidad y de las personas mayores.

En cualquier caso, la crisis del Covid-19 puso de manifiesto la importancia instrumental del acceso a Internet para el ejercicio de otros derechos fundamentales, como el derecho a la educación o la libertad de expresión e información. Las garantías de su ejercicio a día de hoy resultan francamente mejorables.

De otro lado, las destrezas de las personas en el manejo de las tecnologías no son las mismas si pensamos en las generaciones analógicas o en las personas con discapacidad[8]. Por tanto, las Administraciones Públicas deben poner a disposición de estos ciudadanos los canales tradicionales de comunicación para que puedan acceder a los servicios públicos en condiciones de igualdad con los nativos digitales. En este sentido el artículo 97.1c) LOPDGDD: «El Gobierno, en colaboración con las comunidades autónomas, elaborará un Plan de Acceso a Internet con los siguientes objetivos: c) fomentar medidas educativas que promuevan la formación en competencias y habilidades digitales básicas a personas y colectivos en riesgo de exclusión digital y la capacidad de todas las personas para realizar un uso autónomo y responsable de Internet y de las tecnologías digitales». En esta línea, la Red de centros de capacitación digital pretende promover las habilidades digitales de la ciudadanía más vulnerable, en particular en sus relaciones con las Administraciones Públicas[9].

Esto enlaza con la vertiente negativa del derecho de acceso a Internet. Las Administraciones Públicas deben contar con medios que posibiliten las relaciones con los poderes públicos de aquellos ciudadanos que no deseen utilizar Internet y no estén obligados a ello sin que resulten discriminados en relación con aquellos que sí decidan usar estas nuevas tecnologías en sus relaciones con la Administración, entre otros ca-

[8] Artículo 9.3 de la Carta de derechos digitales.

[9] Resolución de 5 de diciembre de 2022, BOE núm.299, de 14 de diciembre de 2022, pp. 173261-173-270.

nales, a través de las Oficinas de asistencia al ciudadano[10]. Se han configurado derechos específicos como el de ser asistidos en el uso de medios electrónicos[11].

En lo que afecta al funcionamiento de la red, es elemental que se respete el principio de neutralidad. El art. 80 de la LOPDGDD regula el derecho a la neutralidad de Internet, literalmente recoge :«Los usuarios tienen derecho a la neutralidad de Internet. Los proveedores de servicios de Internet proporcionarán una oferta transparente de servicios sin discriminación por motivos técnicos o económicos». Según este derecho, cualquier ciudadano debería poder acceder a los mismos servicios, con independencia de las características técnicas de su dispositivo de acceso o el nivel económico del mismo. En este sentido, la discriminación por condiciones económico-sociales se puede convertir en una práctica habitual de la Administración si no garantiza que, con independencia del sistema operativo, todos tengan acceso a la prestación de estos servicios[12].

Por último, en relación con la brecha digital de género, superados los impedimentos de cobertura y acceso a la red, para ser parte de la sociedad digital ahora esta se centra en otros aspectos. En los últimos años se muestra la escasa presencia de las mujeres en el ámbito tecnológico. Esta segunda brecha se mantiene, a pesar de que en un primer momento se haya considerado que el abaratamiento de los dispositivos y la cuasi universalización del acceso acabaría con ella. En la última década, en España se ha reducido la brecha digital de acceso a Internet entre mujeres y hombres hasta alcanzar la paridad. No existen apenas diferencias por género en competencias digitales; sin embargo, sólo el 5,7% de las empresas españolas cuenta con especialistas femeninas en tecnologías de la información, un sector al que sólo se dedica el 1,6% de las mujeres trabajadoras. Las mujeres heredan una serie de roles que impiden la igualdad en el plano educativo, como los que tienen que ver con cuidados. Es clave cambiar las expectativas de género específicas en las profesiones para que las niñas elijan carreras más técnicas[13].

---

[10] El artículo 4 del RD 203/2021 de 30 de marzo concreta el ejercicio de este derecho entre otros canales el presencial a través de las Oficinas de asistencia al ciudadano (artículo 40).

[11] L 39/2015 de 1 de octubre de Procedimiento Administrativo Común de las Administraciones Públicas artículos 12 y 13.

[12] El artículo 1.2 del RD 1112/2018 de 7 de septiembre de accesibilidad de los sitios web y aplicaciones para dispositivos móviles del sector público dispone: «A los efectos de este real decreto se entiende por accesibilidad el conjunto de principios y técnicas que se deben respetar al diseñar, construir, mantener y actualizar los sitios web y las aplicaciones para dispositivos móviles para garantizar la igualdad y la no discriminación en el acceso de las personas usuarias, en particular de las personas con discapacidad y de las personas mayores». La finalidad de esta norma es luchar contra la brecha digital facilitando el acceso a estos recursos y herramientas a todos los ciudadanos.

[13] OBSERVATORIO NACIONAL DE TECNOLOGÍA Y SOCIEDAD, «Brecha digital de género» 2022. Madrid. Ministerio de Asuntos Económicos y Transformación Digital. Disponible en: https://www.ontsi.es/sites/ontsi/files/2022-04/brecha_digital_genero_2022.pdf. Fecha de la consulta:19-01-2023.

II.2. El respeto al derecho fundamental a la protección de datos personales en la actividad de la Administración digital.

Conforme al artículo 18.2 de la Carta de derechos digitales:

> «2. *El principio de transparencia y de reutilización de datos de las Administraciones Públicas guiará la actuación de la Administración digital, de conformidad con la normativa sectorial. En particular, se garantizará el derecho de acceso a la información pública, se promoverá la publicidad activa y la rendición de cuentas y se velará por la portabilidad de los datos y la interoperabilidad de los formatos, sistemas y aplicaciones, en los términos que prevea el ordenamiento jurídico vigente.»*

En el mundo digital, los datos se han convertido en la nueva materia prima, donde las actuaciones administrativas no son una excepción. Las Administraciones Públicas han evolucionado hacia el tratamiento masivo de datos para la gestión pública. Según el artículo 3.2 de Ley de Régimen Jurídico del Sector Público Ley 40/2015, de 1 de octubre (LRJSP): «Las Administraciones Públicas se relacionarán entre sí y con sus órganos, organismos públicos y entidades vinculados o dependientes a través de medios electrónicos, que aseguren la interoperabilidad y seguridad de los sistemas y soluciones adoptadas por cada una de ellas, garantizarán la protección de los datos de carácter personal, y facilitarán preferentemente la prestación conjunta de servicios a los interesados.» Como señala el artículo 21.1 de la Carta: «1. *El uso para el bien común de los datos personales y no personales del sector público y privado se considera un bien de interés general*».

La UE ha impulsado las posibilidades de manejo de información en manos del sector público en el marco de la Estrategia europea de datos. En este sentido a través de la Directiva (UE)2019/1024 de 20 de junio, relativa los datos abiertos y la reutilización de la información del sector público. Y más recientemente el Reglamento (UE) 2022/868, de 30 de mayo de gobernanza europea de datos que será aplicable a partir del 24 de septiembre de 2023.

Por tanto, el elemento básico desde el punto de vista de la gestión pública ya no puede seguir siendo el documento, aunque sea en soporte electrónico, sino el dato. Esto por sí solo no plantea problemas teniendo en cuenta las exigencias de autenticidad e integridad, conservación, calidad, actualización e interoperabilidad, entre otras. Existen múltiples modelos de dimensiones de calidad de datos. Tomando el que recoge Casadeús de Mingo[14], estas serían exactitud, completitud, integridad, consistencia, disponibilidad y trazabilidad. La exactitud se refiere al nivel en que los datos relejan de manera correcta la realidad; la completitud apunta al grado en que se proporcionan los

[14] Según Zhang, autor citado en el libro de Neera Bhansali, *Data Gobernance Creating Value from information asserts* (2013) en Casadeús de Mingo, A., « Gobernanza de datos», en Cerrillo i Martinez, A. (dir.), *La Administración digital*, Dikynson, Madrid, 2022, p.261.

atributos esperados de los datos; la integridad sugiere que los datos sean completos; consistencia alude a que los datos deberían estar sincronizados en toda la organización; disponibilidad indica que los datos deben ser accesibles durante el tiempo que así se requiera; y trazabilidad implica poder acceder a la transacción/operación original pese a nuevas transacciones/ operaciones, modificaciones o informes posteriores. La trazabilidad facilita la transparencia y la confianza en las Administraciones Públicas[15]. En la medida en que los datos contengan errores, sean incompletos, no estén sistematizados o no sean íntegros, bajará la calidad de la información y ello dificultará la producción de resultados fiables en base a ella o la toma de decisiones pertinentes, lo que repercutirá en el buen funcionamiento de las Administraciones, así como en la garantía de los derechos ciudadanos[16].

Todo esto implica un cambio de la mera gestión a la gobernanza de datos. En términos generales, la gobernanza de datos tiene como objetivo dar respuesta a la pluralidad, complejidad y dispersión de los datos en poder de los organismos públicos, necesaria tanto para la toma de decisiones públicas como también para la transparencia y rendición de cuentas[17].

Todas las Administraciones Públicas producen y almacenan gran variedad de datos, aparte de aquellos datos que les proporcionan los ciudadanos. En relación con los datos producidos y almacenados por las Administraciones Públicas, el principio de transparencia, el derecho de acceso a la información pública, el open data y la reutilización de los datos deben promover el derecho de los ciudadanos a comprobar que los datos que sirven para la toma de decisiones administrativas son correctos y, cuando se trate de tratamiento de datos personales, que respetan la normativa de protección de datos.

Y en relación con aquellos datos que proporcionan los ciudadanos, el principio de minimización de datos y las técnicas de anonimización tienen una importancia crucial para proteger los datos personales de los usuarios. Su recogida dependerá de las políticas de participación en asuntos públicos. La Carta de derechos digitales ha tenido en cuenta la necesidad de promover entornos digitales que contribuyan al desarrollo del derecho de participación ciudadana a través de medios digitales, para garantizar la plena democracia digital[18]. En este sentido, las redes sociales implican una nueva forma de actuar por parte de los ciudadanos en sus relaciones con las Administraciones Públicas.

Por último, aunque no se hace alusión en la Carta, cuando se desarrollen servicios digitales personalizados, los tratamientos de datos personales necesarios para ofrecer estas prestaciones adaptadas a las necesidades e intereses específicos de las personas deberán respetar la normativa de protección de datos personales.

---

[15] *Ibid.*, pp.261-262.
[16] *Ibid.*, p.263.
[17] *Ibid.*, p.258.
[18] *Vid*. Artículos 9.2 y 16 de la Carta de derechos digitales.

III. DERECHOS DE LA CIUDADANÍA EN RELACIÓN CON LA INTELIGENCIA ARTIFICIAL EN EL MARCO DE LA ACTUACIÓN ADMINISTRATIVA

Estos derechos se contemplan en el artículo 18.6 y en el artículo 25 de la Carta de derechos digitales:

III.1. Principios de buen gobierno y derecho a una buena Administración digital.

> «*6. Se promoverán los derechos de la ciudadanía en relación con la inteligencia artificial reconocidos en esta Carta en el marco de la actuación administrativa reconociéndose en todo caso los derechos a:*
>
> a) *Que las decisiones y actividades en el entorno digital respeten los principios de buen gobierno y el derecho a una buena Administración digital, así como los principios éticos que guían el diseño y los usos de la inteligencia artificial*».

El principio de buen gobierno y el derecho a una buena administración deben guiar también el funcionamiento de la Administración digital y el uso de la IA. En nuestro ordenamiento jurídico, existen principios de buen gobierno en la Ley 19/2013 de transparencia, acceso a la información y buen gobierno (LTAIBG). Concretamente, su artículo 26 establece que en la Administración General del Estado las personas incluidas en el ámbito de aplicación de la ley «observarán en el ejercicio de sus funciones lo dispuesto en la Constitución Española y en el resto del ordenamiento jurídico y promoverán el respeto a los derechos fundamentales y a las libertades públicas». Asimismo, adecuarán su actividad, entre otros principios, a la transparencia en la gestión de los asuntos públicos, asegurarán un trato igual y sin discriminaciones de ningún tipo en el ejercicio de sus funciones y actuarán con la diligencia debida en el cumplimiento de sus obligaciones y fomentarán la calidad en la prestación de servicios públicos.

El principio de buena administración, que está implícito en nuestra Constitución (artículos 9.3, 103 y 106), ha sido positivizado en la Carta de Derechos Fundamentales de la Unión Europea (artículos 41 y 42); constituye, según la mejor doctrina, un nuevo paradigma del Derecho del siglo xxi referido a un modo de actuación pública que excluye la gestión negligente y no consiste en una pura fórmula vacía de contenido, sino que se impone a las Administraciones Públicas, de suerte que el conjunto de derechos que de él se derivan (audiencia, resolución en plazo, motivación, tratamiento eficaz y equitativo de los asuntos, buena fe) debe tener plasmación efectiva y lleva aparejado, por ello, un correlativo elenco de deberes plenamente exigibles por el ciu-

dadano a los órganos públicos[19]. Se caracteriza por la centralidad de la persona, en cuanto sujeto activo del interés general, por la metodología del entendimiento, en el sentido de que en el Estado de Derecho es fundamental que los administradores de la cosa pública se habitúen a la rendición de cuentas sobre sus decisiones y, sobre todo, a que el poder se ejerza desde la explicación, desde la razón, desde la luz, desde la transparencia, desde la motivación inherente a la posición que se tiene desde arriba y por último, por la promoción de la participación ciudadana[20].

III.2. El principio de transparencia y el derecho a la explicación algorítmica

> «b) *La transparencia sobre el uso de instrumentos de inteligencia artificial y sobre su funcionamiento y alcance en cada procedimiento concreto y, en particular, acerca de los datos utilizados, su margen de error, su ámbito de aplicación y su carácter decisorio o no decisorio.*
>
> *La ley podrá regular las condiciones de transparencia y el acceso al código fuente, especialmente con objeto de verificar que no produce resultados discriminatorios.*
>
> c) *Obtener una motivación comprensible en lenguaje natural de las decisiones que se adopten en el entorno digital, con justificación de las normas jurídicas relevantes, tecnología empleada, así como de los criterios de aplicación de las mismas al caso. El interesado tendrá derecho a que se motive o se explique la decisión administrativa cuando esta se separe del criterio propuesto por un sistema automatizado o inteligente.*
>
> d) *Que la adopción de decisiones discrecionales quede reservada a personas, salvo que normativamente se prevea la adopción de decisiones automatizadas con garantías adecuadas.*
>
> 7. *Será necesaria una evaluación de impacto en los derechos digitales en el diseño de los algoritmos en el caso de adopción de decisiones automatizadas o semiautomatizadas.»*

En la actualidad se ha generalizado el uso de la IA por el sector público. En el caso concreto de las Administraciones Públicas, su empleo tiene como finalidad perseguir con eficacia y objetividad la satisfacción de los intereses generales previsto en el artículo 103 CE, que ha de conciliarse con el respeto a los derechos fundamentales y las garantías que la propia Constitución y el resto del ordenamiento jurídico otorgan a los ciudadanos en sus relaciones con los poderes públicos por exigencia del Estado de Derecho. En definitiva, el recurso a la IA es un instrumento, no un sustitutivo del

[19] Sentencia del Tribunal Supremo, (Sala de lo Contencioso-Administrativo) Sentencia núm. 1309/2020 de 15 octubre.

[20] Rodriguez Arana, J., « La buena administración como principio y como derecho fundamental en Europa», en *Misión Jurídica Revista de derecho y ciencias sociales*, Vol. 6, núm.6, 2013, p.29.

concepto de Administración Pública, tal y como la configura nuestro texto constitucional[21].

En líneas generales, el término «inteligencia artificial» (IA) se aplica a los sistemas que manifiestan un comportamiento inteligente, pues son capaces de analizar su entorno y pasar a la acción —con cierto grado de autonomía— con el fin de alcanzar objetivos específicos[22].

La Propuesta de Reglamento del Parlamento y del Consejo por el que se establecen normas armonizadas sobre la Inteligencia Artificial de la Unión Europea, también conocida como Ley de IA, *Artificial Intelligence Act* (AIA) [23] define en su artículo 3, un sistema de IA como «el software que se desarrolla empleando una o varias de las técnicas y estrategias que figuran en el anexo I y que puede, para un conjunto determinado de objetivos definidos por seres humanos, generar información de salida como contenidos, predicciones, recomendaciones o decisiones que influyan en los entornos con los que interactúa». La definición de sistema de IA pretende ser tecnológicamente neutra y resistir el paso del tiempo lo mejor posible,

Como gráficamente explica Ponce Solé, en la cocina de la IA, los algoritmos son las recetas y los datos los ingredientes[24].

Los algoritmos son un conjunto de instrucciones para solucionar un problema. Con el tiempo se han hecho más complejos. Han pasado de ser estáticos, en los que los programadores diseñan en los mismos los criterios para tomar las decisiones, a ser dinámicos, los de aprendizaje automático (*machine learning*), que tienen capacidad de aprender con el tiempo de los datos y experiencias, para tomar decisiones por sí mismos. Los algoritmos extraen patrones de las masas de datos y los resultados que se obtienen no están relacionados de modo lineal, sino complejo, por lo que no es sencillo determinar la causalidad entre datos y decisión adoptada[25]. Uno de los mayores retos a los que se enfrenta la IA es la relación inversamente proporcional que

---

[21] Martin Delgado, I., «Transparencia y explicabilidad de la IA en el sector público», en Cerrillo *et al, Aportaciones de la Red DAIA a la carta de derechos digitales. Carta de Derechos digitales y sector público: propuestas de mejora,* Red DAIA. Diciembre 2020, https://bit.ly/3paF0H0, Fecha de consulta: 26-01- 2023.

[22] Comision Europea, Comunicación de la Comisión al Parlamento Europeo, al Consejo Europeo, al Consejo, al Comité económico y social europeo y al Comité de las regiones, *Inteligencia artificial para Europa,*COM/2018/237final. Disponible en https://eur-lex.europa.eu/legalcontent/ES/TXT/HTML/?uri=CELEX:52018DC0237&from=ES. Fecha de consulta: 19-01-2023.

[23] COMISIÓN EUROPEA, Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (ley de inteligencia artificial) y se modifican determinados actos legislativos de la Unión Europea, Disponible en:https://eur-.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-958501aa75ed71a1.0008.02/DOC_1&format=PDF. Fecha de la consulta: 19-01-2023. Se trata de una regulación novedosa en esta materia, a la que le queda un largo camino por recorrer hasta que finalmente entre en vigor. El objetivo que persigue es que los sistemas de IA que se utilizan en Europa sean seguros y respeten los derechos fundamentales.

[24] Ponce Solé, J., «Inteligencia artificial, derecho administrativo y reserva de humanidad: Algoritmos y procedimiento administrativo debido tecnológico», en *Revista General de Derecho Administrativo*, 50, 2019, p.7.

[25] *Ibid.*,p.7.

muchas veces existe entre precisión e interpretabilidad, pues los modelos de *machine learning* y, dentro de ellos, especialmente los de *deep learning* basados en redes con una profundidad de capas ocultas, son los más precisos, pero a la vez los menos interpretables[26].

La actuación administrativa automatizada[27] se caracteriza por ser realizada a través de medios electrónicos, actualmente mediante sistemas de IA, a través de algoritmos, en el curso de un procedimiento administrativo, tanto en actos de trámite como resolutorios, sin intervención directa de personas. Esta última característica es aplicable sin duda a las decisiones regladas, pero hay dudas en relación a las decisiones discrecionales. Para Ponce Solé, en el ámbito de las decisiones discrecionales, la actividad administrativa solo puede ser semiautomatizada, no totalmente automatizada. La IA podrá hacerse servir como apoyo, pero la ponderación final que conduzca a la decisión debería ser humana[28]. Por su parte Martin Delgado, entiende que también cabría la automatización en estos casos cuando la discrecionalidad se concrete en criterios técnicos no políticos[29]. Más recientemente, Cerrillo y Martínez opina que la respuesta debe estar presidida por el principio de precaución. Por tanto, cuando el nivel de discrecionalidad sea alto no cabe la automatización sustituyendo a las personas, sino que procede que estos instrumentos sirvan de apoyo para la toma de la decisión. No obstante, esta conclusión no es absoluta ni permanente en el tiempo, por lo que se deberá ir actualizando a medida que vaya evolucionando el desarrollo de la tecnología[30].

Uno de los principales problemas en relación con la actuación administrativa automatizada ha sido la opacidad de los algoritmos[31]. La Administración utiliza instrumentos de gran complejidad técnica considerados como cajas negras (black box) por emplear un lenguaje de programación, por la confidencialidad o secreto en el contenido de los mismos y por la imposibilidad de acceder al código fuente[32]. De ahí se deriva

---

[26] Perez Bernabeu, B., «El principio de explicabilidad algorítmica en la normativa tributaria española: hacia un derecho a la explicación individual», en *Revista española de Derecho Financiero*, núm. 192, 2021, p.146.

[27] Artículo 41 de la Ley 40/2015 de 1 de octubre de Régimen Jurídico del Sector Público (LRJSP) y el RD 203/2021 de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos. También Andalucía, Aragón, Cataluña, Comunidad Valenciana y Galicia han regulado las actuaciones administrativas automatizadas.

[28] Ponce Solé, *op. cit*, nota 20, p.28.

[29] Martin Delgado, I.,« Naturaleza, concepto y régimen jurídico de la actuación administrativa», en *Revista de Administración Pública*, núm.180, 2009, pp. 369-370.

[30] Cerrillo i Martinez, A.,« Actividad administrativa automatizada y utilización de algoritmos» en Castillo Blanco, F. A. *et al*, *Las políticas de buen gobierno en Andalucía: digitalización y transparencia*, Instituto Andaluz de Administración Pública, 2022, p.267.

[31] La mayoría no son conocidos más allá de notas de prensa: « Horas extras que no se pagan: Así es Max, el nuevo algoritmo de la Inspección de Trabajo para acabar con el fraude laboral». Disponible en: https://www.diariosur.es. Fecha consulta 21-01-2023

[32] Baz Lomba, C., «Los algoritmos y la toma de decisiones administrativas. Especial referencia a la transparencia», en *Revista CEF legal*, núm.243, 2021,p.128.

la dificultad de saber cómo se ha tomado la decisión o los datos que se han tenido en cuenta para hacerlo.

No cabe duda que cuando las Administraciones Públicas empleen datos personales en las decisiones automatizadas les será de aplicación todo el régimen de protección de datos personales: el Reglamento General de Protección de Datos (RGPD)[33] y la Ley Orgánica 3/2018, de Protección de datos y Garantía de derechos digitales (LOPDGDD). En general, habrán de ajustarse a los principios que inspiran el tratamiento de esta clase de datos, los derechos y las bases jurídicas en las que se puede fundamentar y la necesidad de realizar evaluaciones de impacto. Y, en particular, observar las obligaciones derivadas del principio de transparencia para el responsable del tratamiento (artículos 13.2 f, 14.2 g y 15.1 h RGPD).

Asimismo, el RGPD regula la prohibición de decisiones individuales automatizadas que produzcan efectos jurídicos o que afecten significativamente de manera similar al interesado (artículo 22 RGPD)[34]. La aplicación de este artículo, con sus garantías reforzadas, no puede obviarse dando por supuesta la mediación humana. La intervención humana deber ser cualitativamente significativa, autorizada y competente para modificar la decisión. Y respecto a qué decisiones producen efectos jurídicos sobre el interesado para que el tratamiento de datos afecte significativamente a una persona, las consecuencias del tratamiento deben ser lo suficientemente importantes como para ser dignas de atención[35].

No obstante, caben excepciones y en ocasiones se permiten las decisiones individuales automatizadas. En el caso de las Administraciones Públicas la única que legitima este tratamiento es la habilitación legal (artículo 22.2 b RGPD). Así, la LRJSP prevé la posibilidad[36] y, en el ámbito tributario, la ley 58/2003 de 17 de diciembre (LGT), en su artículo 96.3.

---

[33] 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. https://www.boe.es/doue/2016/119/L00001-00088.pdf. Fecha 23-01-2023.

[34] El Grupo de trabajo del artículo 29 al abordar si el concepto *derecho* del articulo 22.1 RGPD implica la necesidad de invocación por parte del interesado o una prohibición general, se decanta por esta última interpretación, pues refuerza la idea de que sea el interesado quien tenga el control sobre sus datos personales, lo cual corresponde con los principios fundamentales del RGPD. Grupo de Trabajo para la protección de datos del articulo 29 (2017) *Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679.* p.22. https://www.aepd.es/sites/default/fils/2019-12/wp251rev01-es.pdf. Fecha de consulta: 23-01-2023.

[35] *Ibid*.p.24.

[36] También el artículo 76 de la ley 4/2019, de 17 de julio de Administración digital de Galicia ; el artículo 44 de la ley 26/2010, de 3 de agosto de régimen jurídico y de procedimiento de las Administraciones Públicas de Cataluña; el artículo 43 de la ley 5/2021, de 29 de junio de Organización y Régimen Jurídico del Sector Público Autonómico de Aragón; el artículo 48 de ley 3/2010, de 5 de mayo de Administración electrónica de la Comunidad Valenciana; el artículo 74 de la Ley Foral 11/2019, de 11 de marzo, de la Administración de la Comunidad Foral de Navarra y del Sector Público Institucional Foral; el artículo 40 del Decreto 622/2019 de 27 de diciembre de administración electrónica, simplificación de procedimientos y racionalización organizativa de la Junta de Andalucía.

Según el artículo 22.3 RGPD, los responsables del tratamiento deben proporcionar las garantías apropiadas, incluido «el derecho a obtener la intervención humana (...) a expresar su punto de vista y a impugnar la decisión». En el caso de las Administraciones Públicas, los particulares no gozarán en principio de tales derechos, que solo se prevén cuando el tratamiento sea necesario para la celebración o ejecución de un contrato o cuando esté basado en el consentimiento del particular (art. 22.3 RGPD *ab initio)*, salvo que las normas nacionales los prevean. Coincidimos con Palma Ortigosa en que, si las normas que desarrollen el art.22.2 b) RGPD no contemplan unas garantías adecuadas, estas deberían ser como mínimo el derecho a obtener la intervención humana por parte del responsable, el derecho del interesado a expresar su punto de vista y el derecho a impugnar la decisión automatizada[37]. En este sentido, el artículo 25.3 de la Carta de derechos digitales: «*3. Las personas tienen derecho a solicitar una supervisión e intervención humana y a impugnar las decisiones automatizadas tomadas por sistemas de inteligencia artificial que produzcan efectos en su esfera personal y patrimonial*».

El Parlamento Europeo, en su resolución de 16 de febrero de 2017 sobre recomendaciones a la Comisión sobre las normas de derecho Civil en materia de robótica, contempla entre los principios de ética algorítmica el de transparencia. En este sentido pone de relieve que «consiste en que siempre ha de ser posible justificar cualquier decisión que se haya adoptado con ayuda de la inteligencia artificial y que pueda tener un impacto significativo sobre la vida de una o varias personas; considera que siempre debe ser posible reducir los cálculos del sistema de inteligencia artificial a una forma comprensible para los humanos». Este principio ha sido contemplado por la Carta de Derechos Digitales entre los derechos de la ciudadanía en relación con la IA.

Desde el punto de vista de la ciencia computacional, la transparencia aplicada al algoritmo se predica solo sobre su funcionamiento técnico, es decir, la comprensión del conjunto de reglas en las que consiste el algoritmo (transparencia algorítmica). Por el contrario, la explicabilidad es un concepto más amplio, que requiere conocer no solo su funcionamiento técnico, sino también los datos empleados en el proceso de entrenamiento y el modelo de aprendizaje del mismo, porque se trata de comprender cómo toma las decisiones el modelo[38].

En el plano jurídico es difícil encontrar una base suficiente y efectiva para apoyar el derecho a una explicación a los interesados de una decisión administrativa automatizada sustentada en algoritmos.

---

[37] Palma Ortigosa, A., «Decisiones automatizadas en el RGPD. El uso de algoritmos en el contexto de la protección de datos», en *Revista General de Derecho Administrativo*, num.50, 2019, p.32.

[38] Perez Bernabeu, *op.cit.*, nota 22, p.143. La explicabilidad es un concepto complejo que requiere la concurrencia de dos elementos: completitud (*competeness*) que exige que la explicación obtenida sea suficientemente profunda para poder ser auditada e interpretabilidad, capacidad de explicar o presentar en términos comprensibles para un ser humano un modelo algorítmico. En cualquier caso, la interpretabilidad de un modelo no exige conocer al detalle el funcionamiento del modelo desde el punto de vista técnico sino ser capaz de dar al usuario final una explicación para su decisión en particular.

A nivel internacional, es necesario traer a colación la sentencia del Tribunal del Distrito de la Haya de 5 de febrero de 2020[39]. Esta sentencia fue dictada en relación con el programa «SyRI», sistema algorítmico empleado por el Gobierno de los Países Bajos para evaluar el riesgo de fraude a la seguridad social. El programa generaba informes de riesgo, es decir, señalaba si una persona física o jurídica debía ser investigada con respecto a un posible fraude, uso ilegal e incumplimiento de la legislación. El objeto del proceso judicial era si la ley neerlandesa que amparaba este programa vulneraba el derecho a la vida privada y familiar del artículo 8 CEDH, dada la peculiaridad de la Constitución de los Países Bajos, donde no existe control jurisdiccional de constitucionalidad de las leyes (artículo 120) y este se ha articulado en relación con el CEDH, dada su apertura a los Tratados internacionales que son expresamente vinculantes (artículo 94).

El Tribunal partió de una concepción amplia del derecho al respeto a la vida privada, para englobar también la protección de datos personales y aplicó un canon más estricto de control al legislador de SyRI, por un deber de responsabilidad especial cuando se aplican las nuevas tecnologías. En base a ello, si bien reconoció que la norma contemplaba con suficiente precisión y claridad las restricciones del derecho y su finalidad era legítima, el órgano judicial declaró la violación del artículo 8 CEDH porque la legislación no respetó el principio de proporcionalidad. Aunque el informe de riesgos generado por el algoritmo no tenía una consecuencia legal directa, civil, administrativa o penal, sí tenía un efecto significativo en la vida privada del afectado. Existía el riesgo de que se realicen conexiones involuntarias basadas en sesgos y graves dificultades para que la persona afectada pudiera ejercer su derecho a la defensa. En definitiva, no había garantías suficientes debido a la gran cantidad de datos recopilados, de varios tipos y de fuentes diferentes, y no se conocían los indicadores ni el modelo de riesgo ni los criterios objetivos que subyacían a la validez de estos. Y ello a pesar de que el sistema incluía garantías de anonimización, de división funcional, de borrado y de confidencialidad, todo lo cual se valoró positivamente en la sentencia. No obstante, estas garantías no eran suficientes, porque la forma en que se llevó a cabo la selección definitiva del riesgo no era pública, en definitiva, transparente.

La razón que alegaba el Gobierno acerca de la falta de información a los ciudadanos era que los defraudadores hubieran podido ajustar su conducta para eludir ser considerados perfiles de riesgo a inspeccionar, pero para el Tribunal esta no era justificación bastante. Se echó en falta una revisión exhaustiva de antemano, que hubiera servido para compensar la falta de garantías suficientes. Además del principio de transparencia (caja negra, opacidad, falta de información a los interesados), la sentencia tiene en cuenta los derechos de defensa y de no discriminación (los demandantes

[39] Cotino Hueso, L., «SyRI, ¿a quién sanciono? Garantías frente al uso de la Inteligencia Artificial y decisiones automatizadas en el sector público y la sentencia holandesa de 2020», en *La ley privacidad*, núm.4. 2020.

consideraban que tenía un efecto estigmatizador al investigar los barrios más marginales), aunque todo bajo la cobertura del art.8 CEDH.

A nivel de la UE, el RGPD contempla el derecho a obtener una explicación en el Considerando 71[40], y, en relación con el derecho de acceso a los datos personales el artículo 15.1 h) RGPD dispone que el interesado deberá obtener información sobre «la existencia de decisiones automatizadas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, *información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado*» (la cursiva es nuestra). La doctrina ha puesto el punto de mira en este precepto para fundamentar una nueva garantía, el derecho a la explicación de las decisiones automatizadas[41]. En opinión de Medina Guerrero, de estos preceptos —incluido el Considerando y los problemas de su carácter vinculante o no— es muy difícil sostener que del RGPD se derive inmediatamente el derecho a la explicación algorítmica como norma armonizadora para toda la Unión[42]. Para Boix Palop, se trata de una norma que no está diseñada para establecer las garantías que se han de reconocer a los ciudadanos frente al ejercicio de autoridad de los poderes públicos que pueda afectar a su estatuto jurídico, a sus derechos y libertades, sino para regular el tráfico jurídico privado y proteger a los consumidores frente a empresas que realizan tratamientos de datos cada vez más masivos[43]. El Grupo de Trabajo del artículo 29 ha sostenido que el hecho de que el RGPD exija que el responsable del tratamiento ofrezca una información significativa sobre la lógica aplicada no supone necesariamente una completa explicación de los algoritmos utilizados o la revelación de todo el algoritmo[44].

Paralelamente, la UE ha estado trabajando en buscar recursos para hacer frente a los riesgos que plantea el uso de la IA. Entre los más relevantes, la Comunicación COM (2019) 168 de 8 de abril, «Generar confianza en la IA centrada en el ser hu-

---

[40] El origen del debate se encuentra en la ponencia de Goodman, B. y Flaxman,S.,« EU Regulations on Algorithmic Decision Making and Right to an Explanation», *Workshop on human interpretability in ML*, 2016, en la que defendían la existencia de este derecho en el RGPD aunque no lo mencionase expresamente el articulado. Frente a esta postura otros autores Wachter,S., Mittelstadt, B., Floridi, L., «Why a right to explanation of automated decision makimg does not exist in the General Data Protection Regulation», *International Data Privacy Law*, vol.7 núm. 2, 2017, pp.76-99, niegan el derecho a una explicación ex post de decisiones concretas sobre la base del artículo 22 RGPD, limitando el contenido del derecho a obtener información general de la existencia de decisiones automatizadas y de su lógica general sobre la base del artículo 15 RGPD, véase Roig i Batalla, A., *Las garantías frente a las decisiones automatizadas: del Reglamento General de Protección de Datos a la gobernanza algorítmica*, Bosch, Barcelona, 2020, pp.70-71.

[41] *Ibid*.,p. 28.

[42] Medina Guerrero, M.,« El derecho a conocer los algoritmos utilizados en la toma de decisiones», en *Teoría y realidad constitucional*, núm.49, 2022, p.165.

[43] Boix Palop, A., «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», en *Revista de Derecho Público: Teoría y Método*, Vol.1, 2020, p. 247.

[44] Grupo de Trabajo para la protección de datos del articulo 29 (2017), *op.cit*., nota 20, p.28.

mano», señala entre los requisitos esenciales para una IA fiable, la transparencia y señala que «*A este respecto, en la medida de lo posible debe aportarse la explicabilidad del proceso de toma de decisiones algorítmico, adaptada a las personas afectadas*»[45] (la cursiva es nuestra). Asimismo, el 19 de febrero de 2020, la Comisión Europea presentó el «Libro Blanco sobre inteligencia artificial— un enfoque europeo orientado a la excelencia y a la confianza»[46], en el que considera conveniente mejorar el marco normativo europeo abordando de manera explícita, entre otros retos, la opacidad de los sistemas basados en algoritmos, mediante requisitos de transparencia. En líneas similares, el Parlamento Europeo ha impulsado varias iniciativas[47]. Algunas han pasado a convertirse en mandatos normativos, como el Reglamento (UE) 2021/694 del Parlamento Europeo y del Consejo, de 29 de abril de 2021, por el que se establece el Programa Europa Digital y por el que se deroga la Decisión (UE) 2015/2240. Otras están en fase de elaboración, como la Propuesta del Reglamento del Parlamento y del Consejo por el que se establecen normas armonizadas sobre la Inteligencia Artificial de la Unión Europea, también conocida como Ley de Inteligencia Artificial, *Artificial Intelligence Act* (AIA). La regulación está pensada para proveedores, desarrolladores y usuarios de la IA. La Administración estará incluida en este último grupo, echándose en falta alguna mención expresa a los afectados por estos sistemas, sus derechos y sus garantías. Bajo la premisa del control basado en niveles de riesgo, el articulo 6 y el anexo III contemplan los sistemas de IA de alto riesgo sometidos a estrictos requisitos para su utilización, muchos de los cuales pueden llevarse a cabo por las Administraciones Públicas. En relación con la obligación de transparencia, el Considerando 47 impone «cierto grado de transparencia respecto de los sistemas de IA de alto riesgo para subsanar la opacidad que puede hacer a algunos de ellos incomprensibles o demasiado complejos para las personas físicas. *Los usuarios deben ser capaces de interpretar la información de salida del sistema y de usarla adecuadamente*. En consecuencia, los sistemas de IA de alto riesgo deben ir acompañados de la documentación y las instrucciones de uso oportunas e *incluir información clara y concisa, en particular sobre los posibles riesgos para los derechos fundamentales y de discriminación, cuando corresponda*» (la cursiva es nuestra). En este sentido, los artículos 13 y 52. No obstante, no se reconoce un derecho a la información como tal por parte de las personas físicas afectadas por el funcionamiento del sistema. No hay obligaciones de transparencia como garantía de cara al afectado.

---

[45] Comisión Europea, Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité económico y social europeo y al Comité de las regiones, «Generar confianza en la inteligencia artificial centrada en el ser humano» COM (2019) 168 final, p.6. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52019DC0168&from=ES. Fecha de consulta: 23-01-2023.

[46] «Libro Blanco sobre inteligencia artificial— un enfoque europeo orientado a la excelencia y a la confianza», COM (2020) 65 final. Disponible en: https://eurlex.europa.eu/legalcontent/ES/TXT/PDF/?uri=CELEX:52020DC0065. Fecha de la consulta: 23-01-2023.

[47] *Vid*. Gamero Casado, E., «El enfoque europeo de Inteligencia Artificial» , en *Revista de Derecho Administrativo- CDA,* núm.20, 2021,pp. 268-289.

En cualquier caso, en España, en el ámbito de las relaciones Administración/administrados no deja de percibirse un deber de explicación o motivación de las decisiones concretas, constitucionalmente exigible, derivado del artículo 9.3 CE, en relación con los artículos 24 y 106 CE. En tal sentido se manifiesta el artículo 35 de la ley 39/2015, de 1 de octubre, de procedimiento administrativo común (LPAC).

No obstante, es posible sostener que el fundamento constitucional del derecho a la explicación de las decisiones automatizadas se encuentra en el derecho de acceso a la información pública, recogido en el artículo 105 b) CE, como opción para conocer los algoritmos que emplean las Administraciones Públicas en la toma de decisiones. Este derecho está desarrollado en el artículo 13 d) LPAC y fundamentalmente en los artículos 12 y siguientes de la LTAIBG. Partiendo de un concepto amplio de información pública, que el artículo 13 define como «los contenidos o documentos, *cualquiera que sea su formato o soporte*, que obren en poder de algunos de los sujetos incluidos en el ámbito de aplicación de este título y que hayan sido elaborados o adquiridos en el ejercicio de sus funciones» (la cursiva es nuestra), podría interpretarse que los algoritmos son información pública. En base a este derecho, varias resoluciones del Consejo de Transparencia y Buen Gobierno y de la Comisión de Garantía del derecho de acceso a la información pública de Cataluña (GAIP) han reconocido que el concepto de información pública incluye los algoritmos que haya empleado la Administración[48].

Sin embargo, en estos casos la obligación de transparencia en el uso de algoritmos en las decisiones administrativas tiene una serie de límites. Así, los derechos de propiedad intelectual o secreto empresarial de las aplicaciones informáticas que emplea la Administración Pública cuando sean de titularidad privada (artículo 14.1 j) LTAIBG). A ello cabe añadir la inexistencia de consecuencias jurídicas en el caso de que el ente público incumpla esta obligación.

Con el incremento del uso de los sistemas algorítmicos por parte de las Administraciones Públicas, esta necesidad de explicación de las decisiones automatizadas acabará imponiéndose en la práctica por el desarrollo de la normativa sobre transparencia. En este sentido, ha sido pionera la ley 1/2022, de 13 de abril, de Transparencia y Buen Gobierno de la Comunidad Valenciana, que en su artículo 161.1 l) impone a las Administraciones Públicas, «la obligación de publicar la relación de sistemas algorítmicos o de inteligencia artificial que tengan impacto en los procedimientos administrativos o la prestación de los servicios públicos, con la descripción de manera comprensible de su diseño y funcionamiento, el nivel de riesgo que implican y el punto de contacto al que poder dirigirse en cada caso, de acuerdo *con los principios de transparencia y explicabilidad*» (la cursiva es nuestra). Se integran por tanto en esta norma, por una parte, las exigencias de publicidad activa, relativa específicamente a los sistemas algorítmicos

[48] Resolución 0093/2019 de 22 de febrero de la Comisión de Garantía del derecho de acceso a la información pública de Cataluña (GAIP) y Resoluciones RT 0748/2021 y RT 0253/2021 de 19 de noviembre del Consejo de Transparencia y Buen Gobierno.

de conformidad con lo dispuesto en términos generales por el artículo 5 de la LTAIBG, que señala que las Administraciones Públicas «publicarán de forma periódica y actualizada la información cuyo conocimiento sea relevante para garantizar la transparencia de su actividad relacionada con el funcionamiento y control de la actuación pública». Y por otra, se impone la obligación de facilitar información sobre las características técnicas del algoritmo en su concepción más amplia del derecho a una explicación comprensible, el cual es parte intrínseca de los principios de buen gobierno y del derecho a una buena administración. Por tanto, es una obligación genérica y transversal, en cualquier sector y respecto de cualquier información transmitida, vinculada, desde un aspecto negativo, con la prohibición de interdicción de la arbitrariedad constitucional (art. 9.3 CE) y, en positivo, con la obligación de motivación de las decisiones administrativas (art. 35.1 Ley 39/2015)[49].

III.3. El principio de igualdad y la no discriminación algorítmica

En términos generales se pronuncia el artículo 8 de la Carta de derechos digitales:

> «1. *El derecho y el principio a la igualdad inherente a las personas será aplicable en los entornos digitales, incluyendo la no discriminación y la no exclusión. En particular, se promoverá la igualdad efectiva de mujeres y hombres en entornos digitales. Se fomentará que los procesos de transformación digital apliquen la perspectiva de género adoptando, en su caso, medidas específicas para garantizar la ausencia de sesgos de género en los datos y algoritmos usados.*
>
> 2. *En los procesos de transformación digital se velará, con arreglo a la normativa aplicable, por la accesibilidad de toda clase».*

Por su parte el artículo 25 de la Carta de derechos digitales concreta en el desarrollo y ciclo de vida de los sistemas de inteligencia artificial:

> «a) *Se deberá garantizar el derecho a la no discriminación cualquiera que fuera su origen, causa o naturaleza, en relación con las decisiones, uso de datos y procesos basados en inteligencia artificial».*

El artículo 14 de la Constitución de 1978 proclama el derecho a la igualdad y a la no discriminación, citando como motivos especialmente rechazables el nacimiento, la raza, el sexo y la religión u opinión, y prohibiendo la discriminación por cualquier otra circunstancia personal o social. En el ámbito europeo, los artículos 14 CEDH y 1 del Protocolo 12 del CEDH y el artículo 21 CDFFUE son los instrumentos que deben

[49] Ponce Solé, *op.cit.*, nota 20,p.40.

aplicarse en los casos de discriminación algorítmica. Estos prohíben la discriminación por razón de sexo, raza, color, idioma, religión, opiniones políticas u otras, origen nacional o social, pertenencia a una minoría nacional, fortuna, nacimiento o cualquier otra situación. La CDFUE añade origen étnico, discapacidad, edad y orientación sexual.

Uno de los mayores problemas que plantea el uso de algoritmos en las decisiones administrativas automatizadas es la posibilidad de sesgos. Según el Parlamento Europeo, «sesgo» significa cualquier percepción personal o social prejuiciosa de una persona o grupo de personas sobre la base de sus rasgos personales[50]. Aun cuando los sesgos se hallen presentes en cualquier proceso decisorio, los peligros asociados a los mismos parecen incrementarse cuando se producen en el campo de la IA, en atención a su gran potencial aplicativo. Básicamente, la diferencia se plasma en el mayor riesgo de expansión y perpetuación de los sesgos que se deriva de la utilización de la IA, lo cual cobra una especial relevancia en el sector público, porque sus efectos se proyectan sobre una gran cantidad de destinatarios; y de otro lado, la IA también permite reforzar y prolongar el sesgo en el tiempo. La cuestión es si los posibles sesgos existentes en los datos que manejan los algoritmos, o en el propio modelo, serían susceptibles de generar discriminaciones jurídicamente relevantes, entendidas como diferencias de trato basadas en algún motivo protegido, y carentes de una justificación objetiva y razonable[51].

En el uso de la inteligencia artificial los sesgos pueden provenir:

A) De los programadores humanos, por la perpetuación de estereotipos. La discriminación algorítmica será considerada como discriminación directa cuando el sistema procese una categoría sospechosa y considere la pertenencia a un subgrupo desventajado como factor de entrada negativo en la decisión que se adopte. Es poco probable que se den supuestos de discriminación algorítmica de esta clase de manera consciente por los programadores. Sin embargo, puede ocurrir que el algoritmo atribuya un valor negativo a la pertenencia a un grupo desventajado, pero el resultado final no dependa exclusivamente de dicha característica, sino de la combinación de variables[52]. De ahí la importancia del principio de transparencia. En el caso de Espa-

[50] PARLAMENTO EUROPEO, Resolución de 20 de octubre de 2020, con recomendaciones a la Comisión sobre un marco de aspectos éticos de la inteligencia artificial, la robótica y las tecnologías relacionadas, (2020/2012(INL) articulo 4. DOUE C404 6/10/2021 pp. 63-106. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=OJ:C:2021:404:FULL&from=ES. Fecha de la consulta: 19-01-2023.

[51] Martin López, J., «Inteligencia artificial, sesgos y no discriminación en el ámbito de la inspección tributaria», en *Crónica Tributaria* núm. 182, 2022, pp.66-67.

[52] Soriano Arranz, A., «Discriminación algorítmica: garantías y protección jurídica», en Cotino Hueso, L. *Derechos y garantías ante la inteligencia artificial y las decisiones automatizadas*, Aranzadi, Cizur Menor (Navarra), 2022 , p.151. Cabe también la posibilidad de que el algoritmo discrimine en base a muchos atributos protegidos interrelacionados, *vid*. Capellá Ricart, A., «Discriminación algorítmica: Límites de la regulación antidiscriminación europea y recomendaciones preliminares», en *Quaderns IEE*, Vol. 1 Núm. 2 , 2022, pp.37-40.

ña, los afectados por el algoritmo (BOSCO) empleado en la concesión del bono social eléctrico, solicitaron el acceso al código fuente de este, que fue rechazado por el Ministerio para la Transición Ecológica. Presentada reclamación ante el Consejo Estatal de Transparencia y Buen Gobierno, la denegó amparándose en la protección de la propiedad intelectual del sistema, límite al derecho de acceso a la información pública. La Sentencia 143/2021, de 30 de diciembre, del Juzgado Central Contencioso Administrativo número 8 de Madrid, desestimó igualmente la demanda de acceso al código fuente. Sobre el límite de la propiedad intelectual señala esta resolución que: «hay que tener en cuenta que el código fuente de la mencionada aplicación informática no está dentro de las exclusiones de la propiedad intelectual, mencionadas en el artículo 13 del Real Decreto Legislativo 1/1996, de 12 de abril, de propiedad intelectual, precepto invocado por la entidad recurrente, pues dicho código no es una norma ni un acto administrativo». A los límites impuestos por la propiedad intelectual hay que añadir los derivados de la enorme complejidad para comprender el funcionamiento de estos sistemas.

También puede ocurrir que el propio algoritmo infiera la pertenencia a un grupo desventajado a través de otros datos a los que atribuye un valor negativo. Se trataría de discriminación algorítmica por inferencia. Junto a esta, caben las situaciones de discriminación indirecta, cuando una disposición, práctica o criterio aparentemente neutros dan lugar a resultados más perjudiciales para los miembros de un grupo especialmente protegido que para las personas no pertenecientes al mismo[53]. Para que la medida se considere justificada debe acreditarse que persigue un objetivo legítimo y supera el test de proporcionalidad: adecuación, necesidad y proporcionalidad en sentido estricto.

El diseño de los sistemas algorítmicos debe basarse en el respeto a la igualdad, incluyéndose en la evaluación de impacto los posibles riesgos de discriminación. Los responsables de la programación deben contar con equipos humanos multidisciplinares para evitar riesgos de discriminación en el diseño. Hay que vigilar que el tratamiento de los datos no realice clasificaciones o predicciones sobre la base de circunstancias especialmente sensibles y que sus correlaciones resulten justificables.

B) De los datos empleados, porque sean insuficientes, no representativos, erróneos o no actualizados. Los datos de entrenamiento deben ser representativos de la sociedad. Es imprescindible contar con datos de buena calidad. Los conjuntos de datos deben ser adecuados, precisos y generalizables, de forma que alcancen la mayor representatividad posible en términos cuantitativos y cualitativos. Por tanto, el modelo ha de ser entrenado y testado con datos que reflejen todas las características relevantes y representen con gran fidelidad la realidad sobre la que se quiere operar[54].

[53] STJUE de 22 de noviembre de 2012, asunto C-385/11, Isabel Elbal Moreno contra Instituto Nacional de las Seguridad Social, Tesorería General de la Seguridad Social.

[54] Martin López, *op.cit.*, p.80

A tales efectos, el 22.4 RGPD prohíbe expresamente que las decisiones individuales automatizadas se basen en las categorías especiales de datos personales contempladas en el artículo 9.1 RGPD, es decir, datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos relativos a la salud o datos relativos a la vida u orientación sexual de una persona física.

Con respecto a la minimización de sesgos, el Considerando 38 de la propuesta europea de ley de IA (AIA) advierte que, si el sistema de IA no está entrenado con datos de buena calidad, no cumple los requisitos oportunos en términos de precisión o solidez, o no se diseña y prueba debidamente antes de introducirlo en el mercado o ponerlo en servicio, puede señalar a personas de manera discriminatoria, incorrecta o injusta. Por eso regula en su artículo 10 los datos y la gobernanza de los datos de los sistemas de IA considerados de alto riesgo. Y precisa que los conjuntos de datos utilizados para el entrenamiento, validación y prueba de estos sistemas deberán cumplir los criterios de calidad que se detallan en sus distintos apartados. En particular, según el apartado tercero «serán pertinentes y representativos, carecerán de errores y estarán completos».

C) Del propio funcionamiento del algoritmo: correlaciones erróneas a través del uso de datos en apariencia neutros que revelan atributos personales y sensibles. Hay muchas posibilidades de que se introduzcan sesgos durante el desarrollo de estos sistemas. La falta de transparencia de algunos sistemas de inteligencia artificial, entendida como la imposibilidad de comprender la base de sus acciones, llevaría aparejado que tampoco se alcanzaran a entender las razones por las que sus resultados estarían sesgados[55]. Ello podría conllevar que una hipotética discriminación generada por la inteligencia artificial no pudiera probarse debido a la imposibilidad de conocer los motivos por los cuales se ha producido el sesgo subyacente.

El algoritmo puede no ser objeto de una explicación fácil. El coste de proporcionar una explicación puede ser excesivo, además de tener como límite los derechos de propiedad intelectual y los secretos comerciales, o, en ocasiones, puede vulnerar el derecho a la intimidad o a la protección de datos personales. En el artículo 14 de la propuesta de Reglamento se recoge el deber de que se diseñen y se desarrollen de tal manera que puedan ser supervisados de manera efectiva por personas físicas durante el período que estén en uso, para prevenir o reducir al mínimo los riesgos para los derechos fundamentales. Para Gamero Casado, las medidas en este sentido son relevantes, pero insuficientes, pues considera que, para ajustarse a esta finalidad, la supervisión humana debe llevarse a cabo por especialistas, de ahí que debería confiarse expresamente a equipos multidisciplinares, en el que tengan cabida tanto técnicos como juristas[56]. Por

[55] Ibid.p.76

[56] Gamero Casado, *op.cit.* nota 41,p.282.

tanto, desde una perspectiva exclusivamente jurídica, el foco debería situarse en la motivación del acto. Si ambos procesos decisorios, humano y computacional, originan actos con su correspondiente fundamentación, el destinatario podrá conocer las razones jurídicas que los sustenten y, en caso de no estimarlas conforme a Derecho, proceder a la oportuna impugnación, permaneciendo así incólume su derecho de defensa.[57]

Con el objetivo de dar respuesta a esta problemática, la Ley 15/2022, de 12 de julio, contempla un derecho antidiscriminatorio específico, que intenta a dar cobertura a las discriminaciones que existen y a las que puedan surgir, ya que los desafíos de la igualdad cambian con la sociedad y, en consecuencia, también deberán hacerlo en el futuro las respuestas debidas. En este sentido, su ámbito objetivo de aplicación se extiende a la IA y gestión masiva de datos, así como a otras esferas de análoga significación. Señala cómo deberán las Administraciones Públicas diseñar los algoritmos utilizados en la toma de decisiones. Así, dispone en su artículo 23:

«Inteligencia Artificial y mecanismos de toma de decisión automatizados.

1. En el marco de la Estrategia Nacional de Inteligencia Artificial, de la Carta de Derechos Digitales y de las iniciativas europeas en torno a la Inteligencia Artificial, las Administraciones Públicas favorecerán la puesta en marcha de mecanismos para que los algoritmos involucrados en la toma de decisiones que se utilicen en las Administraciones Públicas tengan en cuenta criterios de minimización de sesgos, transparencia y rendición de cuentas, siempre que sea factible técnicamente. En estos mecanismos se incluirán su diseño y datos de entrenamiento, y abordarán su potencial impacto discriminatorio. Para lograr este fin, se promoverá la realización de evaluaciones de impacto que determinen el posible sesgo discriminatorio.
2. Las Administraciones Públicas, en el marco de sus competencias en el ámbito de los algoritmos involucrados en procesos de toma de decisiones, priorizarán la transparencia en el diseño y la implementación y la capacidad de interpretación de las decisiones adoptadas por los mismos.
3. Las Administraciones Públicas y las empresas promoverán el uso de una Inteligencia Artificial ética, confiable y respetuosa con los derechos fundamentales, siguiendo especialmente las recomendaciones de la Unión Europea en este sentido.
4. Se promoverá un sello de calidad de los algoritmos.»

A la vista de lo dispuesto en la Carta de derechos digitales, esta regulación resulta claramente insatisfactoria, pues se deja depender de la dotación de medios técnicos la puesta en marcha de mecanismos para que los algoritmos que se empleen por las Administraciones Públicas tengan en cuenta los criterios de minimización de sesgos,

[57] Martin López, *op.cit.* p78.

transparencia y rendición de cuentas. Sí resulta interesante lo dispuesto en el art. 40 de la Ley integral de igualdad de trato, la previsión de la Autoridad Independiente para la Igualdad de Trato y la No Discriminación, en el ámbito de la Administración del Estado como encargada de proteger y promover la igualdad de trato y no discriminación de las personas por razón de las causas y en los ámbitos competencia del Estado previstos en esta ley, tanto en el sector público como en el privado, garantía institucional que puede ayudar al control de los sistemas de IA siempre que se la dote de equipos multidisciplinares que puedan detectar los posibles riesgos discriminatorios.

Finalmente, el artículo 8 de la Carta de derechos digitales dispone:

> «b) *Se establecerán condiciones de transparencia, auditabilidad, explicabilidad, trazabilidad, supervisión humana y gobernanza. En todo caso, la información facilitada deberá ser accesible y comprensible.*
>
> c) *Deberán garantizarse la accesibilidad, usabilidad y fiabilidad».*

La Estrategia Nacional de Inteligencia Artificial (ENIA) presentada por el Gobierno de España contempla una regulación ética y social para luchar contra la discriminación algorítmica, en la que se identifica este principio de transparencia con la idea de trazabilidad al definirse como aquella obligación de garantizar que las decisiones ejecutadas por sistemas algorítmicos puedan ser auditadas, evaluadas y explicadas por las personas responsables[58].

En cualquier caso, es precisa la rendición de cuentas por parte de las instituciones que empleen estos sistemas, que deben ser responsables de las decisiones tomadas por los algoritmos, aunque no sea posible explicar con detalle cómo se producen sus resultados. En relación con la rendición de cuentas, el artículo 17 de la propuesta europea de ley de IA (AIA) señala que los sistemas de IA de alto riesgo establecerán un sistema de gestión de la calidad que garantice el cumplimiento del presente Reglamento, que incluirá «m) un marco de rendición de cuentas que defina las responsabilidades del personal directivo y de otra índole en relación con todos los aspectos enumerados en este apartado».

IV. CONCLUSIONES

Estamos inmersos en una cuarta revolución tecnológica. Hablar hoy de derechos digitales no es solo aludir a derechos de nueva creación para dar respuesta a necesidades inéditas, sino también adaptar nuestros derechos fundamentales a los riesgos y las amenazas que implica el entono digital, partiendo de una concepción centrada en la

[58] GOBIERNO DE ESPAÑA, Estrategia nacional de inteligencia artificial. Gobierno de España, 2020, p.67, disponible en: https:/portal.mineco.gob.es/RecursosArticulo/mineco/ministerio/ficheros/201202_ENIA_V1_0.pdf . Fecha de consulta: 22-01-2023.

persona y en su inalienable dignidad. La realidad demanda más que nunca la toma de conciencia de que los avances tecnológicos deben correr paralelos al respeto y la garantía de los derechos fundamentales. Los ordenamientos jurídicos deben reforzar los mecanismos que eviten un retroceso en el ejercicio de los derechos ante la transformación digital de la actividad de los poderes públicos. En el ámbito de la Administración Pública, esta evolución está discurriendo ahora por la irrupción de nuevas tecnologías y el empleo de la IA en la toma de decisiones. Estos cambios han planteado nuevos retos para el Derecho en general y para los derechos fundamentales en particular.

De los derechos digitales de la ciudadanía en sus relaciones con las Administraciones surgen nuevos desafíos para el principio de igualdad. El acceso a Internet no tiene la consideración de derecho fundamental en nuestro ordenamiento jurídico, pero ha desempeñado un papel importante, sobre todo tras la pandemia provocada por el Covid-19, para el ejercicio de otros derechos fundamentales, como la educación o las libertades informativas. Su naturaleza de derecho instrumental ha puesto en jaque al principio de igualdad. La brecha digital no solo afecta al acceso, disposición y formación en las herramientas tecnológicas, sino que puede tener efectos discriminatorios para el Estado social. Factores como la edad, el género, las capacidades limitadas, el entorno geográfico o las condiciones socioeconómicas pueden ser causas de discriminación ante la Administración digital. En particular, la brecha digital de género ha puesto de manifiesto en los últimos tiempos la escasa presencia de las mujeres en el ámbito tecnológico. No se puede construir un Estado democrático digital si falta una parte de la ciudadanía. En este campo, queda hoy por hoy mucho por hacer.

Paralelamente, la gestión pública ha evolucionado hacia el tratamiento masivo de datos. El respeto al derecho fundamental a la protección de datos personales se impone en la actividad de las Administraciones Públicas. La gobernanza de datos es esencial para la toma de decisiones públicas, pero también para la transparencia y la rendición de cuentas. Es necesario que las Administraciones Públicas pongan el punto de mira en la calidad de datos, como prioridad. De ahí que la Carta de derechos digitales, que nos ha servido de documento de referencia a lo largo de estas páginas, afirme que el uso para el bien común de los datos personales y no personales del sector público y privado se considera un bien de interés general. Aparte del respeto a la normativa de protección de datos personales, la calidad de los datos que maneja la Administración Pública es decisiva para la confianza en la toma de decisiones y para la garantía de los derechos de los ciudadanos.

Esta nueva realidad repercute en el uso de la IA. Como hemos visto, el empleo de la IA se ha generalizado en el sector público. El principio de buen gobierno y el derecho a una buena administración están presentes en nuestro ordenamiento jurídico por lo que además de la transparencia, la igualdad y la no discriminación y la diligencia en la gestión pública añaden al entorno digital la centralidad de la persona y la metodología del entendimiento, es decir, que el poder se ejerza desde la explica-

ción. La necesidad de motivación de los actos administrativos es una garantía del derecho de defensa, pero tiene mayor trascendencia cuando los algoritmos son elementos sustanciales para la toma de decisiones, aunque formalmente estas sean tomadas por humanos.

Dos son los principales problemas en relación con la actuación administrativa automatizada: la opacidad y la producción de efectos discriminatorios derivada de los sistemas algorítmicos.

En primer término, la complejidad de estos sistemas dificulta saber cómo se han tomado las decisiones y qué datos se han tenido en cuenta para hacerlo. En el plano jurídico, es difícil encontrar una base para apoyar el derecho a una explicación a los interesados de una decisión automatizada sustentada en algoritmos. Se ha reconocido en el deber de motivación de las decisiones administrativas, que tiene su fundamento en la interdicción de la arbitrariedad de los poderes públicos y también en el derecho de acceso a la información pública, partiendo de una concepción amplia de información pública que incluya los algoritmos. Sin embargo, esta obligación tiene límites cuando los algoritmos que emplea la Administración son de titularidad privada. En la práctica, este derecho acabará imponiéndose como ya lo ha hecho la Ley de Transparencia y Buen Gobierno de la Comunidad Valenciana.

Sin embargo, no basta con el cumplimiento de las obligaciones de publicidad activa. Las posibles discriminaciones algorítmicas que, como hemos visto, pueden venir de las personas que programen estos sistemas, de los datos empleados para entrenar al algoritmo o del propio funcionamiento del mismo, exigen transparencia interna a través del establecimiento de requisitos en su diseño y la supervisión y evaluación de su actividad durante su ciclo de vida, en particular, sobre los datos que usa y de auditoría a través de un órgano especializado e independiente. Este es el primer paso para la protección contra la discriminación.

Con carácter general, no hay que renunciar al recurso a estas herramientas siempre que los datos se empleen y el modelo se diseñe correctamente, ya que no necesariamente se traducirán en una discriminación jurídicamente relevante. La clave está en la prevención: en un buen diseño del modelo, en la calidad de los datos, así como en su evaluación en las distintas fases para comprobar si se han producido sesgos y, en su caso, cuáles han sido sus efectos, en orden a que no se repitan en el futuro. Se trataría, pues, de alcanzar una ética algorítmica que sea capaz de remover los obstáculos que plantea el desarrollo de la IA, para mejorar la libertad humana en una sociedad democrática.

La innovación tecnológica debe ser un instrumento para avanzar en un modelo de gestión que refuerce la transparencia, el control y la rendición de cuentas de las Administraciones Públicas, otorgando un protagonismo central a los ciudadanos, a su participación y al respeto a sus derechos.

V. BIBLIOGRAFÍA

Baz Lomba, C., «Los algoritmos y la toma de decisiones administrativas. Especial referencia a la transparencia», en *Revista CEF legal*, núm.243, 2021.

Boix Palop, A., «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», en *Revista de Derecho Público: Teoría y Método*, Vol.1, 2020.

Capellá Ricart, A., «Discriminación algorítmica: Límites de la regulación antidiscriminación europea y recomendaciones preliminares», en *Quaderns IEE,* Vol. 1 Núm. 2, 2022.

CARTA DE DERECHOS DIGITALES. Disponible en: https:// www.lamoncloa.gob.es/presidente/actividades/Documents/2021/140721-Carta_Derechos_Digitales_RedEs.pdf. Fecha de consulta: 19-01-2023.

Casadeús de Mingo, A., « Gobernanza de datos», en Cerrillo i Martinez, A.,(-dir.), *La Administración digital*, Dikynson, Madrid, 2022.

COMISIÓN EUROPEA, Comunicación de la Comisión al Parlamento Europeo, al Consejo Europeo, al Consejo, al Comité económico y social europeo y al Comité de las regiones, «Inteligencia artificial para Europa», COM/2018/237 final. Disponible en: https://eurlex.europa.eu/legalcontent/ES/TXT/HTML/?uri=CELEX:52018DC0237&from=ES. Fecha de consulta: 19-01-2023.

—— Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité económico y social europeo y al Comité de las regiones, «Generar confianza en la inteligencia artificial centrada en el ser humano», COM(2019) 168 final, Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:-52019DC0168&from=ES. Fecha de consulta: 23-01-2023.

—— «Libro Blanco sobre inteligencia artificial— un enfoque europeo orientado a la excelencia y a la confianza», COM(2020) 65 final. Disponible en: https://eurlex.europa.eu/legalcontent/ES/TXT/PDF/?uri=CELEX:52020DC0065. Fecha de la consulta: 23-01-2023.

—— Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (ley de inteligencia artificial) y se modifican determinados actos legislativos de la Unión Europea, COM (2021) 206 final. Disponible en: https://eur-.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb--9585-01aa75ed71a1.0008.02/DOC_1&format=PDF. Fecha de la consulta: 19-01-2023.

Cotino Hueso, L., «SyRI, ¿a quién sanciono? Garantías frente al uso de la Inteligencia Artificial y decisiones automatizadas en el sector público y la sentencia holandesa de 2020», en *La ley privacidad*, núm.4, 2020.

—— «Nuevo paradigma en la garantía de los derechos fundamentales y una nueva protección de datos frente al impacto social y colectivo de la inteligencia artificial», en

COTINO HUESO, L.,(dir.), *Derechos y garantías ante la inteligencia artificial y las decisiones automatizadas*, Aranzadi, Cizur Menor (Navarra), 2022.

Cerrillo i Martinez, A., « Actividad administrativa automatizada y utilización de algoritmos» en Castillo Blanco, F. A.*et al*, *Las política de buen gobierno en Andalucía: digitalización y transparencia*, Instituto Andaluz de Administración Pública, 2022.

Expósito Gázquez, A.,« Los derechos digitales: apertura del debate jurídico para su concreción y desarrollo» en Cerrillo i Martinez, A.(dir.), *La Administración digital*, Dykinson, Madrid, 2022.

Gamero Casado, E., «El enfoque europeo de Inteligencia Artificial», en *Revista de Derecho Administrativo- CDA,* núm.20, 2021.

GOBIERNO DE ESPAÑA, Estrategia nacional de inteligencia artificial, 2020, disponible en: https:/portal.mineco.gob.es/RecursosArticulo/mineco/ministerio/ficheros/201202_ENIA_V1_0.pdf. Fecha de consulta: 22-01-2023.

GRUPO DE TRABAJO PARA LA PROTECCIÓN DE DATOS DEL ARTICULO 29 (2017) «Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679». Disponible en: https://www.aepd.es/sites/default/files/2019-12/wp251rev01-es.pdf. Fecha de consulta: 23-01-2023.

Martin Delgado, I., «Naturaleza, concepto y régimen jurídico de la actuación administrativa», en *Revista de Administración Pública*, núm.180, 2009.

——«Transparencia y explicabilidad de la IA en el sector público» en Cerrillo et al, Aportaciones de la Red DAIA a la carta de derechos digitales. *Carta de Derechos digitales y sector público: propuestas de mejora*, Red DAIA. Diciembre 2020, https://bit.ly/3paF0H0, Fecha de consulta: 26-01- 2023.

Martin López, J. ,« «Inteligencia artificial, sesgos y no discriminación en el ámbito de la inspección tributaria», en *Crónica Tributaria* núm. 182, 2022.

Medina Guerrero, M., «El derecho a conocer los algoritmos utilizados en la toma de decisiones», en *Teoría y realidad constitucional*, núm.49, 2022.

OBSERVATORIO NACIONAL DE TECNOLOGÍA Y SOCIEDAD, Informe «Brecha digital de género». 2022. Madrid. Ministerio de Asuntos Económicos y Transformación Digital. Disponible en: https://www.ontsi.es/sites/ontsi/files/2022-04/brecha_digital_genero_2022.pdf. Fecha de la consulta:19-01-2023.

Palma Ortigosa, A., «Decisiones automatizadas en el RGPD. El uso de algoritmos en el contexto de la protección de datos», en *Revista General de Derecho Administrativo*, num.50, 2019.

PARLAMENTO EUROPEO, Resolución de 20 de octubre de 2020, con recomendaciones a la Comisión sobre un marco de aspectos éticos de la inteligencia artificial, la robótica y las tecnologías relacionadas, (2020/2012(INL), DOUE C404 6/10/2021 pp. 63-106. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=OJ:C:2021:404:FULL&from=ES. Fecha de la consulta: 19-01-2023.

Pérez Bernabeu ,B., «El principio de explicabilidad algorítmica en la normativa tributaria española: hacia un derecho a la explicación individual» en *Revista española de Derecho Financiero*, núm. 192,2021

Ponce Solé, J., «Inteligencia Artificial, Derecho Administrativo y reserva de humanidad: algoritmos y procedimiento administrativo debido tecnológico», en *Revista de Derecho Administrativo*, núm. 50, 2019.

Rallo Lombarte, A., « Una nueva generación de derechos digitales», en *Revista de Estudios Políticos*, 187, enero-marzo, 2020.

Rodriguez Arana, J.,« La buena administración como principio y como derecho fundamental en Europa», en *Misión Jurídica Revista de derecho y ciencias sociales*, Vol. 6, núm.6, 2013.

Roig i Batalla, A., *Las garantías frente a las decisiones automatizadas: del Reglamento General de Protección de Datos a la gobernanza algorítmica*, Bosch, Barcelona, 2020.

Soriano Arranz, A., «Discriminación algorítmica: garantías y protección jurídica» en Cotino Hueso, L. *Derechos y garantías ante la inteligencia artificial y las decisiones automatizadas*, Aranzadi, Cizur Menor (Navarra), 2022.

CAPÍTULO 4

DERECHOS DIGITALES, INTELIGENCIA ARTIFICIAL Y TRANSPARENCIA

Joaquín Meseguer Yebra

Coordinador del Grupo de trabajo de transparencia y acceso a la información pública de la Red de Entidades Locales por la Transparencia y Participación Ciudadana (FEMP)
Secretario ejecutivo del capítulo español de la Red Académica de Gobierno Abierto Internacional (RAGAInt)

SUMARIO

I. INTRODUCCIÓN: DEL MUNDO ANALÓGICO AL DIGITAL

La evolución de la administración automatizada y de los algoritmos y sistemas de inteligencia artificial (IA, en adelante) en los que las administraciones públicas empiezan a apoyar su actuación es tan vertiginosa que, tan solo en las semanas que han discurrido desde la celebración del seminario que ha dado lugar a esta publicación, se han tomado decisiones importantes en nuestro país. Basta solo mencionar a título de cita, más anecdótica que de otro tipo, la decisión del Gobierno español de ubicar la futura sede de la Agencia Española de Supervisión de Inteligencia Artificial en A Coruña o la elección de Sevilla como sede del Centro Europeo para la Transparencia Algorítmica (ECAT en sus siglas en inglés) por la Comisión Europea. Parece que algo se mueve en esta materia en nuestro país, lo que ya era evidente en el contexto europeo donde la IA era una inquietud en las dos últimas décadas.

Hasta la Fundación del Español Urgente (FundéuRAE) acaba de otorgar estos días el título de palabra del año a la expresión «inteligencia artificial», y cito literal, «por su importante presencia en los medios de comunicación durante estos últimos doce me-

ses, así como en el debate social, debido a los diversos avances desarrollados en este ámbito y las consecuencias éticas derivadas».

La pretensión de este trabajo, pues, es únicamente dejar apuntadas algunas de las cuestiones más controvertidas y que generan debate en torno a la transparencia de la administración algorítmica que se expusieron en el seminario «Administración Digital», celebrado en el Centro de Estudios Políticos y Constitucionales en octubre de 2022. Todas ellas con la profundidad que permite un trabajo de esta extensión y con la sola pretensión de exponer algunos de los retos a los que nos enfrentamos. En nuestra doctrina científica contamos afortunadamente con muy valiosas aportaciones doctrinales de calado y máximo rigor, como algunas a las que haré referencia en la bibliografía de este capítulo y que vienen de la mano de expertos como Andrés Boix Palop, Estrella Gutiérrez David, Juli Ponce, Gabriele Vestri, Alejandro Huergo Lora, Lorenzo Cotino Hueso y muchos y muchas más.

El punto de partida bien puede ser el reconocimiento actual de los llamados «derechos digitales» en nuestro país, que están aterrizando en nuestro derecho positivo a través de la legislación sectorial y, especialmente, ya con un enfoque más transversal, con la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. Este reconocimiento cobra mayor intensidad, aunque carente de fuerza normativa, con la aprobación de algunos documentos e instrumentos de «soft law» como es la Carta de Derechos Digitales, adoptada por nuestro Gobierno en julio de 2021 con el propósito de servir como marco referencial para garantizar los derechos de la ciudadanía en la nueva realidad digital y reconocer los retos que plantea la adaptación de los derechos actuales al entorno virtual y digital[1].

Mucho se ha hablado y se sigue haciendo sobre si nos hallamos ante nuevos derechos o, por el contrario, ante los mismos derechos del mundo analógico ya conocidos, pero en su versión digital, un debate más doctrinal que práctico en la medida que el reconocimiento y garantía efectiva de cualquier derecho pasa necesariamente por la aprobación de normas que así lo contemplen y, en el caso de derechos fundamentales, por el encaje que estos puedan tener en nuestra Constitución a la vista, también, de la interpretación que se desprenda de los tratados y acuerdos internacionales ratificados por España.

Para alguien como este autor con una visión muy focalizada en la transparencia de la gestión pública como medio para garantizar la necesaria rendición de cuentas, lo que debe quedar claro es que el «target» del desarrollo y avance tecnológico debe situarse en todo caso en las personas y en la necesidad de que, con todos los equilibrios y balances que sean precisos, la tecnología facilite el ejercicio de los derechos, pero no los limite, arrolle o fagocite. Debemos recuperar o reforzar la visión humanista y ética de

[1] Se puede acceder al texto en la siguiente url: https://www.lamoncloa.gob.es/presidente/actividades/Documents/2021/140721-Carta_Derechos_Digitales_RedEs.pdf

la tecnología, adoptar una gobernanza digital vinculante con este enfoque. Hace ya un par de años, en un documento de la Fundación Novagob sobre Retos 2021 para una Administración Innovadora, defendía una apuesta por más tecnología e innovación en la administración, pero sin olvidar empaparla, no solo de inteligencia artificial y algoritmos, sino también de ética y transparencia, que es a aquellas, como el alma al cuerpo. Esta, creo, debe ser la senda a seguir.

En este trabajo vamos a centrarnos en la «intersección» de los derechos de participación y conformación del espacio público, por un lado, y ciertos derechos digitales en entornos específicos, en concreto, los derechos ante la inteligencia artificial, derechos todos ellos mencionados en la citada Carta de Derechos Digitales. No es irrelevante ni debería pasar inadvertido, en absoluto, el uso de la preposición «ante» que emplea la Carta, lo que parece sugerir de alguna manera una voluntad de proteger los derechos de las personas ante el avance de la inteligencia artificial.

II. HACIA UNA GESTIÓN CADA VEZ MÁS AUTOMATIZADA (¿E INTELIGENTE?)

Como antes decíamos, los debates a los que estamos asistiendo en los últimos tiempos son ciertamente inquietantes, tanto como necesarios. Basta citar tres ejemplos:

- La Resolución del Parlamento Europeo, de 16 de febrero de 2017, con recomendaciones destinadas a la Comisión sobre normas de Derecho civil sobre robótica, sugiere regular a largo plazo un estatuto de persona electrónica para los robots autónomos más complejos que tomen decisiones autónomas inteligentes o interactúen con terceros de forma independiente.
- En abril de 2018 los medios de comunicación se hacían eco de la candidatura de Michihito Matsuda a las elecciones en un distrito de la ciudad de Tokio. Lo peculiar de la noticia es que se trataba de un robot operado por inteligencia artificial. La noticia podría haber quedado en la anécdota si no hubiera sido porque el aspirante quedó en tercer puesto, lo que nos lleva a preguntarnos si confiamos más en la gestión automatizada que podría llevar a cabo una máquina que la que podrían realizar nuestros congéneres humanos.
- Los representantes del proyecto AIP (The Artificial Inventor Project) solicitaron patentes en 2019 para dos invenciones en las que, en lugar de identificar a un inventor humano en los formularios, se indicó que era Dabus AI, un sistema de inteligencia artificial. Tanto la oficina de patentes del Reino Unido como de la Unión Europea consideraron que, aunque las invenciones en sí mismas pueden ser dignas de ser objeto de patente, las solicitudes debían rechazarse porque el «inventor» no era un ser humano.

Más allá de la anécdota o de lo que algunos puedan juzgar extravagante («mañana», seguramente, serán alternativas más que aceptables y factibles), lo cierto es que la administración camina actualmente hacia una gestión cada vez más automatizada para lograr ser más eficiente debido al gran volumen de datos que debe gestionar cotidianamente y, también, más objetiva. En muchos casos, sin poder cifrar a qué porcentaje nos referimos, la Administración aplica soluciones algorítmicas «regladas», simples fórmulas, para resolver un número muy importante de procedimientos que, en caso de exigir la intervención humana, ralentizarían de una forma significativa, si no fatalmente, una gestión mínimamente eficiente.

Sin entrar en tecnicismos, la revolución industrial 4.0 nos ha traído el internet de las cosas (IoT), los algoritmos (deterministas o reglados), pero también sistemas de inteligencia artificial (IA), predictivos (machine learning/deep learning), que imitan redes neuronales y que, en algún caso, son verdaderas «black boxes» de las que poco o nada se sabe sobre su funcionamiento. El proceso de toma de decisiones en la Administración ya se apoya en muchos casos en herramientas de este tipo y, en algún caso, hasta puede ser plenamente automatizado. ¿Estamos ante normas como sostiene Andrés Boix o, más bien, ante la traducción tecnológica del procedimiento administrativo para la producción de estas decisiones?

La desconexión digital en este contexto puede ser definido como el derecho que correspondería a cualquiera de exigir que la decisión que pudiera afectarle se tome por personas, por humanos. La traducción de esto la encontramos en la Carta de Derechos Digitales que garantiza a las personas que no quieran o puedan utilizar recursos digitales a elegir otras alternativas en el mundo físico que garanticen sus derechos (apartado 3.XVIII). Pero, por otra parte, la Carta también dice que quien resuelva separándose del criterio propuesto por un sistema automatizado o inteligente, deberá razonar o explicar su decisión. Esto es, la carga de la motivación se hace recaer sobre las personas cuando estas consideren que la «máquina» sugiere un modo de proceder que difiere del juicio de quienes son titulares y pueden/deben ejercer las competencias. Y todo ello en un momento como el actual en el que la norma básica que establece las reglas generales que rigen los procedimientos administrativos, la Ley 39/2015, de 1 de octubre, aún no ha determinado que los algoritmos tengan el valor de precedente administrativo como para tener que justificar por qué decidimos apartarnos de sus predicciones o «decisiones».

El panorama futuro, pues, por mucho que nos resistamos a admitirlo, apunta a que será difícil —o, incluso, poco recomendable— que quien lo desee pueda mantener un estatus analógico. Esto no significa, insistimos, que la gestión automatizada o los sistemas de IA no sean herramientas que presentan indudables ventajas y oportunidades en el campo de la gestión pública. Sería absurdo negar que en el futuro tendremos que apoyarnos necesariamente en este tipo de soluciones, tanto como obviar que estas soluciones también albergan importantes riesgos, como demuestra, solo a título de ejemplo, que la Ley francesa núm. 2019-222 de programación 2018-2022 y de refor-

ma para la justicia, prohíba la reutilización y análisis de datos de jueces y magistrados con el objeto de predecir su actuación al resolver o que ya haya algunos países que se hayan mostrado reticentes al uso de sistemas de reconocimiento facial biométrico en espacios públicos.

Esto me hace recordar inevitablemente lo que Isaac Asimov en su obra *Círculo vicioso*, publicada hace ya ocho décadas, nos quería hacer ver cuando enunciaba las tres leyes de la robótica:

- Un robot no hará nunca daño a un ser humano (o por inacción, nunca permitirá que esto suceda);
- Un robot siempre obedecerá las órdenes de los seres humanos, salvo que entren en conflicto con la primera norma;
- Un robot debe proteger su propia existencia salvo que entre en conflicto con las dos primeras normas.

III. GESTIÓN AUTOMATIZADA MOTIVADA (Y EXPLICABLE)

Contamos en la actualidad con una variedad importante (y en aumento) de algoritmos y sistemas de IA de todo tipo que tratan datos personales, aunque también conviene advertir que no todos lo hacen. Pensemos, por ejemplo, en los modelos de predicción meteorológica. No huelga hacer esta precisión por cuanto, al igual que sucede en materia de transparencia, la protección de datos personales y los efectos de su tratamiento suele ser uno de los principales escollos que nos encontramos en el abordaje de esta materia, y no siempre con la suficiente justificación.

En las actuaciones automatizadas, el resultado que arroja el algoritmo o la predicción que suministra el sistema de IA resulta ser en muchos casos parte o toda la justificación que requiere una decisión pública. La necesidad de motivar, lo sabemos, era y es un requisito en el mundo analógico según dispone el artículo 35 de la Ley 39/2015, de 1 de octubre, de Procedimiento Administrativo Común de las Administraciones Públicas. Así lo decían también las leyes que la precedieron en el siglo pasado. Esto significa que las decisiones que hoy en día se apoyan en los razonamientos, juicios o criterios que ofrecen aquellas soluciones tecnológicas deben garantizar que puedan explicarse en iguales condiciones y que se entienda la decisión adoptada. Sería inaceptable dispensar de un requisito así, más aún cuando las decisiones o su fundamentación pueda proceder de una fuente no humana. La cuestión es que, como todos los expertos advierten, hay una relación inversa entre explicabilidad y rendimiento de los modelos, tal que cuanto más sofisticados resultan ser —esto es, más valor pueden añadir a lo que la mente humana ya hace—, más difícil es saber cómo operan o actúan.

Los órganos de control en materia de transparencia ya han empezado a decirlo en «voz alta y clara». El Consejo de Estado Italiano, en su sentencia 08747/2019, de 13

de diciembre, que resuelve el recurso interpuesto contra la sentencia del Tribunal Administrativo del Lazio en el asunto que enfrentaba al Gobierno con un grupo de docentes que había cuestionado la gestión del sistema de concursos de profesorado por un algoritmo, concluye que estos sistemas deben respetar «el pleno conocimiento previo del modelo utilizado y de los criterios aplicados». Y es que, conocer el algoritmo (cómo opera a partir de unos determinados datos para obtener un resultado) permitiría identificar posibles sesgos, vulneraciones de derechos, etc., e, incluso, mejorar su funcionamiento dado que, a la vista de todos, todos podrían también de alguna forma contribuir a la corrección de posibles fallos que se detecten.

Esto no tiene una relevancia anecdótica. Todo lo contrario. Pensemos que en el funcionamiento de los algoritmos y los sistemas de IA puede haber sesgos (bias, en la nomenclatura anglosajona) de todo tipo y con impacto en diferentes momentos:

- En los datos —inputs— que utilizan aquellos o con los que se entrenan para crear patrones. Los conjuntos de datos (datasets) que se utilizan para esta tarea buscan representar el mundo real, pero la mayoría de las veces no consiguen hacerlo. O reflejan estereotipos y prejuicios, o bien, la base o muestra de datos de entrenamiento resulta no ser completa y, por este motivo, no recoge todo el universo de situaciones posibles. Esto determinará irremisiblemente que los resultados de la toma de decisión automatizada replicarán estos sesgos.

  Un buen ejemplo sería el paradigmático caso Estado de Wisconsin contra Loomis, también conocido como caso COMPAS *(*Correctional Offender Management Profiling for Alternative Sanctions), según se cite el litigio o el algoritmo. COMPAS lo utilizan las autoridades judiciales en el proceso penal norteamericano para valorar el grado de riesgo de reincidencia del sujeto y así ayudar a fijar la condena. Opera sobre la base de un análisis complejo que implica el uso de la información obtenida de una encuesta de 137 preguntas (que versan, entre otros ámbitos, sobre raza, sexo, entorno o pobreza del barrio donde se reside), divididas en varias secciones, así como sobre información relativa a los antecedentes penales individuales. Se realiza una entrevista a la persona procesada con el fin de obtener toda la información necesaria para efectuar la ponderación y determinar un puntaje del nivel de riesgo de reincidencia. Del caso concreto citado se desprendió como una de las conclusiones que las personas de raza negra tenían el doble de posibilidades que las personas blancas de ser clasificadas por error como de «alto riesgo».
- En el propio código fuente. Los algoritmos están diseñados por personas, y las personas tenemos todas nuestra propia escala de valores, prejuicios, experiencias y opinión.

  Son buenas muestras de esta modalidad de sesgos los casos DELIVEROO o SyRI. El primero aborda el caso de la plataforma de Deliveroo, una de las más populares de envío de comida a domicilio. El rider accede a la plataforma

para reservar franjas horarias de forma anticipada, pudiendo elegir en el momento de entrar tanto horarios como área o áreas disponibles. Los riders pueden entrar cada lunes para reservar sus horarios de trabajo según la puntuación que tengan en el ranking de la empresa. Los riders con mejor puntuación pueden acceder a partir de las 11:00 horas, el 25% siguiente a partir de las 15:00 horas, y el resto a partir de las 17:00 horas.

La puntuación de los riders depende de la fiabilidad y disponibilidad. El índice de fiabilidad tiene en cuenta el número de ocasiones en que el rider no ha cumplido con una sesión de trabajo previamente reservada, mientras que el índice de disponibilidad tiene en cuenta el número de veces que el rider está disponible en los horarios de mayor demanda (de 20:00 a 22:00 horas de viernes a domingo).

Pues bien, el Tribunal Ordinario de Bolonia (Italia) consideró que se había producido una discriminación indirecta contra los trabajadores de Deliveroo debido a que la plataforma actúa con una «inconsciencia y ceguera» deliberada respecto de ciertas causas (justificadas) de incumplimiento de la reserva de trabajo realizada por el rider. Entiende el Tribunal que esta discriminación se produce cuando se da el mismo trato a situaciones distintas que merecen un trato diferente. En otras palabras, aprecia la discriminación porque la aplicación valora negativamente tanto la ausencia o falta de puntualidad del rider sin discriminar si esta es caprichosa o se debe a circunstancias tales como el ejercicio del derecho de huelga, un estado de enfermedad o el cuidado de menores a cargo.

El caso SyRI (System Risk Indication) versa sobre un sistema de detección de fraudes de asistencia social utilizado por el gobierno en los Países Bajos. El resultado del procesado de datos por este sistema son informes de riesgo sobre la probabilidad de que alguien defraude a la seguridad social, pudiendo aconsejar que se lleve a cabo una investigación. Se trata de un instrumento de ayuda para las autoridades públicas encargadas de la investigación del fraude a la seguridad social, que pueden valerse de las inferencias del sistema para sus tareas de inspección y, en caso de detectar incumplimientos o fraudes, iniciar procedimientos sancionadores.

El modelo de riesgo elaborado por SyRI presentaba efectos no deseados según el Tribunal de Distrito de La Haya, al estigmatizar y discriminar a determinados ciudadanos, no solo por cantidad de información personal que recopilaba, sino también por la falta de transparencia del algoritmo y, especialmente, por el uso sesgado del instrumento, utilizado en barrios donde vivían personas con rentas bajas o zonas donde residían personas pertenecientes a minorías.

Los algoritmos pueden emplearse como fórmula de apoyo o auxilio en la toma de decisiones, pero también, incluso, pueden tomar la propia decisión, lo que denomina-

mos «automatización íntegra». El artículo 41 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público define actuación automatizada como aquel acto o actuación realizada *íntegramente* a través de medios electrónicos por una Administración en el marco de un procedimiento administrativo y en la que *no haya intervenido de forma directa un empleado público.*

De hecho, el artículo 22 del Reglamento General de Protección de Datos[2] habla de decisiones basadas íntegramente en tratamientos automatizados que produzcan efectos jurídicos o afecten a la persona de forma significativa. En estos casos, existe el derecho, con algunas excepciones, a no ser objeto de decisiones de este tipo o a exigir la supervisión/intervención humana (apartado 5.XXV.3 de la Carta de Derechos Digitales). Según la Agencia Española de Protección de Datos (AEPD), deben evitarse este tipo de sistemas y dar la opción siempre a que un operador humano pueda ignorar el algoritmo en un momento dado. Adoptar sistemas de este tipo, además, conlleva decidir a quién se imputa el acto, cuál es el régimen de impugnaciones, el régimen de responsabilidad ante eventuales daños, etc. Los sistemas de gestión automatizada ponen a prueba la teoría clásica del órgano, que tendría que adaptarse a las nuevas condiciones que impone un modelo diferente de ejercicio y, en su caso, de atribución de competencias.

Por otra parte, y retomando el debate sobre la explicabilidad, en aquellos casos en los que cualquiera sea objeto de una decisión de este tipo la AEPD considera que las personas deben poder disponer de información significativa sobre la lógica aplicada, la importancia y las consecuencias previstas y, en concreto, sobre:

- El detalle de los datos empleados para la toma de decisión, más allá de la categoría en particular, e información sobre los plazos de uso de los datos.
- La ponderación de cada uno de ellos en la toma de decisión.
- La calidad de los datos de entrenamiento y el tipo de patrones utilizados.
- Los perfilados realizados y sus implicaciones.
- Los valores de precisión o de error según la métrica adecuada para medir la bondad de la inferencia.
- La existencia o no de supervisión humana cualificada.
- La referencia a auditorías, así como la existencia de certificaciones realizadas sobre el sistema de IA.
- En el caso de que el sistema de IA contenga información sobre terceros identificables, la prohibición de tratar esa información sin legitimación y de las consecuencias de realizarlo.

[2] 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.

Luego está determinar, si es que consideramos que esta cuestión es relevante, en qué tipo de potestades o competencias debería ser más aceptable el uso de este tipo de soluciones. Las facultades que se ejercen en la administración pueden ser del todo (o en buena parte) regladas, esto es, todos o la mayor parte de sus presupuestos y condiciones estar preestablecidos en la norma y, una vez corroborados, solo tener cabida una aplicación automática de aquella. Por el contrario, si la norma puede dejar un margen abierto o libre a la apreciación subjetiva de quien ejerce la competencia, pero siempre dentro del marco jurídico. Esto último es lo que denominamos, potestades o competencias discrecionales.

La pregunta es si puede un algoritmo o un sistema de IA concretar en el caso concreto el contenido de un concepto jurídico indeterminado, resolver qué es o no equitativo o apreciar circunstancias que no estén tipificadas, estandarizadas o mecanizadas con un previo valor asignado. Esta cuestión es importante de resolver para despejar las suspicacias que el uso de estos sistemas puede suscitar y, personalmente, me recuerda a la publicidad de una conocida marca de refrescos donde se representaba una entrevista de trabajo llevada a cabo por un sistema de IA a un candidato humano. La entrevistadora concluía diciendo que no había nada que los seres humanos pudieran aportar que ellos no pudieran hacer, a lo que el joven respondía que ellos solo se actualizan, y versión a versión quedan obsoletos y necesitan de sustitución. Los seres humanos son compatibles con más de siete millones de sistemas operativos y, de una forma poética y sugerente, aseguraba que se reafirman, se reenamoran y renacen a cada instante, y eso tiene más valor que la primera vez que lo hacen. Una manera romántica de expresar los límites a los que puede enfrentarse un modelo de este tipo.

Parece haber cierto consenso en que el ámbito material en el que deben o pueden operar estas soluciones no debe ser incondicionado y que los ámbitos más reglados son los idóneos para que puedan desplegarse. La sentencia 08747/2019, de 13 de diciembre, del Consejo de Estado italiano en el asunto del algoritmo para los concursos de traslados de profesores así viene a exigirlo y también el § 35 de la Ley alemana de procedimiento administrativo cuando expresa que «un acto administrativo puede ser adoptado enteramente por órganos automáticos, siempre que así lo permita la ley *y que no exista ni discrecionalidad ni margen de apreciación*».

IV. DE LA VUELTA A LA TRANSPARENCIA Y LA EXPLICABILIDAD

Esta parece ser la línea a la que apunta en nuestro país la inflada relación de estrategias y guías, documentos de «soft law», que hablan de la necesidad de incrementar la transparencia y monitorización en el uso de estas tecnologías. Solo por hacer una referencia a las más importantes, podemos citar:

- Guía sobre adecuación al Reglamento General de Protección de Datos de tratamientos que incorporan IA. Una introducción —AEPD, febrero 2020—[3].
- España Digital 2025 —ahora 2026, después de su revisión en julio 2022, tras dos años de despliegue—[4].
- Estrategia Nacional de Inteligencia Nacional (ENIA) de noviembre de 2020 —versión 1.0—[5].
- Carta de Derechos Digitales —julio 2021—.
- Información algorítmica en el ámbito laboral. Guía práctica y herramienta sobre la obligación empresarial de información sobre el uso de algoritmos en el ámbito laboral —Ministerio de Trabajo y Economía Social, mayo 2022—[6].

Detengámonos, aunque sea solo a título de cita, en algunas de las afirmaciones que se contienen en el documento de la ENIA, para comprobar el compromiso que el gobierno español asume actualmente sobre transparencia algorítmica:

> «Adoptar decisiones de forma transparente. Es preciso que el acceso a la información de interés público esté al alcance, fomentando el gobierno abierto y permitiendo a la ciudadanía monitorizar a la Administración en las políticas que se implementen. Para ello, se mejorará la calidad de los datos aportados y su accesibilidad, fomentando la cultura de orientación al dato, utilizando algoritmos transparentes y explicables, estrechando la relación entre la Administración y la ciudadanía.
>
> Crear repositorios de datos públicos que permitan el acceso en condiciones óptimas de seguridad, legalidad, integridad confidencialidad y protección de la privacidad de los ciudadanos para desarrollar nuevas aplicaciones y oportunidades, tanto para el sector público (sistemas en el ámbito de la gestión sanitaria, la educación, la seguridad, la transición ecológica, la gestión urbana o la movilidad sostenible) como para el sector privado.
>
> » (…) la Inteligencia Artificial es útil para mejorar la transparencia y comunicación de la actividad pública en los sectores de sanidad y servicios sociales, medio ambiente y energía, justicia, transporte y logística, educación, empleo y seguridad.
>
> » Es la ciudadanía quien debe monitorizar la actividad de la Administración, sentirla más cerca y poder usar aplicaciones adaptadas y personalizadas a sus necesidades.

[3] Se puede acceder al texto en la siguiente url: https://www.aepd.es/sites/default/files/2020-02/adecuacion-rgpd-ia.pdf

[4] Se puede acceder al texto en la siguiente url: https://espanadigital.gob.es/sites/espanadigital/files/2022-07/Espa%C3%B1aDigital_2026.pdf

[5] Se puede acceder al texto en la siguiente url: https://www.lamoncloa.gob.es/presidente/actividades/Documents/2020/ENIA2B.pdf

[6] Se puede acceder al texto en la siguiente url: https://www.lamoncloa.gob.es/serviciosdeprensa/notasprensa/trabajo14/Documents/2022/100622-Guia_algoritmos.pdf

> » Debemos evaluar si nuestras normas de convivencia están adaptadas a las necesidades del momento, si es suficiente con el marco ético y jurídico que nos ha acompañado hasta hoy o qué ajustes y revisiones necesita para preservar los derechos de la ciudadanía en un mundo digital y anteponer objetivos éticos y democráticos al desarrollo de la IA.
>
> » Supervisión humana. La IA debe estar sometida a supervisión continua, y debe ser comprensible para las personas.
>
> Gobierno de los datos y sistemas. Los datos no se utilizarán para perjudicar a la sociedad, o violar los derechos fundamentales de los ciudadanos. Los datos tienen tanto un aspecto personal, como un carácter de bien público. Las normas éticas y jurídicas con las que establecer el equilibrio democrático entre ambas deberán ser profundizadas tanto en el comité ético de la IA como en la revisión y reforma legal pertinentes.
>
> Transparencia (trazabilidad). Se debe garantizar la trazabilidad de los sistemas de IA. Esto significa garantizar que las decisiones ejecutadas por sistemas algorítmicos puedan ser auditadas, evaluadas y explicadas por las personas responsables.»

Afortunadamente, el grado de vinculación no se reduce solo a documentos de esta naturaleza, sino que el derecho positivo empieza a acoger también obligaciones en este ámbito:

- La llamada ley «rider» (Ley 12/2021, de 28 de septiembre, por la que se modifica el texto refundido de la Ley del Estatuto de los Trabajadores, aprobado por el Real Decreto Legislativo 2/2015, de 23 de octubre, para garantizar los derechos laborales de las personas dedicadas al reparto en el ámbito de plataformas digitales).

  Esta ley reconoce el derecho del comité de empresa a ser informado por la empresa de los parámetros, reglas e instrucciones en los que se basan los algoritmos o sistemas de inteligencia artificial que afectan a la toma de decisiones que pueden incidir en las condiciones de trabajo, el acceso y mantenimiento del empleo, incluida la elaboración de perfiles.
- El artículo 23 de la Ley 15/2022, de 12 de julio, integral para la igualdad de trato y la no discriminación, establece que las administraciones favorecerán la puesta en marcha de mecanismos para que los algoritmos involucrados en la toma de decisiones que se utilicen en las administraciones tengan en cuenta criterios de minimización de sesgos, *transparencia y rendición de cuentas*, siempre que sea factible técnicamente. En estos mecanismos se incluirán su *diseño y datos de entrenamiento*, y abordarán su *potencial impacto discriminatorio*. Para lograr este fin, se promoverá la realización de *evaluaciones de impacto* que determinen el posible sesgo discriminatorio

  Las administraciones priorizarán la transparencia en el diseño y la implementación y la capacidad de interpretación de las decisiones. Promoverán el uso de una IA ética, *confiable* y respetuosa con los derechos fundamentales, siguiendo

especialmente las recomendaciones de la Unión Europea en este sentido, y la creación de un sello de calidad de los algoritmos.

La realidad demuestra, sin embargo, que a pesar de los compromisos formales o las obligaciones legales, las administraciones siguen arrastrando los pies cuando de transparencia algorítmica hablamos. Ni existe publicidad activa real sobre los algoritmos y modelos de IA que se utilizan, ni se hacen grandes esfuerzos por facilitar el conocimiento de su funcionamiento. Una buena muestra podemos hallarla en las resoluciones denegatorias al ejercicio del derecho de acceso a la información pública cuando se formulan solicitudes sobre esta materia:

- De los informes relativos a soluciones tecnológicas de computación inteligente adjudicados por el Centro para el Desarrollo Tecnológico Industrial a dos empresas (Resolución de la Secretaría General de Innovación de 14 de diciembre de 2021), fundándola en la protección de los intereses económicos y comerciales, y de la protección propiedad intelectual e industrial[7].
- Del desarrollo de inteligencia artificial para la planificación de la actuación inspectora en materia laboral, detección y persecución de infracciones en el orden social (Resolución de la Dirección del Organismo Estatal de Inspección de Trabajo y Seguridad Social de 8 de agosto de 2022)[8], motivándola en la prevención, investigación y sanción de los ilícitos penales, administrativos o disciplinarios y las funciones administrativas de vigilancia, inspección y control.
- De la documentación técnica y código fuente del framework MOVA/MOVA2 con el que se realizan todas las apps móviles de la Comunidad de Madrid (Resolución de la Consejera Delegada de la Agencia para la Administración Digital de la Comunidad de Madrid de 14 de junio de 2022)[9], fundándola en que la solicitud es abusiva y la denegación resulta justificada y proporcionada por concurrir un interés público en el mantenimiento de los servicios públicos y en el respeto de los derechos de propiedad intelectual.

V. UNA VEZ MÁS, LOS CONSEJOS Y COMISIONADOS DE TRANSPARENCIA AL RESCATE

En efecto, son los Consejos y Comisionados de transparencia estatal y autonómicos quienes están defendiendo con mayor tesón la apertura de esta información sobre

[7] https://www.ciencia.gob.es/dam/jcr:fa01b67b-8fb6-439b-b79c-3600d596a1c5/Resolucion_S_062688.pdf

[8] https://www.mites.gob.es/es/publica/resoluciones-denegatorias/RESOLUCION_65400.pdf

[9] https://www.comunidad.madrid/transparencia/sites/default/files/servicios/documentos/resoluciones/18-open-00012.4-2022.pdf

la base de experiencias comparadas como la francesa. La CADA (Commission d'accès aux documents administratifs) ha obligado en varias ocasiones a facilitar el código fuente de algunas aplicaciones tributarias, de la plataforma PARCOURSUP para la preinscripción en el primer curso de enseñanza universitaria, del programa utilizado por el Fondo Nacional de Susidio Familiar para el cálculo de determinadas prestaciones familiares y sociales, etc., y tanto el Código de Relaciones entre el Público y la Administración[10] como la Ley francesa para una República Digital[11] han tomado el testigo a nivel normativo.

En nuestro país este papel lo han ejercido esencialmente el Consejo de Transparencia y Buen Gobierno estatal (CTBG, en adelante) y la Comisión de Garantía del Derecho de Acceso a la Información Pública de Cataluña (GAIP, en adelante). Citamos solo a título de ejemplo algunas de las resoluciones de estos comisionados y su estado de cumplimiento por parte de la administración «reclamada»:

- Resolución RT/0379/2020, de 10 de noviembre, del CTBG: documentos sobre el sistema de cálculo de la asignación para el funcionamiento a los centros públicos docentes de Madrid y sobre los criterios objetivos utilizados para valorar las necesidades de gasto (estima la reclamación y aparece como cumplida por la Comunidad de Madrid)[12].
- Resolución R/0058/2021, de 20 de mayo, del CTBG: algoritmo con el que el programa de cálculo de la pensión realiza los porcentajes de cálculo correspondientes a los años completos de servicio efectivo (estima la reclamación y aparece como cumplida por la Administración del Estado)[13].

Merece la pena reproducir parte del texto de su fundamentación jurídica: «En el contexto actual de progresivo desarrollo e implantación la administración electrónica y uso creciente de la inteligencia artificial, los algoritmos están adquiriendo una rele-

[10] El artículo R311-3-1-2 establece que la administración debe comunicar a la persona sujeta a una decisión individual adoptada sobre la base de un tratamiento algorítmico, a petición de esta, en forma inteligible y sin vulnerar los secretos protegidos por la ley, la siguiente información:

1° El grado y modo de contribución del procesamiento algorítmico a la toma de decisiones;
2° Los datos tratados y sus fuentes;
3° Los parámetros de tratamiento y, en su caso, su ponderación, aplicados a la situación del interesado;
4° Las operaciones realizadas por el tratamiento.

[11] La Ley núm. 2016-1321 de 7 de octubre de 2016 para una República Digital introduce los códigos fuente en la lista de documentos administrativos sujetos al derecho de acceso y también prevé la publicación en línea de las normas que definan los principales procesamientos algorítmicos utilizados en el desempeño de las competencias de los sujetos obligados por la ley cuando sean la base de decisiones individuales.

[12] https://www.consejodetransparencia.es/ct_Home/dam/jcr:663bd7fc-7222-4664-9e47-7661c0a40e32/RT_0379_2020.pdf

[13] https://www.consejodetransparencia.es/ct_Home/dam/jcr:445a5ac9-c09a-4163-bf72-2a407aec15e4/R-0058-2021-bis.pdf

vancia decisiva, a la vez que se incrementa su complejidad. Pueden sustentar la toma de decisiones públicas o, directamente, ser fuente de decisiones automatizadas con consecuencias muy relevantes para las personas. Esta evolución está generando una creciente demanda ciudadana de transparencia de los algoritmos utilizados por las Administraciones públicas como condición inexcusable para preservar la rendición de cuentas y la fiscalización de las decisiones de los poderes públicos y, en último término, como garantía efectiva frente a la frente a la arbitrariedad o los sesgos discriminatorios en la toma de decisiones total o parcialmente automatizadas.

Mientras no se instauren otros mecanismos que permitan alcanzar los fines señalados con garantías equivalentes —como podrían ser, por ejemplo, auditorías independientes u órganos de supervisión—, el único recurso eficaz a tales efectos es el acceso al algoritmo propiamente dicho, a su código, para su fiscalización tanto por quienes se puedan sentir perjudicados por sus resultados como por la ciudadanía en general en aras de la observancia de principios éticos y de justicia».

- Resolución RT/0253/2021, de 19 de noviembre, del CTBG: código fuente de la aplicación utilizada para el sorteo de tribunales asociado a procesos selectivos de personal docente en la Comunidad de Madrid (estimada y actualmente en vía contencioso-administrativa)[14].

  El CTBG descarta que la petición sea abusiva y considera que «en la medida en que esa aplicación informática tiene una participación en la toma de una decisión pública no cabe considerar la solicitud como no justificada con la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno».
- Resolución RT/0748/2021, del CTBG: código fuente asociado al algoritmo de la aplicación utilizada para la admisión de alumnos para el curso 2021/2022 en la Comunidad de Castilla-La Mancha (estimada y aparece cumplida).

  La Administración ya había facilitado parte del código fuente y una descripción del algoritmo (pseudocódigo).
- R/0007/2023, de 11 de enero, del CTBG: copia el código fuente asociado al algoritmo de cálculo de días cotizados a la Seguridad social (estimada y a la fecha de revisión de este artículo no existe información publicada por el CTBG sobre su cumplimiento).

  Ya se había suministrado por el SEPE información relativa a la forma de cálculo de los días.
- Resoluciones de 21/9/2016 y 200/2017, de 21 de junio, de la GAIP: acceso al algoritmo para la selección de miembros de tribunales de las pruebas de acceso a la universidad.

[14] https://www.consejodetransparencia.es/ct_Home/dam/jcr:ddb7deb0-76fd-46cd-bf14-3b14f3f-3dcc7/RT_0253_2021.pdf

Según la GAIP, conocer el algoritmo es imprescindible, por ejemplo, para garantizar la proporción entre hombres/mujeres, profesores de universidad/de bachillerato, etc., que exige la normativa. Se trata de un algoritmo «reglado» sin que se comprenda el interés en ocultarlo so pretexto de la confidencialidad. La Comisión estima el acceso, pero lo restringe a la finalidad expresada en la solicitud, «prohibiendo» la difusión del algoritmo y el uso sin permiso de su titular (Consejo Interuniversitario de Cataluña).

- Resolución 93/2019, de 22 de febrero, de la GAIP: reafirma el carácter de información pública de los algoritmos o bases de datos informáticas.
- Resolución 1023/2021, de 18 de noviembre, de la GAIP: archiva la reclamación por pérdida sobrevenida del objeto del procedimiento (y, por tanto, por satisfacción del derecho de acceso) ante la denegación del acceso al informe técnico que describía el análisis estadístico realizado para establecer la fórmula de cálculo de la base imponible del impuesto sobre las emisiones de dióxido de carbono de vehículos de tracción mecánica.

La transparencia, el derecho de acceso a la información pública o las exigencias mínimas de explicabilidad algorítmica, como sucede con cualquier otro derecho, no son absolutos y tienen también sus lógicas limitaciones y condiciones. Entre las que son alegadas y, en algún caso, tomadas en consideración están la protección de la propiedad intelectual e industrial o los secretos comerciales (integrantes del límite de los intereses económicos y comerciales o la confidencialidad). Directamente conectado con este límite, surge el interesante debate sobre la pertinencia de aplicarlo en productos desarrollados «indoor» por la propia Administración pública o en aquellos supuestos en los que es titular de los derechos de explotación de estas soluciones. Aunque el debate excede del contenido de este capítulo, se trata de una línea de trabajo muy interesante que debería tener solución en la legislación patrimonial y de contratos de las administraciones públicas. A este respecto, resulta muy interesante la fundamentación dada por la Abogacía General del Estado en su escrito de oposición al recurso de apelación presentado por Civio frente a la sentencia núm. 143/2021, de 30 de diciembre, del Juzgado Central de lo Contencioso-Administrativo núm. 8 en el conocido caso BOSCO.

También la protección de la seguridad pública figura entre los límites invocados más a menudo. Hay decisiones de la CADA francesa que deniegan el acceso al código fuente del Sistema de Alerta y de Información de la Población, que permite notificar mensajes de alerta ante sospecha de eventuales atentados o eventos excepcionales de seguridad civil, o de la aplicación ALICEM, que permite el acceso a servicios públicos en línea mediante la autentificación certificada de identidad por reconocimiento facial biométrico.

En el caso español, no se ha apreciado riesgo para este límite en los casos en los que se ha planteado el acceso a algoritmos o códigos fuente, básicamente por falta de argu-

mentación de las resoluciones denegatorias, pero en el caso BOSCO, antes mencionado, sí lo ha apreciado el juzgado central de lo contencioso-administrativo haciendo suyas las consideraciones del Centro Criptológico Nacional.

VI. PROPUESTAS PARA AVANZAR EN TRANSPARENCIA ALGORÍTMICA Y DE LOS SISTEMAS DE IA

Sin duda, es buen punto de partida la posición que ha ido forjándose sobre estos temas en la Unión Europea, que actúa aquí como un verdadero «tractor» de los cambios adoptados por parte de los estados miembros. El Reglamento General de Protección de Datos, como ya vimos, establece determinadas restricciones a los tratamientos cuando sean íntegramente automatizados y produzcan efectos jurídicos o afecten a las personas de forma significativa.

También son dignas de tener muy en cuenta, entre otras muchas referencias, las Directrices éticas para una IA fiable del Grupo Independiente de Expertos de Alto Nivel sobre IA creado por la Comisión Europea (abril 2019) y el Reglamento (UE) 2019/1150 del Parlamento Europeo y del Consejo, de 20 de junio de 2019, sobre el fomento de la equidad y la transparencia para los usuarios profesionales de servicios de intermediación en línea, que dispone que los titulares de las plataformas y motores de búsqueda deben dar publicidad a los parámetros principales de funcionamiento de sus algoritmos de prelación de ofertas.

El Parlamento Europeo también ha sido prolífico en resoluciones sobre esta materia. Podemos destacar la Resolución de 6 de octubre de 2021 sobre la IA en el Derecho Penal y su uso por autoridades judiciales y policiales en asuntos penales, que alude a que estas herramientas deben respetar los principios de rendición de cuentas, transparencia, no discriminación y explicabilidad, o su otra Resolución de 3 de mayo de 2022, sobre la inteligencia artificial en la era digital.

Y, finalmente, encima de la mesa está la propuesta de la Comisión para la aprobación de un Reglamento de normas armonizadas sobre inteligencia Artificial (Ley de Inteligencia Artificial), en la que se plantea la necesidad de que se informe individualmente de qué decisiones se toman con base en algoritmos de una forma similar a como se formula en el ya citado Código francés de Relaciones entre el Público y la Administración.

Ya en nuestro país, sería necesario empezar por mejorar la publicidad activa de esta información, dado que, salvo la excepción que se dirá, es un espacio yermo y por estrenar en España. Podría comenzarse por publicar siquiera la relación de los algoritmos que maneja la Administración, en qué procesos operan, cuáles son sus reglas esenciales, etc. Por lo general nos enteramos de estos algoritmos por las noticias, dada la gran dificultad de localizar las adjudicaciones para realizar este tipo de desarrollos en la plataforma de contratación del sector público (hablamos de soluciones a ejecutar por parte de terceros).

Ya la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común y, en términos muy parecidos, la Ley 11/2007, de 22 de junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos, ambas derogadas, establecían que «los programas y aplicaciones electrónicos, informáticos y telemáticos que vayan a ser utilizados por las Administraciones Públicas para el ejercicio de sus potestades, habrán de ser previamente aprobados por el órgano competente, quien deberá difundir públicamente sus características». En su lugar, el artículo 157.2 de la ya citada Ley 40/2015, de 1 de octubre, prevé que las aplicaciones desarrolladas por las Administraciones o que hayan sido objeto de contratación y de cuyos derechos de propiedad intelectual sean titulares, podrán ser declaradas como fuentes abiertas, cuando de ello se derive una mayor transparencia en el funcionamiento de la Administración Pública o se fomente con ello la incorporación de los ciudadanos a la Sociedad de la información.

La reciente Ley 1/2022, de 13 de abril, de Transparencia y Buen Gobierno de la Comunitat Valenciana, obliga ya a publicar la relación de sistemas algorítmicos o de inteligencia artificial que tengan impacto en los procedimientos administrativos o la prestación de los servicios públicos con la descripción de manera comprensible de su diseño y funcionamiento, el nivel de riesgo que implican y el punto de contacto al que poder dirigirse en cada caso, de acuerdo con los principios de transparencia y explicabilidad (entrará en vigor en mayo de 2023).

En España ha habido hasta la fecha muy pocas decisiones de liberar el código de aplicaciones para la gestión, lo que permitiría que las aplicaciones u algoritmos evolucionasen con aportaciones de expertos o se corrigieran errores, como ya advertimos. Un ejemplo, aunque llegó tarde, fue la aplicación Radar COVID.

La Oficina Digital y de Datos británica ha publicado aproximadamente hace un año un estándar (no vinculante) de transparencia algorítmica dirigido a las entidades del sector público en el que se incluye una plantilla para ayudar a estas organizaciones a dar una información estándar sobre cada sistema de inteligencia artificial. En esta plantilla se incluyen dos contenidos:

a) Descripción no técnica del sistema: el porqué de su utilización, cómo funciona y qué problema trata de resolver.
b) Información más técnica: quién es el responsable y titular, para qué se ha diseñado, cómo influye en la toma de decisiones, si está supervisada por humanos, su impugnación, datos que utiliza, evaluaciones de impacto realizadas, descripción de riesgos y acciones previstas para mitigarlos.

La Ley francesa nº 216-1321 (2016) para una República numérica (o Digital), ya citada en este trabajo, y el reglamento de 2017 que la desarrolla, recordemos, ya hablan de la necesidad de informar no solo personalmente sino de difundir públicamente las principales operaciones algorítmicas con un cierto detalle descriptivo de en qué consisten.

En el ámbito local, los ayuntamientos de Amsterdam o Helsinki están publicando el registro de algoritmos —la mayor parte de ellos son chatbots— que utilizan (por ejemplo, multas de aparcamiento, detección de alquileres turísticos ilegales, recogida de residuos, detección de personas en riesgo de pobreza, alerta de aglomeraciones de personas, situaciones de tráfico peligrosas, gestión de los fondos bibliotecarios, etc.). Muchos de estos proyectos se pueden consultar en el Atlas del Observatorio Global de Inteligencia Artificial Urbana[15]. En nuestro país destaca especialmente el Ayuntamiento de Barcelona, que el pasado 23 de diciembre ha publicado en su Gaceta Municipal el Protocolo de Definición de metodologías de trabajo y los protocolos para la implementación de sistemas algorítmicos. En abril de 2023, el Ayuntamiento crea el Consejo Asesor en Inteligencia Artificial, Ética y Derechos Digitales para asistir y asesorar el consistorio en el uso de la inteligencia artificial y proponer actuaciones y proyectos con el objetivo de convertir Barcelona en una ciudad referente del humanismo tecnológico.

VII. OTRAS MEDIDAS Y RETOS DE ESPAÑA DIGITAL 2026

La estrategia citada que se ha visto recientemente revisada comprende diferentes acciones en las que debemos seguir trabajando si queremos realmente avanzar en transparencia algorítmica. Alguna de ellas ya está ejecutada y finalizada como es la constitución en julio de 2020 del Consejo Asesor de Inteligencia Artificial, de cuya actuación, sin embargo, poco o nada se sabe (nos referimos a informes o documentos elaborados por él). También hemos progresado en la creación de la Agencia Española de Supervisión de la Inteligencia Artificial, ya con dotación presupuestaria y sede, como advertíamos al inicio de este capítulo, adscrita a la Secretaría de Estado de Digitalización e Inteligencia Artificial.

En junio de 2022 nuestro país ha presentado en Bruselas junto con autoridades de la Comisión Europea un proyecto piloto para la creación de un sandbox regulatorio para el despliegue de la futura Ley de Inteligencia Artificial de la Unión Europea. La finalidad es desarrollar guías prácticas y herramientas que apoyen a las entidades que desarrollan IA de alto riesgo con el fin de facilitar el cumplimiento de los requisitos del futuro reglamento y generar guías de supervisión y auditoras para las futuras autoridades competentes de vigilancia de mercado. El mes de diciembre pasado, el grupo parlamentario socialista en el Congreso de los Diputados presentó, además, una proposición no de ley para que se regule la creación de estos «laboratorios». Y a finales de mayo de 2023, finalizó la consulta pública previa formulada por el Ministerio de Economía y Transformación Digital para la aprobación de un real decreto que regule este sandbox.

[15] https://gouai.cidob.org/atlas/

Otras medidas interesantes son:

- La adopción de un Plan de protección específico para colectivos vulnerables en IA y un Plan de sensibilización y confianza hacia la IA, desarrollando estudios bianuales.
- La creación del Observatorio del impacto social y ético de los algoritmos (OBISAL), que realizará evaluaciones que permitan generar recomendaciones y buenas prácticas.
- La creación de un Sello de IA confiable para los productos y servicios IA que no sean de alto riesgo. Debe incluir la creación de una colección de herramientas (toolkit) que guíen el diseño de tecnologías de conformidad con los criterios recomendados por el sello.

Al margen de estas iniciativas, debe trabajarse en auditorías independientes que monitoricen periódicamente los sistemas para garantizar la inexistencia de sesgos, auditorías que validen los modelos y documenten los métodos y resultados. También la creación de certificaciones y sistemas de autorregulación que fijen códigos éticos o de conducta, similares a los sistemas de compliance, pero en este ámbito. En octubre pasado saltaba la noticia de que Adigital (Asociación Española de la Economía Digital), en colaboración con la Fundación Eticas y con el apoyo de Blablacar, Cabify, Fintonic y Holaluz, había comenzado el diseño de una certificación de transparencia algorítmica para empresas. El objetivo es diseñar mecanismos que garanticen que las empresas certificadas se comprometen a aportar información sobre los sistemas de IA que utilizan, para que su uso sea más transparente y responsable.

En el sustrato de todos estos mecanismos, hay otras acciones previas, de mayor calado y que exigen un compromiso de todas las áreas. Una de ellas es la educación digital de toda la población, pero especialmente de las personas y colectivos en situación de riesgo de exclusión, menores y mayores, pero también la mejora del marco normativo de la reutilización de la información pública, los datos abiertos. Como ya sabemos, llegamos nuevamente tarde a la transposición de la última directiva sobre esta materia que, finalmente, ha tenido que realizarse por vía urgente (Real Decreto-ley 24/2021, de 2 de noviembre). La creación de repositorios de datos compartidos y la mejora del acceso a ellos permitirá que la tarea de entrenamiento de los modelos de IA y sus resultados sean cada vez mejores.

VIII. BIBLIOGRAFÍA

Transparencia algorítmica buenas prácticas y estándares de transparencia en el proceso de toma de decisiones automatizadas. Consejo para la Transparencia de Chile, octubre 2020.

Arellano Toledo, W. «El derecho a la transparencia algorítmica en big data e inteligencia artificial». Revista General de Derecho Administrativo (Iustel), núm. 50, enero 2019.

Boix Palop, A. «Transparencia en la utilización de inteligencia artificial por parte de la Administración». El Cronista del Estado Social y Democrático de Derecho, núm. 100, septiembre 2022.

Capdeferro Villagrasa, O. «La inteligencia artificial del sector público: desarrollo y regulación de la actuación administrativa inteligente en la cuarta revolución industrial». Revista de Internet, Derecho y Política núm. 30, marzo 2020.

Cotino Hueso, L. «Sistemas de inteligencia artificial con reconocimiento facial y datos biométricos. Mejor regular bien que prohibir mal». El Cronista del Estado Social y Democrático de Derecho, núm. 100, septiembre 2022.

——«Qué concreta transparencia e información de algoritmos e inteligencia artificial es la debida». *Revista Española de la Transparencia,* núm. 16 (primer semestre, enero-junio 2023).

Fernández Aller, C. «La Carta de Derechos Digitales de España. desafíos pendientes». Revista de Privacidad y Derecho Digital, núm. 25, enero-marzo 2022.

Fuertes López, M. «Reflexiones ante la acelerada automatización de actuaciones administrativas». Revista Jurídica de Asturias, núm. 45/2022.

González López, E. «Los derechos digitales fundamentales: ¿es necesaria su reconfiguración en el ordenamiento jurídico?». Revista de Derecho Administrativo, núm. 20, 2021.

Gutiérrez David, M. E. «Administraciones inteligentes y acceso al código fuente y los algoritmos públicos. Conjurando riesgos de cajas negras decisionales». Revista Derecom, núm. 30, marzo-septiembre 2021.

Huergo Lora, A. «El uso de algoritmos y su impacto en los datos personales». Revista de Derecho Administrativo, núm. 20, 2021.

——«Gobernar con algoritmos, gobernar los algoritmos». El Cronista del Estado Social y Democrático de Derecho, núm. 100, septiembre 2022.

Mendilibar Navarro, P. «La aplicación de sistemas algorítmicos en el sector público: la actuación administrativa automatizada y las predicciones algorítmicas». Derecho Digital e Innovación, núm. 13, julio-septiembre 2022.

Moreno Brenes, P. «La dictadura del algoritmo: el derecho como respuesta». Diario La Ley, núm. 10166, 9 de noviembre de 2022.

Ponce Solé, J. «Inteligencia artificial, Derecho administrativo y reserva de humanidad: algoritmos y procedimiento administrativo debido tecnológico». Revista General de Derecho Administrativo (Iustel), núm. 50, enero 2019.

——«Reserva de humanidad y supervisión humana de la Inteligencia artificial». El Cronista del Estado Social y Democrático de Derecho, núm. 100, septiembre 2022.

Presno Linera, M. A. «Fundamentales e inteligencia artificial: una aproximación». Revista Jurídica de Asturias, núm. 45/2022.

——«Derechos fundamentales e inteligencia artificial en el estado social, democrático y digital de Derecho». El Cronista del Estado Social y Democrático de Derecho, núm. 100, septiembre 2022.

Soto Bernabeu, L. «La importancia de la transparencia algorítmica en el uso de la inteligencia artificial por la administración tributaria». Crónica Tributaria, núm. 179/2021.

Vestri, G. «La inteligencia artificial ante el desafío de la transparencia algorítmica. Una aproximación desde la perspectiva jurídico-administrativa». Revista Aragonesa de Administración Pública núm. 56, 2021.

Villanueva Turnes, A. «La inteligencia artificial: Regulación y límites en el sector público». Revista española de Derecho Administrativo, núm. 221, julio-septiembre 2022.

CAPÍTULO 5

LA TRANSPARENCIA ALGORÍTMICA EN EL SECTOR PÚBLICO

Manuel Medina Guerrero

Catedrático de Derecho Constitucional. Universidad de Sevilla

SUMARIO

I. INTRODUCCIÓN.LA GARANTÍA DE LA TRANSPARENCIA ALGORÍTMICA EN EL CONSTITUCIONALISMO DIGITAL

Desde hace algún tiempo, la noción de «constitucionalismo digital» ha adquirido carta de naturaleza para designar las medidas que se han adoptado —o deberían tomarse— para hacer frente a los retos que la sociedad algorítmica plantea en el reparto y delimitación de poderes tanto públicos como privados. Medidas que en última instancia están orientadas a la salvaguarda de los propios derechos de la ciudadanía frente a la enorme potencialidad intrusiva que supone para los mismos la toma de decisiones automatizadas. En este contexto, el término «constitucionalismo» se emplea en un sentido muy amplio —alejado de la estricta conexión con la Constitución como norma escrita—, toda vez que abarca la totalidad de las normas que organizan el poder en general e, incluso, se vinculan a dicho concepto textos o documentos que no son genuinas normas jurídicas, sino *soft law*[1].

Sea como fuere, un integrante esencial de ese «constitucionalismo digital» lo conforma el reconocimiento de específicos derechos digitales a favor de la ciudadanía[2], de entre los cuales descuella el de conocer los tratamientos automatizados de datos de los que podamos ser objeto.

Así se apunta ya en la pionera Declaración italiana de derechos de internet, aprobada por la Comisión para los derechos y deberes en internet de la Cámara de Diputados el 28 de julio de 2015, en donde —siguiendo muy de cerca la normativa europea en materia de protección de datos personales— se reconoce el derecho de todas las personas de conocer las modalidades técnicas de tratamiento de datos que les afecten (art. 6.1), así como la obligación de poner en conocimiento de los afectados el empleo de algoritmos (art. 9.2).

Pero, sin duda, fue la Ley francesa nº 2016/1321, de 7 de octubre, por una República digital, la que supuso un cambio sustancial en el tratamiento de la cuestión, al abandonar el terreno de la *mera* declaración de principios programáticos para pasar a configurar verdaderos derechos jurídicamente exigibles[3]. Dado que tendremos que volver de forma recurrente a la normativa francesa más adelante, bastará ahora con mencionar que esta Ley vino a modificar el «Código de relaciones entre el público y la administración» a fin de incluir expresamente al «código fuente» entre los documentos sujetos al derecho de acceso a la información pública (artículo L. 300-2), estableciendo

[1] Así, por ejemplo, el constitucionalista Lawrence LESSIG aclara ya al comienzo de su libro que emplea el término «Constitución» al modo británico, esto es, entendido como una «*arquitectura*… que estructura y limita el poder jurídico y social a fin de proteger *valores* fundamentales -principios e ideas que van más allá de los compromisos de la política habitual» (*Code and other laws of cyberspace*, Basic Books, New York, 1999, p. 5).

[2] Celeste, E., *Digital Constitutionalism. The Role of Internet Bill of Rights*, Routledge, Abingdon, 2023.

[3] En este sentido, Rallo Lombarte, A., «Una nueva generación de derechos digitales», en: *Revista de Estudios Políticos*, núm. 187, 2020, p. 110.

asimismo la obligación de dar determinada información a los afectados cuando son objeto de una decisión administrativa basada en un tratamiento algorítmico (artículo L. 311-3-1).

A partir de entonces, sea ya bajo la forma de declaración programática de derechos o como derechos efectivamente tutelados, lo cierto es que los diferentes documentos que se han ido aprobando en la materia en el ámbito europeo contemplan el acceso a la información como un eje central de las garantías de la ciudadanía frente a la creciente utilización de la inteligencia artificial.

En esta línea, la muy destacable Carta Portuguesa de Derechos Humanos en la Era Digital (aprobada por la Ley nº 27/2021, de 17 de mayo)[4], tras exigir que en la utilización de la inteligencia artificial se garantice «un justo equilibrio entre los principios de explicabilidad, de seguridad, de transparencia y de responsabilidad» (artículo 9.1), impone que se comunique a los afectados las decisiones con impacto significativo que se adopten mediante el uso de algoritmos (art. 9.2). Y ya concretamente al regular los derechos digitales frente a la Administración pública, se menciona el derecho a obtener información digital relativa a procedimientos y actos administrativos [artículo 19 b)].

Y, a nivel de la Unión Europea, la reciente Declaración Europea sobre los Derechos y Principios Digitales para la Década Digital[5] incluye entre los compromisos el de asegurar «la transparencia en el uso de los algoritmos y la inteligencia artificial» (Capítulo III: Libertad de elección).

En lo que a España concierne, habida cuenta de que en el listado de derechos digitales contenido en el Título X de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantías de derechos digitales (en adelante, LOPDGDD), ninguna mención se hace a la transparencia algorítmica, no se cuenta al respecto con más referencias expresas de alcance general que las que proporciona la Carta de Derechos Digitales de España (2021). Carta que, aun recogiendo interesantes y abundantes consideraciones en torno a este asunto según veremos a continuación, no sirve más que como pauta orientadora para los poderes públicos, por lo que son muy libres de llevar a efecto, o no, en la práctica el catálogo de recomendaciones que contiene.

Pese a este notabilísimo condicionante, la Carta esboza un horizonte en el que los derechos y obligaciones de información en este ámbito resultan enormemente potenciados en comparación con el escenario normativo hoy vigente. Ciñéndonos a las previsiones que guardan más estrecha relación con el tema que nos ocupa, debe notarse que la Carta dedica enteramente su artículo XVIII a los «Derechos digitales de la ciudadanía en sus relaciones con las Administraciones Públicas». Tras proclamar el

[4] Para más detalles, consúltese Soares Fariño, D., «The Portuguese Charter of Human Rights in the Digital Age: a legal appraisal», en: *Revista Española de la Transparencia*, núm. 13, 2021, pp. 85-101.

[5] Comisión Europea, Bruselas, 26 de enero de 2022 COM (2022) 28

principio de transparencia como eje rector de la actuación de la Administración digital y subrayar en consecuencia la necesidad de garantizar el derecho de acceso a la información pública y la publicidad activa (apartado segundo), su apartado sexto procede ya a delimitar los concretos derechos digitales que asisten a la ciudadanía en esta esfera. Especialmente reseñables a los efectos de este trabajo son los consagrados en las letras b) y c), a saber, por una parte, el derecho a «[l]a transparencia sobre el uso de instrumentos de inteligencia artificial y sobre su funcionamiento y alcance en cada procedimiento concreto y, en particular, acerca de los datos utilizados, su margen de error, su ámbito de aplicación y su carácter decisorio o no decisorio»[6]. Y, por otro lado, el derecho a «[o]btener una motivación comprensible en lenguaje natural de las decisiones que se adopten en el entorno digital, con justificación de las normas jurídicas relevantes, tecnología empleada, así como de los criterios de aplicación de las mismas al caso»; al que se añade a continuación el derecho del interesado «a que se motive o se explique la decisión administrativa cuando esta se separe del criterio propuesto por un sistema automatizado o inteligente»[7].

Y, por último, el apartado séptimo de este artículo XVIII establece que «[s]erá necesaria una evaluación de impacto en los derechos digitales en el diseño de los algoritmos en el caso de adopción de decisiones automatizadas o semiautomatizadas».

El artículo XVIII de la Carta recoge, pues, en sus apartados sexto y séptimo —junto a alguna pura remisión al legislador, como sucede con el acceso al código fuente— un extenso listado de derechos y garantías, algunos de los cuales evocan directamente reglas e instituciones establecidas en el Reglamento General de Protección de Datos (prohibición de no adoptar decisiones totalmente automatizadas salvo que lo autorice el legislador estatal con las necesarias garantías, evaluaciones de impacto, etc.).

Asimismo hemos de hacernos eco del artículo XXV que la Carta encomienda a los «Derechos ante la inteligencia artificial», toda vez que se reiteran los compromisos en materia de transparencia. Más concretamente, su apartado segundo establece al respecto: «En el desarrollo y ciclo de vida de los sistemas de inteligencia artificial: a) Se deberá garantizar el derecho a la no discriminación cualquiera que fuera su origen, causa o naturaleza, en relación con las decisiones, uso de datos y procesos basados en inteligencia artificial. b) Se establecerán condiciones de transparencia, auditabilidad, explicabi-

[6] Junto a este derecho, la letra b) del apartado sexto del artículo XVIII prevé que «[l]a ley podrá regular las condiciones de transparencia y el acceso al código fuente, especialmente con objeto de verificar que no produce resultados discriminatorios».

[7] Los otros derechos mencionados en este apartado sexto que no tienen una relación directa con el tema analizado son el derecho a que «las decisiones y actividades en el entorno digital respeten los principios de buen gobierno y el derecho a una buena Administración digital, así como los principios éticos que guían el diseño y los usos de la inteligencia artificial» (a); y el derecho a que «la adopción de decisiones discrecionales quede reservada a personas, salvo que normativamente se prevea la adopción de decisiones automatizadas con garantías adecuadas» (d).

lidad, trazabilidad, supervisión humana y gobernanza. En todo caso, la información facilitada deberá ser accesible y comprensible. c) Deberán garantizarse la accesibilidad, usabilidad y fiabilidad.» [8]

En resumidas cuentas, la Carta contiene un más que razonable catálogo de derechos frente a los sistemas automatizados de toma de decisiones empleados por las Administraciones públicas. Su finalidad es, obviamente, la de servir de orientación y criterio a las diferentes Administraciones que decidan avanzar en la senda de un empleo razonable de las decisiones basadas en algoritmos[9]. Naturaleza de pauta o línea directriz que la Carta quiso reforzar explícitamente respecto del nivel de gobierno estatal cuando aclara su «Eficacia» en el artículo XXVIII: «El Gobierno adoptará las disposiciones oportunas, en el ámbito de sus competencias, para garantizar la efectividad de la presente Carta».

En el último apartado del trabajo comprobaremos en qué medida las propuestas de la Carta han ido abriéndose paso en la práctica con motivo de su recepción en normas jurídicamente exigibles.

Pero antes —claro está— tendremos que examinar cuál es el nivel de transparencia algorítmica en el sector público que ya había alcanzado nuestro ordenamiento en virtud de los dos grandes bloques normativos que inciden en la materia: los que regulan la protección de datos personales, por una parte, y la transparencia de las Administraciones públicas, por otro lado[10].

---

[8] Y su apartado tercero concluye con el reconocimiento de determinados derechos: «Las personas tienen derecho a solicitar una supervisión e intervención humana y a impugnar las decisiones automatizadas tomadas por sistemas de inteligencia artificial que produzcan efectos en su esfera personal y patrimonial.»

[9] La Carta dedica su artículo XXVII a la «Garantía de los derechos digitales», en donde claramente se refleja su naturaleza de *soft law* (remisiones a la legislación vigente, compromisos de que se promoverán actuaciones, etc.): «1. Todas las personas tienen derecho a la tutela administrativa y judicial de sus derechos en los entornos digitales de acuerdo con lo dispuesto en la legislación vigente. 2. Asimismo, se promoverá la garantía de los derechos reconocidos en esta Carta en el marco de las relaciones con la Administración de Justicia y, particularmente, los derechos relacionados con la inteligencia artificial, cuando se recurra a ésta para la utilización o el desarrollo de sistemas de soporte a las decisiones o de herramientas de justicia predictiva. 3. Se promoverán mecanismos de autorregulación, control propio y procedimientos de resolución alternativa de conflictos, con la previsión de incentivos adecuados para su utilización con arreglo a la normativa vigente. 4. Se promoverá la evaluación de las leyes administrativas y procesales vigentes a fin de examinar su adecuación al entorno digital y la propuesta en su caso de reformas oportunas en garantía de los derechos digitales».

[10] Es de cita obligada el muy documentado trabajo de Gutiérrez David, M. E., «Administraciones inteligentes y acceso al código fuente y los algoritmos públicos. Conjurando riesgos de cajas negras decisionales», en: *Derecom*, 30, 2021, pp. 143-228 (https://www.derecom.com/derecom/; última lectura: 28 de febrero de 2023). Las numerosas referencias jurisprudenciales y bibliográficas que contiene, atinentes no sólo a España sino también a los principales países de nuestro entorno, me han sido de gran utilidad en la confección de este trabajo.

II. EL ACCESO AL CONOCIMIENTO DE LOS ALGORITMOS UTILIZADOS POR LAS ADMINISTRACIONES PÚBLICAS EN LA NORMATIVA REGULADORA DEL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES

La toma de datos automatizada tiene una regulación específica en el artículo 22 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo (Reglamento general de protección de datos, en adelante RGPD)[11], que comienza en su apartado primero consagrando una regla general, a saber, la prohibición de que pueda adoptarse una decisión fundamentada exclusivamente en el tratamiento automatizado de datos: «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».

Sin embargo, este derecho a no ser objeto de decisiones totalmente automatizadas consagrado en el primer apartado del artículo 22.1 RGPD no se configura como una regla absoluta, incondicionada, toda vez que acto seguido su apartado segundo apunta las diversas excepciones a la misma: «El apartado 1 no se aplicará si la decisión: a) es necesaria para la celebración o la ejecución de un contrato entre el interesado y un responsable del tratamiento; b) está autorizada por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento y que establezca asimismo medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, o c) se basa en el consentimiento explícito del interesado».

Conviene notar que es el supuesto b) el que parece llamado a servir de cobertura para la adopción de decisiones plenamente automatizadas en el ámbito de las relaciones Administración/administrados, habida cuenta del papel absolutamente marginal que el RGPD atribuye al consentimiento como base de licitud del tratamiento por parte de las Administraciones públicas[12]. Comoquiera que sea, el art. 22.2 RGPD úni-

[11] Para un más detenido tratamiento de la cuestión en el RGPD, véase Medina Guerrero, M., «El derecho a conocer los algoritmos utilizados en la toma de decisiones. Aproximación desde la perspectiva del derecho fundamental a la protección de datos personales», en: *Teoría y Realidad Constitucional*, núm. 49, 2022, pp. 141-171.

[12] Según aclara el Considerando 43: «Para garantizar que el consentimiento se haya dado libremente, este no debe constituir un fundamento jurídico válido para el tratamiento de datos de carácter personal en un caso concreto en el que exista un desequilibrio claro entre el interesado y el responsable del tratamiento, en particular cuando dicho responsable sea una autoridad pública y sea por lo tanto improbable que el consentimiento se haya dado libremente en todas las circunstancias de dicha situación particular». Así, pues, como regla general, cuando de tratamientos de Administraciones públicas se trata, será preciso acudir a otras bases jurídicas más adecuadas [Huergo Lora, A., «Una aproximación a los algoritmos desde el Derecho Administrativo», en: Huergo Lora, A. (dir.) *La regulación de los algoritmos*, Thomson Reuters Arazandi, Cizur Menor, 2020, p. 57; Vilasau Solana, M., «El consentimiento general y de menores», en: Rallo Lombarte, A. (dir.), *Tratado de protección de datos*, Tirant lo Blanch, Valencia, 2019, p. 201; Valero Torrijos, J., «Las garantías jurídicas de la inteligencia artificial en la actividad administrativa desde la perspectiva de la buena administración», *Revista Catalana de Dret Públic*, núm. 58, 2019, p. 90].

camente vincula expresamente con este supuesto b) la exigencia de que se establezcan «medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado».

Exigencia que, sin embargo, el apartado tercero del art. 22 RGPD sí va a extender a los restantes supuestos, aunque con la importante singularidad de que respecto de ellos sí se impongan unas específicas garantías mínimas: «En los casos a que se refiere el apartado 2, letras a) y c), el responsable del tratamiento adoptará las medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, como mínimo el derecho a obtener intervención humana por parte del responsable, a expresar su punto de vista y a impugnar la decisión».

II.1. Las reglas de transparencia aplicables a las decisiones basadas en tratamiento automatizado de datos

El principio de transparencia del tratamiento consagrado en el artículo 5.1 a) RGPD tiene dos principales manifestaciones a lo largo del propio Reglamento. Por una parte, se proyecta en el establecimiento de específicos deberes de información que se imponen al responsable del tratamiento, tanto cuando los datos personales los recaba del propio interesado (art. 13 RGPD) como si no los obtiene de él (art. 14 RGPD). Y, por otro lado, se plasma en el derecho del interesado a acceder a sus datos personales y a determinada información en los términos previstos en el artículo 15 RGPD.

Pues bien, con independencia de que los tratamientos automatizados de datos entren o no en el ámbito de cobertura del artículo 22 RGPD, es obvio que a todos ellos se extiende la obligación genérica de los responsables de suministrar la información básica aludida en el primer apartado de los artículos 13 y 14 RGPD[13], así como las exigencias informativas previstas en su apartado segundo que resulten de general aplicación. En relación con la información mencionada en el primer apartado —la frecuentemente denominada «primera capa»—, conviene destacar la obligación de que se dé cuenta a los interesados de los fines del tratamiento y la base jurídica del mismo [art. 13.1.c) y art. 14.1.c)]. Y en virtud de estas previsiones, según ha declarado el Grupo

[13] Según establece el primer apartado del artículo 14 RGPD: «Cuando los datos personales no se hayan obtenido del interesado, el responsable del tratamiento le facilitará la siguiente información: a) la identidad y los datos de contacto del responsable y, en su caso, de su representante; b) los datos de contacto del delegado de protección de datos, en su caso; c) los fines del tratamiento a que se destinan los datos personales, así como la base jurídica del tratamiento; d) las categorías de datos personales de que se trate; e) los destinatarios o las categorías de destinatarios de los datos personales, en su caso; f) en su caso, la intención del responsable de transferir datos personales a un destinatario en un tercer país u organización internacional y la existencia o ausencia de una decisión de adecuación de la Comisión, o, en el caso de las transferencias indicadas en los artículos 46 o 47 o el artículo 49, apartado 1, párrafo segundo, referencia a las garantías adecuadas o apropiadas y a los medios para obtener una copia de ellas o al hecho de que se hayan prestado».

de trabajo sobre protección de datos del artículo 29, «debe aclararse al usuario el hecho de que el tratamiento tiene fines tanto de a) elaboración de perfiles como de b) adopción de una decisión sobre la base del perfil generado»[14].

Estas exigencias de transparencia se intensifican, ciertamente, cuando se trata de toma de decisiones plenamente automatizadas en el marco de lo previsto en el artículo 22 RGPD. En efecto, en estos casos el apartado segundo de los artículos 13 y 14 RGPD impone a los responsables del tratamiento que informen además sobre: «la existencia de decisiones automatizadas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado» [art. 13.2 f) y art. 14.2.g)].

Y en la hipótesis de que alguien que no haya obtenido tal información del responsable sospeche que sus datos son empleados en esos procedimientos de toma de decisiones totalmente automatizas, o sencillamente haya tenido conocimiento de que es objeto de una decisión de tal naturaleza, el artículo 15.1.h) RGPD —que reproduce literalmente idéntica formulación que el art. 13.2.f) y el art. 14.2.g) RGPD— le confiere el derecho de acceder a la misma.

Reina, sin embargo, un acuerdo prácticamente generalizado en entender que proporcionar «información significativa sobre la lógica aplicada» no equivale a exigir el acceso directo al algoritmo o a su código fuente.

Por una parte, se argumenta que este acceso no es necesario para que el afectado pueda comprobar la corrección de la decisión y esté en condiciones de hacer valer los derechos que le atribuye el RGPD[15]. En efecto, por lo general el afectado no tendrá interés en conocer el entero algoritmo o el código fuente, sino que antes bien su interés se concentra en saber qué hace el algoritmo a partir de sus datos y para qué[16].

Y por otro lado se ha esgrimido que la apertura al afectado del entero algoritmo no sería por lo general compatible con la tutela de los secretos comerciales y del derecho a la propiedad intelectual sobre los programas informáticos[17], cuya salvaguarda se exige

---

[14] *Directrices sobre decisiones individualizadas automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679*, del Grupo de Trabajo sobre Protección de Datos del Artículo 29, adoptadas el 3 de octubre de 2017 y revisadas el 6 de febrero de 2018 (WP215rev.01), p. 18.

[15] Kaminski, M. E., «The Right to Explanation, Explained», en: *University of Colorado Law Legal Studies Research Paper* No. 18-24, *Berkeley Technology Law Journal* Vol. 34, No.1, 2019, p. 19 (disponible en https://ssrn.com/abstract=3196985, así como en http://dx.doi.org/10.2139/ssrn.319695); Martini, M.; Nink, D., «Wenn Maschinen entscheiden … — vollautomatisierte verwaltungsverfahren und der Persönlichkeitsschutz», en: *Neue Zeitschrift für Verwaltungsrecht-Extra*, 10, 2017, pp. 10-11.

[16] En esta línea, Weichert, T., «Die verfassungsrechtliche Dimension der Algorithmenkontrolle», en: *Datenschutz Nachrichten* 3/2018, p. 134.

[17] Buchner, B., «Comentario al artículo 22», en: Kühling, J.; Buchner, B. (Hrsg.), *Datenschutz-Grundverordnung Bundesdatenschutzgesetz. Kommentar*, 2. Auflage, C. H. Beck, München, 2018, p. 517; Kühling, J.; Martini, M. *et al.*, *Die Datenschutz-Grundverordnung und das nationale Recht. Erste Überlegungen zum innerstaatlichen Regelungsbedarf*, Verlagshaus Monsenstein und Vannerdat, Münster, 2016, pp. 65-66.

taxativamente en el Considerando 63: «Todo interesado debe… tener el derecho a conocer y a que se le comuniquen, en particular, […] la lógica implícita en todo tratamiento automático de datos personales y, por lo menos cuando se base en elaboración de perfiles, las consecuencias de dicho tratamiento. […] Este derecho no debe afectar negativamente a los derechos y libertades de terceros, incluidos los secretos comerciales o la propiedad intelectual y, en particular, los derechos de propiedad intelectual que protegen programas informáticos».

Así, pues, según se desprende del marco trazado por el RGPD, parece evidente que el tope máximo de información algorítmica que puede suministrarse sin quebrantar el secreto comercial o el derecho a la propiedad intelectual no puede llevarse hasta el extremo de exigir la transmisión de conocimientos técnicos esenciales (*know how*) que se quieren mantener confidenciales ni, mucho menos, la totalidad del algoritmo. Y, en este sentido, el Grupo de trabajo sobre protección de datos del artículo 29 ha sostenido que el «RGPD exige que el responsable del tratamiento ofrezca información significativa sobre la lógica aplicada, no necesariamente una compleja explicación de los algoritmos utilizados o la revelación de todo el algoritmo»[18].

Esta operatividad en la práctica de los referidos límites ya se había puesto de manifiesto antes de la aprobación del RGPD, como lo atestigua la Sentencia del Tribunal Supremo alemán en el caso SCHUFA, de 28 de enero de 2014 —VI ZR 156/13—[19], probablemente la más relevante referencia jurisprudencial europea que abordó frontalmente la cuestión en el marco de la anterior Directiva 95/46, de 24 de octubre de 1995. En esta resolución, la referencia al límite de los secretos comerciales efectuada en el Considerando 41 de la Directiva sirvió para realizar una lectura restrictiva del derecho de acceso a la información de los afectados (§ 33), llegando a la conclusión de que no resultaba obligado trasladarles la fórmula de evaluación (*Scoreformel*) utilizada para determinar la solvencia de los que pretenden acceder a un préstamo. El deber de información del responsable del tratamiento —argumenta el Tribunal Supremo— se circunscribe a poner en conocimiento del interesado los datos personales tomados en consideración y su influencia en la concreta evaluación realizada. El objetivo, pues, de la información a suministrar es que sea visible para el afectado qué específicas circunstancias se incorporaron en el cálculo de su nivel de solvencia. Sin embargo, el deber de informar no se extiende a los elementos abstractos del sistema de calificación (*Scorecard*) en sus detalles, como los grupos de comparación y su ponderación (§ 29).

---

[18] *Directrices sobre decisiones individuales automatizadas… op. cit.*, nota 14, p. 28.

[19] Scheja, K., «Schutz von Algorithmen in Big Data Anwendungen», en: *Computer und Recht*, 8/2018, p. 487; Schulte, U.; Timm, M., «Entscheidungsanmerkung zu dem Urteil des Bundesgerichtshofes vom 28.1.2014 — VI ZR 156/13. Umfang des Auskunftsanspruches gegen die Schufa-Scorewerte», *Neue Juristische Wochenschrift*, Heft 17/2014, pp. 1235-1239.

II.2. El derecho del afectado a recibir una explicación de la específica decisión adoptada

Admitido generalizadamente que el RGPD no reconoce la posibilidad de acceder directamente al entero algoritmo o al código fuente, el principal interrogante suscitado por el RGPD en la materia que nos ocupa reside en determinar si del mismo cabe derivar un derecho del interesado a que se le explique la concreta decisión automatizada de la que ha sido objeto.

En buena medida aquellos que sostienen la existencia de un derecho de explicación sobre decisiones específicas lo fundamentan en una lectura integradora del artículo 15 en combinación con el artículo 22 RGPD (señaladamente su apartado tercero) y el Considerando 71[20].

Recuérdese que el apartado tercero del art. 22 RGPD viene a establecer unas garantías mínimas en el caso de que las decisiones totalmente automatizadas se adopten en el marco de la conclusión o el cumplimiento de un contrato, o bien mediando el previo consentimiento del afectado [los supuestos contemplados en el art. 22.2 a) y c) RGPD]; a saber: «el derecho a obtener intervención humana por parte del responsable, a expresar su punto de vista y a impugnar la decisión».

Bajo este prisma, se ha defendido una lectura funcional del derecho de acceso a la información tendente a preservar dichas garantías mínimas explicitadas en el art. 22.3 RGPD, según la cual la explicación de la concreta decisión puede considerarse una premisa casi inexcusable para que tales derechos sean verdaderamente eficaces y operativos, señaladamente el que reconoce al afectado la capacidad de impugnar la decisión[21].

Y, por su parte, el Considerando 71 opera como elemento central en esta línea argumental, toda vez que es en el único lugar del Reglamento donde aparece explíci-

---

[20] Selbst, A. D.; Powles, J., «Meaningful information and the right to explanation», en: *International Data Privacy Law*, 2017, Vol. 7, No. 4, p. 233 y ss. [doi:10.1093/idpl/ipx022]; Brkan, M., «Do Algorithms Rule the World? Algorithmic Decision-Making in the Framework of the GDPR and Beyond», en: *International Journal of Law and Information Technology*, 11 January 2019, p. 15 (he utilizado la versión disponible en https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3124901).Véase asimismo Franck, L., «Comentario al artículo 15», en: Gola, P.; Heckmann, D. (Hrsg.), *Datenschutz-Grundverordnung VO (EU) 2016/679. Bundesdatenschutzgesetz. Kommentar*, 3ª edición, C. H. Beck, München, 2022, p. 487.

[21] En este sentido, se ha sostenido que el test sobre si la información a suministrar es o no «significativa» debe ser funcional, vinculando la misma con alguna acción que la explicación posibilite al afectado, como sucede con el derecho a impugnar la decisión (Selbst, A. D./Powles, J., *op. cit.*, nota 20, p. 236; Kaminski, M. E., *op. cit.*, nota 16, p. 20). Incluso los que se inclinan por negar la existencia de un derecho a la explicación sobre decisiones específicas derivado directamente del RGPD admiten que la jurisprudencia puede interpretar ampliamente las garantías mínimas del art. 22.3 RGPD para reconocerlo, sobre la base de que la explicación es necesaria para que el afectado exprese su punto de vista e impugne la decisión [Wachter, S.; Mittelstadt, B.; Floridi, L.,«Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation», en: *International Data Privacy Law,* 2017, Vol. 7, No. 2, p. 91 (doi:10.1093/idpl/ipx005)].

tamente la idea de la existencia de un derecho a la explicación sobre decisiones ya adoptadas:

> «[…] se deben permitir las decisiones basadas en tal tratamiento [automatizado], incluida la elaboración de perfiles, si lo autoriza expresamente el Derecho de la Unión o de los Estados miembros aplicable al responsable del tratamiento, incluso con fines de control y prevención del fraude y la evasión fiscal, realizada de conformidad con las reglamentaciones, normas y recomendaciones de las instituciones de la Unión o de los órganos de supervisión nacionales y para garantizar la seguridad y la fiabilidad de un servicio prestado por el responsable del tratamiento, o necesario para la conclusión o ejecución de un contrato entre el interesado y el responsable del tratamiento, o en los casos en los que el interesado haya dado su consentimiento explícito. En cualquier caso, dicho tratamiento debe estar sujeto a las garantías apropiadas, entre las que se debe incluir la información específica al interesado y *el derecho* a obtener intervención humana, a expresar su punto de vista, *a recibir una explicación de la decisión tomada después de tal evaluación* y a impugnar la decisión» (el énfasis es nuestro).

Pues bien, según refleja el fragmento transcrito, el Considerando 71 viene a incluir el derecho a recibir una explicación junto a las garantías mínimas establecidas en el art. 22.3 RGPD; precepto este último que vincula únicamente tales garantías con los supuestos a) y c) del art. 22.2 RGPD (decisiones necesarias para la celebración o ejecución de un contrato; decisiones basadas en el consentimiento explícito del interesado). En relación con estos supuestos, podría sostenerse que el reconocimiento del derecho a la explicación no resulta incompatible con lo dispuesto en el art. 22.3 RGPD, ya que cabría considerarlo fruto de una lectura funcional e integradora del precepto perfectamente posible: una explicación de la específica decisión tomada se concibe como un paso previo conveniente para que puedan desplegar su eficacia las garantías mínimas consagradas en el art. 22.3 RGPD, especialmente los derechos del afectado a expresar su punto de vista y a impugnar la decisión[22].

Diferente puede ser la apreciación respecto del supuesto contemplado en la letra b) del artículo 22.2 RGPD (decisiones autorizadas por el Derecho de la Unión o de los Estados miembros), que queda extramuros del ámbito de aplicación del art. 22.3 RGPD y al que, por tanto, no se proyectan directa, necesariamente, las repetidas garantías mínimas. Y no debe de ser motivo de extrañeza esta distinta regulación entre ambas categorías de supuestos, habida cuenta de los diferentes destinatarios que tienen los correspondientes preceptos: mientras que el art. 22.3 RGPD, en relación con los supuestos a) y c) del art. 22.2 RGPD, se dirige directamente a los responsables del

[22] A esta dirección parece apuntar el Grupo de trabajo del artículo 29 al efectuar en el Anexo 2 las observaciones correspondientes al art. 22.3 RGPD y al Considerando 71 (*Directrices sobre decisiones individuales automatizadas… op. cit.*, nota 14, p. 40).

tratamiento imponiéndoles determinadas garantías mínimas; cuando del supuesto b) se trata, el art. 22.2 RGPD tiene como destinatario a los Estados miembros, atribuyéndoles un cierto margen de maniobra para desviarse de la regulación del RGPD en lo concerniente a la concretización de cuáles sean «las medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado». A lo sumo, las garantías mínimas en las que el art. 22.3 RGPD viene a concretar las «medidas adecuadas» para los supuestos a) y b) servirían como líneas orientadoras para los legisladores nacionales, pero en ningún caso podrían considerarse inmediatamente vinculantes para los Estados miembros.

Por consiguiente, extender el derecho que nos ocupa al supuesto b), por considerarlo necesario para la adecuada salvaguardia de las garantías mínimas del art. 22.3 RGPD, forzaría —hasta quebrantarlo— el tenor literal del RGPD, que claramente ha querido reservar a los Estados miembros un margen de libertad de configuración en punto a la determinación de tales garantías. No hay, pues, en relación con ese supuesto un derecho a la explicación que nazca directamente del RGPD: es precisa, en suma, una actuación legislativa interna que haga aflorarlo.

Dicho esto, no puede dejar de notarse que en el ámbito de las relaciones Administración/administrados —al que resulta especialmente de aplicación el reiterado supuesto b)— un deber de explicación o motivación de las concretas decisiones automatizadas sería en todo caso constitucionalmente exigible, pero no ya como una exigencia derivada del derecho fundamental a la protección de datos personales, sino como una obligación impuesta por manifestaciones esenciales del principio del Estado de Derecho como las contenidas en los artículos 9.3 y 106.1 CE[23].

II.3. La limitada transparencia algorítmica salvaguardada por el RGPD

Tras este examen a vuela pluma del estado de la cuestión en el RGPD —que en ningún modo se ha visto matizado o afectado por la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, ya que nada nuevo dice en relación con el derecho a la información en este ámbito—, se hace evidente lo estrecho de este cauce para acceder a los algoritmos empleados por las Administraciones públicas en su toma de decisiones.

[23] En este sentido, Ponce Solé ha considerado el derecho a la explicación de las decisiones administrativas una exigencia genérica derivada del derecho a la buena administración, que a su vez está vinculado con la prohibición de la arbitrariedad del artículo 9.3 CE («Inteligencia artificial, Derecho administrativo y reserva de humanidad: algoritmos y procedimiento debido tecnológico», en: *Revista General de Derecho Administrativo* 50, 2019, pp. 39-40). Véase asimismo Soriano Arnanz, A. «Decisiones automatizadas: problemas y soluciones jurídicas. Más allá de la protección de datos», en: *Revista de Derecho Público: Teoría y Método*, Vol. 3, 2021, pp. 101-102.

En primer término, excluido el acceso directo al algoritmo o a su código fuente según la interpretación prácticamente unánime del RGPD en virtud de los límites de la propiedad intelectual e industrial y del secreto empresarial, únicamente cabe hablar —hoy por hoy— del derecho a que se informe sobre la «lógica aplicada» [art. 15.1.h) RGPD] y, a lo sumo, de un derecho a la explicación de la concreta decisión individual adoptada con base en algoritmos (en aplicación del artículo 22.3 RGPD en conexión con el Considerando 71). Y aun asumiendo que del RGPD nazca directamente ese derecho a la explicación, ha de notarse, por una parte, que el mismo únicamente sería exigible frente a las decisiones totalmente automatizadas —que no a aquellas adoptadas por un ser humano con el auxilio de un sistema algorítmico—; y, por otro lado, que es más que dudoso que este derecho a la explicación garantizado por el RGPD se extienda al supuesto b) del artículo 22.2 RGPD, que es precisamente el que habitualmente será de aplicación a los casos de toma de decisiones totalmente automatizadas por las Administraciones públicas[24].

En segundo lugar, debe tenerse presente que la posibilidad de acceder a esa información sobre la decisión basada en algoritmos tan sólo corresponde a la concreta persona física objeto de la decisión. Esta restricción plantea un doble orden de problemas.

Primero, dificulta que pueda combatirse eficazmente el potencial discriminatorio de los algoritmos. En efecto, si únicamente es dable acceder a la explicación de la concreta decisión individualizada que afecta al titular del derecho, resulta más que complicado enjuiciar si el diseñado proceso algorítmico de toma de decisiones incorpora una discriminación sistémica, al introducir sesgos negativos para una determinada clase o grupo de la población.

Segundo, el acceso a la información algorítmica por parte del concreto individuo afectado quizá tampoco asegure una transparencia verdaderamente operativa, habida cuenta de las dificultades de comprensión que la misma puede entrañar para cualquier ciudadano que no tenga unos mínimos conocimientos técnicos.

Ambos problemas podrían de algún modo mitigarse si se habilitara la presencia de entidades expertas en la materia que actuasen en representación de los afectados en el procedimiento de acceso a la información algorítmica[25]. Y algunas vías abre al respecto el propio RGPD en su artículo 80.

En su apartado primero, reconoce a los interesados el «derecho a dar mandato a una entidad, organización o asociación sin ánimo de lucro […] cuyos objetivos estatutarios sean de interés público y que actúe en el ámbito de la protección de los derechos y libertades de los interesados en materia de protección de sus datos personales, para

[24] En contra de la aplicación a este supuesto, Wachter, S.; Mittelstadt, B.; Floridi, L., *op. cit.*, nota 21, pp. 93-94.

[25] Véase, por ejemplo, Edwards, L.; Veale, M., «Enslaving the Algorithm: From a «Right to an Explanation» to a «Right to Better Decisions»?», en: *IEEE Security & Privacy* (2018) 16(3), pp. 46—54 (doi:10.1109/MSP.2018.2701152).

que presente en su nombre la reclamación, y ejerza en su nombre los derechos contemplados en los artículos 77 [derecho a presentar una reclamación ante una autoridad de control], 78 [derecho a la tutela judicial efectiva contra una autoridad de control] y 79 [derecho a la tutela judicial efectiva contra un responsable o encargado del tratamiento], y el derecho a ser indemnizado mencionado en el artículo 82, si así lo establece el Derecho del Estado miembro».

El artículo 80.1 RGPD permite, por tanto, que los afectados recurran a entidades especializadas para tutelar su pretensión de acceder a la información algorítmica; y facilita asimismo que tales entidades presenten «acciones colectivas en nombre de un grupo más o menos amplio de interesados, acumulando las diferentes acciones individuales en un único asunto que será examinado por el juez o tribunal competente»[26]. Ahora bien, esta fórmula —que paliaría la falta de conocimientos técnicos de los concretos afectados y articularía una mejor defensa frente a los algoritmos discriminatorios— se supedita a una condición *sine qua non*: su establecimiento por el Derecho de los diferentes Estados miembros.

Y el apartado segundo del artículo 80 RGPD habilita otro cauce para que las entidades puedan operar en este ámbito, al autorizar expresamente a todo Estado miembro a atribuirles, «con independencia del mandato del interesado, derecho a presentar en ese Estado miembro una reclamación ante la autoridad de control que sea competente en virtud del artículo 77 y a ejercer los derechos contemplados en los artículos 78 y 79, si considera que los derechos de los interesados con arreglo al presente Reglamento han sido vulnerados como consecuencia de un tratamiento».

Una y otra vía, sin embargo, dependen de la decisión de los correspondientes Estados miembros[27]. Y, en lo que a España concierne, éste es otro ámbito del RGPD susceptible de desarrollo normativo desaprovechado por el legislador, habida cuenta de que ninguna previsión incorporó al respecto la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales[28].

En este contexto, no es de extrañar que de modo generalizado las miradas se dirijan a las respectivas leyes reguladoras del acceso a la información pública para superar la opacidad de la toma de decisiones automatizadas, toda vez que extienden su ámbito

---

[26] Villalba Cano, L., «La representación de los interesados (Comentario al artículo 80 RGPD)», en: Troncoso Reigada, A. (dir.), *Comentario al Reglamento General de Protección de Datos y a la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales*, Tomo II, Civitas/Thomson Reuters, Cizur Menor, 2021, p. 3023.

[27] Al considerarse escasamente operativa esta dimensión colectiva abierta por el art. 80 RGPD, la apertura de las decisiones algorítmicas a periodistas y entidades especializadas se ha pretendido fundamentar en la jurisprudencia del TEDH recaída sobre el artículo 10 del Convenio [véase Mazur, J., «Right to Access Information as a Collective-Based Approach to the GDPR's Right to Explanation in European Law», en: *Erasmus Law Review*, december 2018 | No. 3 - doi: 10.5553/ELR.000116 (disponible en: https://ssrn.com/abstract=3356770)].

[28] Sobre la forma en que otros países europeos —como Francia, Bélgica o Portugal— han llevado a su legislación estas habilitaciones del RGPD, véase Villalba Cano, L., *op. cit.*, nota 26, pp. 3022-3028.

de aplicación, no sólo a los concretos afectados, sino también a la sociedad en su conjunto y, particularmente, a la prensa[29]. Así es; dada la amplitud con que suele configurarse la titularidad del derecho de acceso *ex* legislación de transparencia, ya que puede ser ejercitado por cualquier persona física o jurídica aunque no sea objeto de una decisión basada en algoritmos, se abre el paso a que expertos en la materia (periodismo de investigación, ONG's, etc) puedan desentrañar el proceso automatizado de toma de decisiones. A este respecto, es de justicia destacar el importante papel que el periodismo especializado está llamado a desempeñar —de hecho, está ya desempeñando— en el fomento de la transparencia y la rendición de cuentas de los sistemas algorítmicos de toma de decisiones[30], como lo acredita su presencia en la puesta en marcha de una de las más relevantes organizaciones no gubernamentales europeas que operan en este ámbito, *AlgorithmWatch*[31].

En suma, los notables condicionantes y obstáculos derivados de la normativa reguladora de la protección de datos para el acceso a la toma de decisiones automatizadas pueden verse sustancialmente compensados, cuando de Administraciones Públicas se trata, por la legislación reguladora de la transparencia[32]. Sobre la premisa de entender que los algoritmos empleados por aquéllas son «información pública» a los efectos de esta legislación, el acceso se extendería a todo proceso de toma de decisiones automatizadas, con independencia por tanto de si hay o no intervención humana y de la naturaleza e intensidad de la misma. Por otro lado, la pretensión de acceder tampoco tendría ningún condicionante material que operase apriorísticamente, por lo que, en línea de principio, cabría solicitar el acceso a la totalidad del algoritmo o a su código fuente.

La cuestión, sin embargo, no es tan sencilla, pues —como comprobaremos en las siguientes páginas— las diferentes normativas reguladoras de la transparencia plantean no pocos interrogantes al respecto, además de establecer condicionantes y restricciones al acceso a la información que resultan señaladamente de aplicación a la materia que nos ocupa.

---

[29] En este sentido, Bloch-Wehba, H., «Access to Algorithms», en: *Fordham Law Review* Vol. 88, 2020, p. 1269.

[30] Sector periodístico que se vio sin duda agitado por el debate suscitado a raíz de los trabajos de Nicholas Diakopoulos [«Algorithmic Accountability Reporting: On the Investigation of Black Boxes», Columbia Journalism School, Tow Center for Digital Journalism, 2014 (https://doi.org/10.7916/D8ZK-5TW2); así como «Algorithmic Accountability. Journalistic investigation of computational power structures», en: *Digital Journalism*, 2014 (https://dx.doi.org/10.1080/21670811.2014.976411)].

[31] Véase al respecto Spielkamp, M., «AlgorithmWatch: What Role Can a Watchdog Organization Play in Ensuring Algorithmic Accountability?», en: Cerquitelli, T.; Quercia, D.; Pasquale, F. (Eds.), *Transparent Data Mining for Big and Small Data*, Springer, 2017, pp. 207-215.

[32] En este sentido, Palma Ortigosa, A., «Decisiones automatizadas en el RGPD. El uso de algoritmos en el contexto de protección de datos», en: *Revista General de Derecho Administrativo*, 50, 2019, p. 26.

III.LA APERTURA DE LOS SISTEMAS ALGORÍTMICOS UTILIZADOS POR LAS ADMINISTRACIONES PÚBLICAS EN LA LEGISLACIÓN REGULADORA DE LA TRANSPARENCIA

III.1. La consideración de los algoritmos como «información pública» a los efectos de las leyes de transparencia

III.1.1. *Aproximación desde el Derecho Comparado*

Desde el momento en que las Administraciones comenzaron a utilizar de forma habitual las nuevas tecnologías (software, programas de ordenador etc.)[33], surgieron las dudas acerca de si esas tecnologías en sí mismas consideradas podían catalogarse como «información pública» a los efectos de las correspondientes leyes reguladoras del derecho de acceso a la información.

En aras de la sistematización, son esencialmente dos los enfoques que se han empleado en Derecho Comparado para valorar si los programas de ordenador utilizados por las Administraciones públicas (y, más específicamente, los algoritmos que los integran y sus códigos fuente) forman parte del ámbito material protegido por el derecho de acceso a la información. Frente a la línea que sostiene que sí constituyen información pública a la luz de la definición de este concepto en su correspondiente marco normativo; otros tienden a negar que puedan catalogarse como tales, al tratarse de meras herramientas técnicas que *per se* no aportan datos y por tanto no contienen información.

Tras una primera aproximación al tema en varios países de nuestro entorno, cabe ya adelantar —con las matizaciones que se verán— que el principal criterio que opera al respecto reside en comprobar si el programa informático utilizado se vincula directamente con el objetivo esencial de la legislación de transparencia: el control por parte de la opinión pública de las decisiones adoptadas por las diferentes Administraciones. Resulta, por tanto, determinante la distinción entre informática instrumental e informática decisional[34].

---

[33] No existe en la Unión Europea, a nivel jurídico, una clara diferenciación entre los conceptos programa de ordenador (*computer program*) y software de ordenador (*computer software*). De ahí que la tendencia general sea que los términos software y programa se utilicen como sinónimos [en este sentido, Schneider, J., «Urheberrechtsschutz für Software», en: Schneider, J. (ed.), *Handbuch EDV-Recht: IT-Recht mit IT-Vertragsrecht, Datenschutz, Rechtsschutz und E-Business*, Otto Schmidt KG, 2017, p. 1031; Fernández Masía, E., *La protección de los programas de ordenador en España*, Tirant lo Blanch, Valencia, 1996, pp. 39-41]. No obstante, en las «Disposiciones tipo sobre la protección del software de ordenador» (*Model Provisions on the Protection of Computer Software*), que aprobó en el año 1977 la Organización Mundial de la Propiedad Intelectual, la noción de «software de ordenador» definida en su Sección 1ª se configura como un concepto más amplio, por cuanto el «programa de ordenador» aparece como la materia protegida por aquélla o una de las materias protegidas junto a la «descripción del programa» y el «material de apoyo» [estas *Model Provisions* fueron publicadas en *Copyright. Monthly Review of the World Intellectual Property Organization (WIPO)*, January 1978, p. 66 y ss].

[34] Véase Gutiérrez David, M. E., *op. cit.*, nota 10, pp. 159-160. En efecto, como ha sostenido Boix Palop, cuando el uso de algoritmos y programas es puramente instrumental y mecánico no resulta jurídi-

Pero examinemos con más detenimiento esta cuestión, abordándola específicamente en relación con algunos países que hemos considerado representativos.

Las dudas sobre la eventual proyección de la legislación de transparencia a los programas de ordenador ya se suscitaron abiertamente en uno de los países pioneros en este ámbito, los **Estados Unidos**. Así es; en el Informe elaborado en 1990 por el Departamento de Justicia sobre la noción de «documento electrónico» (*electronic record*) en el marco de la *Freedom of Information Act* (en adelante, FOIA)[35], se abordó específicamente el estatus del «software de ordenador». Y el primer asunto sobre el que se interroga el informe es si el software puede considerarse «documento» en el sentido genuino del término, toda vez que por lo general se entiende que «documento» es un soporte, cualquiera que sea la forma que adopte, en el que se graba la información a fin de preservar su contenido. En consecuencia, si se trata de un software que no sirve por sí mismo para almacenar información, sino que sirve simplemente como medio para tratar la información en el seno de un sistema automatizado de procesamiento de datos, el informe se cuestiona abiertamente sobre la eventual catalogación del mismo como *record* en el sentido de la FOIA. O, como formulará el interrogante en otros términos más adelante el reiterado informe, «la cuestión reside en determinar si los elementos del software pueden más propiamente considerarse depósitos de información (como los datos), por una parte, o meras herramientas (como el hardware), por otro lado». Y en la medida en que puede haber variaciones significativas en el carácter de los diferentes elementos del software, el informe termina concluyendo que la respuesta podría variar de un elemento del software a otro.

Debe notarse, en cualquier caso, que el legislador estadounidense fue sensible a la creciente utilización de las nuevas tecnologías, de tal modo que se reformó la propia definición del concepto de «documento» (*record*) para incorporar explícitamente la actuación digital de la Administración. Frente a la más tradicional descripción de la noción de «documento» de la versión inicial de la FOIA —que incluía «todos los libros, papeles, mapas, fotografías, materiales legibles por máquinas u otros materias documentales, con independencia de su forma física o características»—, la reforma acometida en el año 2014 amplía de modo expreso su ámbito de cobertura a las nuevas tecnologías: «el término `información documentada´ incluye todas la formas tradicionales de documentos, con independencia de su forma física o características, incluyen-

camente relevante: «No hay ninguna diferencia jurídica entre escribir una resolución en una máquina de escribir o hacerlo por medio de un programa de procesamiento de textos. En la medida en que el aporte de la informática y de los programas empleados sea meramente instrumental y basado en la ayuda a operaciones de apoyo, por mucha mejora que suponga, no se altera esta realidad» («Transparencia en la utilización de inteligencia artificial por parte de la Administración», en: *El Cronista del Estado Social y Democrático de Derecho*, núm. 100, septiembre-octubre 2022, 228).

[35] *Department of Justice Report on «Electronic Record» FOIA Issues*, Part II. FOIA Update Vol. XI, Nº 3, 1990.

do la información creada, manipulada, comunicada o almacenada en forma digital o electrónica».

Pues bien, aunque —como abundaremos más adelante al examinar el límite de la propiedad intelectual— la transparencia algorítmica encuentra un primer obstáculo en la rigurosa interpretación de la exigencia jurisprudencial de que la Administración «controle» el programa informático para que sea accesible en el marco de la FOIA[36], el factor determinante es apreciar si lo solicitado se acomoda a la finalidad última perseguida por la ley.

Aspectos ambos que, en alguna ocasión, se sobreponen o solapan en la argumentación jurisprudencial, como sucedió en la Sentencia del Tribunal del noveno distrito de California, de 13 de marzo de 1995 (*Baizer v. United States Department of the Air Force*)[37]. Ante la pretensión del solicitante de que el Departamento de Defensa Aérea suministrase las Sentencias del Tribunal Supremo en formato electrónico obtenidas de la base de datos JURIS, el Tribunal enfocaría la cuestión examinando la forma en que la Administración usaba el material objeto de la solicitud de información, apoyándose expresamente en dos precedentes: «Tanto en *Tax Analysts*[38] como en *SDC Development* […] los tribunales de circuito se centraron en cómo la agencia utilizó el material solicitado. Si una agencia integra material en sus archivos y se fundamenta en él para la toma de decisiones, entonces la agencia controla el material. Si, por otro lado, el material se mantiene únicamente con fines de referencia o como herramienta de investigación, entonces faltan indicios de control». A partir de esta argumentación, se llegaría a la conclusión de que la base de datos de las resoluciones del Tribunal Supremo no podía catalogarse como un «documento» de la agencia, habida cuenta de que no cabía afirmar que el Departamento de la Fuerza Aérea «controlase» las decisiones del TS en el sentido antes apuntado.

En el segundo de los precedentes mencionados —*SDC Development Corp. v. Mathews,* 542 F.2d 1116 (9th Cir.1976)— lo solicitado eran las referencias bibliográficas en materia de medicina que obraban en el banco de datos informático de la National Library of Medicine. El Tribunal, tras examinar el procedimiento de elaboración de la FOIA, llegaría a la conclusión de que «el tipo de documentos que el Congreso pretendía incluir en la disposición relativa a la divulgación pública de la FOIA eran primordialmente aquellos que tratan de la estructura, funcionamiento y proceso de toma de decisiones de las diversas agencias gubernamentales». Y en la medida en que el material

[36] Véase Bloch-Wehba, H., *op. cit.*, nota 30, p. 1299.

[37] 887 F. Supp. 225 (N.D.Cal. 1995).

[38] En esta resolución —*U.S. Dept. of Justice v. Tax Analysts*, 492 U.S. 136 (1989)— el Tribunal Supremo consideró que sí debía atenderse la pretensión del solicitante de que la División de Impuestos del Departamento de Justicia le facilitase las decisiones en materia impositiva de todos los tribunales de distrito remitidas a la misma, al considerar que controlaba tales decisiones que recibía en su condición de parte en el proceso, incorporaba en su archivo de casos y utilizaba para posibles apelaciones de las sentencias.

pretendido de la biblioteca no encajaba en esta categorización, se desestimaría la petición de acceso a tal información.

Enfoque relativo a si el programa informático se incardina al objetivo perseguido por la Ley que utilizaría asimismo el Tribunal de Distrito de Columbia en la Sentencia de 16 de enero de 1996 (*Tax Analysts II*)[39], en la que se resolvió la solicitud dirigida al Departamento de Justicia para que revelase su sistema JURIS (*Justice Retrieval and Inquiry System*), una base de datos electrónica. El Tribunal apoyaría la decisión denegatoria de la Administración al considerar que no ostentaba un auténtico «control» de la base de datos, puesto que tenía muy restringidas sus facultades de disposición al respecto, razón por la cual no podía catalogarse propiamente como «documento de la agencia». Pero, una vez llegada a esta conclusión, abundaría en el argumento de la finalidad de la ley:

> «Finalmente, […] no es el tipo de información que el Congreso, al aprobar la FOIA, pretendía poner a disposición del público. Como ha declarado el Tribunal Supremo, `[e]l objetivo básico de [la] FOIA es garantizar una ciudadanía informada, vital para una sociedad democrática, que necesita controlar la corrupción y hacer a los gobernantes responsables ante sus gobernados´ […] La FOIA promueve la divulgación de aquella información que informe al público de lo que está haciendo el poder ejecutivo; esto es, que revele `información oficial´ sobre la estructura y el funcionamiento de las agencias […]. En este caso, el demandante no está buscando información sobre la estructura, el funcionamiento o los procesos de toma de decisiones del Departamento. Impedir el acceso a esta base de datos no permite al Departamento de Justicia aislarse del escrutinio público en relación con sus actividades y decisiones normativas. La base de datos no suministra información sobre la conducta del Departamento, y la divulgación de los datos no proyectaría ninguna luz sobre la conducta de ninguna agencia o funcionario».

Y, en fin, un esquema similar seguiría el Tribunal del Distrito Norte de California en la Sentencia *Gilmore,* al abordar la pretensión de acceder a CLERVER, un software de videoconferencia empleado por el Departamento de Energía[40]. Tras argumentar en torno a la falta de «control» del software por parte del Departamento, abundaría en la idea de que, aun cuando realmente hubiese estado bajo su control, tampoco podría considerarse un documento sujeto a la FOIA porque no suministraba «información sobre el funcionamiento, la estructura o los procesos de toma de decisiones del gobierno».

En **Alemania**, el tratamiento de la cuestión ha estado directamente condicionado por la conceptuación de «información oficial» realizada en la Ley federal reguladora del

[39] *Tax Analysts v. US Dept. of Justice*, 913 F. Supp. 599 (D.D.C. 1996).
[40] *Gilmore v. US Dept. of Energy*, 4 F. Supp. 2d 912 (N.D. Cal. 1998).

acceso a la información[41] —seguida generalizadamente por las leyes de los Länder—; o, para ser más exacto, de la interpretación jurisprudencial recaída sobre este concepto. Según se establece en su § 2(1), se entiende por «información oficial» en el sentido de dicha Ley «todo registro (*Aufzeichnung*) que sirva para fines oficiales, independientemente de cómo se almacene», y excluye expresamente del mismo a los borradores y notas que no formen parte de un procedimiento.

Una línea jurisprudencial ha tendido a considerar que los algoritmos no están cubiertos por el derecho de acceso, recurriendo para ello a una lectura estricta del requisito de que debe servir a una finalidad oficial para que pueda catalogarse una información como pública a los efectos de la Ley.

A esta dirección apunta ya la Sentencia del Tribunal Administrativo de Darmstadt, de 8 de mayo de 2019[42], en la que se resolvió un litigio que versaba sobre la pretensión de acceder al código fuente del programa «Polara», diseñado para el desarrollo, aplicación y funcionamiento operativo de procedimientos meteorológicos. La controversia tiene su origen en el proyecto de una empresa —dedicada a la construcción y explotación de centrales eólicas— de erigir determinadas instalaciones en una concreta localidad; proyecto cuya autorización sería denegada por la autoridad administrativa competente arguyendo que la altura diseñada afectaría al funcionamiento del radar que tenía en la localidad el Servicio Meteorológico Alemán, ya que podría interferir en los algoritmos automatizados de alerta, de tal suerte que podrían emitirse avisos meteorológicos no queridos. Fue en el contexto de esta controversia con la Administración cuando la empresa solicitaría información sobre la recogida y el tratamiento de los datos de dicho radar.

Debe notarse que, en la referida Sentencia, el órgano judicial se limitaría a exponer sus serias dudas acerca de que el código fuente satisficiera los requisitos impuestos por el transcrito § 2 de la Ley federal para ser considerado «información oficial», pues no sería esta la *ratio decidendi* que le llevaría a rechazar la pretensión del solicitante, sino el hecho de que el acceso perjudicaría los intereses fiscales del Bund en el tráfico mercantil (§ 3.6 de dicha Ley). Sea como fuere, la Sentencia pone el acento en la idea de que la información solicitada «se refiere a los detalles del procesamiento y tratamiento informáticos de los datos recogidos por el radar meteorológico, esto es, se refiere casi a los detalles sobre un medio de tratamiento, pero no al contenido de la información en sí». Y, siendo esto así, satisfacer la pretensión del solicitante «significaría que la autoridad no sólo tendría que dar la información oficial que adquiera como consecuencia del desempeño de sus tareas, sino también información sobre todos los medios de procesamiento y tratamiento, comenzando por el número de bolígrafos, lápices y hojas de papel, y pasando por las estructuras de los programas informáticos aplicados […]». En

[41] *Gesetz zur Regelung des Zugangs zu Informationen des Bundes (Informationsfreiheitsgesetz)*, de 5 de septiembre de 2005.

[42] VG Darmstadt, Urteil vom 08.05.2019 - 3 K 1708/17. DA.

suma, a juicio del Tribunal Administrativo de Darmstadt, resulta dudoso que estas modalidades o formas de tratamiento puedan reconducirse a la noción de «información oficial», toda vez que su definición legal apunta más al «contenido» y al «fin» del registro (*Aufzeichnung*) que a la «forma» del mismo (apartado 65).

Una clara asunción de la tesis de que los códigos fuente en sí mismos considerados son meros instrumentos técnicos exceptuados de la legislación de transparencia se desprende de la Sentencia del Tribunal Administrativo de Wiesbaden, de 17 de enero de 2022[43], en donde se ventilaba la pretensión de un profesor de acceder al código fuente de determinadas aplicaciones del portal web de las escuelas de Hesse[44]. Acceso que le sería denegado tras llegar a la conclusión de que el código fuente no es «información oficial» en el sentido de la Ley reguladora de la libertad de información y la protección de datos del Land de Hesse[45], cuyo § 80 (1) —siguiendo muy de cerca la definición del § 2 (1) de la Ley federal reguladora del acceso a la información— cataloga como «informaciones oficiales» todo registro que sirva para fines oficiales, con independencia del modo como se almacenen.

El Tribunal reconoce, ciertamente, que el código fuente resulta determinante para conocer el funcionamiento de un programa o una aplicación, y que debe catalogarse como un «registro oficial» a los efectos de la referida Ley (apartado 53); pero no cumple, sin embargo, el segundo de los requisitos necesarios para que pueda considerarse incluido en su ámbito de aplicación, a saber, que sirva para fines oficiales. Sencillamente, el objetivo del derecho de acceso a la información pública —mejorar el control de la actuación administrativa por parte de los ciudadanos— hace que no sea necesario incluir en el ámbito de aplicación de la ley todo lo que no pueda catalogarse como actuación administrativa (apartado 55). Y —prosigue argumentando la Sentencia en su apartado 56— «la posesión del registro del código fuente no es necesaria para el desempeño de tareas públicas, ni siquiera cuando se trabaje con un programa basado en él. Así, el Land de Hesse no tiene el código fuente del sistema operativo Windows, aunque el personal que trabaja en el ámbito de la tecnología de la información se apoye de forma absolutamente esencial en este producto. En otras palabras, la información no es necesaria para la actuación administrativa, como tampoco son información pública los datos sobre las características de los bolígrafos, de las puertas de las habitaciones o de las carrocerías de los automóviles de servicio».

Por otra parte, el Tribunal del Wiesbaden llega a la misma conclusión partiendo de una interpretación teleológica del concepto de «información oficial». «El control de la actuación pública —argumenta en el apartado 57— no requiere el conocimiento de las condiciones marco de la concreta actividad pública de que se trate. Para el control de la legalidad y también de la objetividad (*Sachgerechtigkeit*) de la

[43] VG Wiesbaden, Urteil vom 17.01.2022 - 6 K 784/21. WI.

[44] El portal está alojado en el Ministerio de Cultura de Hesse, apareciendo como organismo ejecutor del proyecto la Academia de profesores (*Lehrkräfteakademie*).

[45] *Hessisches Datenschutz- und Informationsfreiheitsgesetz* (HDSIG), de 3 de mayo de 2018.

actuación pública, es en principio irrelevante la calidad que tenga el material de trabajo de la Administración pública. El control de la legalidad y la objetividad sólo puede afectar al control del contenido de la actuación pública. El "fin oficial" se realiza con la utilización del programa por parte del personal de la Administración, pero no requiere conocer el código fuente, que resulta únicamente accesible a los expertos en tecnología informática».

Ahora bien, concluye su razonamiento en el apartado 58 de la Sentencia, «el Tribunal no desconoce que la adquisición de material defectuoso, llegado el caso, puede ser un asunto de interés público y podría fundamentar indirectamente el derecho de acceso a la información. Si la Administración demandada elaborase un informe sobre los defectos del software adquirido o el cumplimiento de los estándares de seguridad informática, este informe entraría indudablemente en el concepto de «información oficial», porque la finalidad de la elaboración del informe tiene una finalidad pública (presupuestaria). La Ley reguladora del acceso a la información de Hesse, sin embargo, no tiene por objetivo que los ciudadanos se pongan en lugar de la Administración y revisen por su propia iniciativa la calidad del material de trabajo, generando así, consiguientemente, desde el primer momento la información oficial».

Esta concepción más restrictiva de la noción de «información pública» a los efectos del derecho de acceso no se extiende, sin embargo, a otros países de nuestro entorno más próximo. Así sucede ciertamente en el caso de **Francia**. La *Commission d'accès aux documents administratifs* (en adelante, CADA) asumió con bastante naturalidad una interpretación amplia de la noción de «documentos administrativos» establecida en la Ley nº 78-753[46], que permitía aplicar la legislación de transparencia a las nuevas tecnologías informáticas empleadas en el proceso de toma de decisiones. Ya en un Dictamen fechado el 16 de octubre de 2014 (*Avis* 20142953), que resolvía la solicitud dirigida al Consejo General del Ródano de acceder a un programa informático que había sido desarrollado por una sociedad privada, no dudó en afirmar que su objeto revestía el carácter de documento administrativo y, por tanto, que resultaba accesible a la ciudadanía, salvo —claro está— que fuesen de aplicación alguno de los límites al acceso legalmente previstos[47].

Pero sería el Dictamen relativo al código fuente del software (*logiciel*) para el cálculo del impuesto sobre la renta de las personas física el que marcaría el punto de inflexión sobre el particular (*Avis* 20144578, de 8 de enero de 2015), en la medida en

[46] Loi n° 78-753 du 17 juillet 1978 portant diverses mesures d'amélioration des relations entre l'administration et le public et diverses dispositions d'ordre administratif, social et fiscal.

[47] La versión del entonces vigente artículo 1 de la Ley nº 78-753 decía así: «Sont considérés comme documents administratifs, au sens des chapitres Ier, III et IV du présent titre, quels que soient leur date, leur lieu de conservation, leur forme et leur support, les documents produits ou reçus, dans le cadre de leur mission de service public, par l'Etat, les collectivités territoriales ainsi que par les autres personnes de droit public ou les personnes de droit privé chargées d'une telle mission. Constituent de tels documents notamment les dossiers, rapports, études, comptes rendus, procès-verbaux, statistiques, directives, instructions, circulaires, notes et réponses ministérielles, correspondances, avis, prévisions et decisions».

que sería respaldado jurisprudencialmente. En efecto, esta resolución sería confirmada por el Tribunal Administrativo de París en la Sentencia de 10 de marzo de 2016[48], que vendría en consecuencia a imponer a la dirección general de finanzas públicas que comunicase al solicitante la información pretendida. Decisión a la que llegaría el Tribunal a partir de la amplia definición del concepto de documento administrativo establecida en el artículo 1 de la Ley nº 78-753, y tras valorar el hecho de que el código fuente de los programas informáticos no figurase en el listado de documentos no comunicables contenido en el artículo 6 de dicha Ley. Por lo demás, rechazó asimismo la alegación de la Administración de que se trataba de un software inacabado que se hallaba en constante evolución; sencillamente, a juicio del Tribunal, «cada versión del código fuente de un mismo programa informático reviste el carácter de documento administrativo finalizado y puede ser comunicado en ese estado».

Y poco después la CADA, en el *Avis* 20161990 de 23 de junio de 2016, insistiría en que los ficheros informáticos que contenían el código fuente o algoritmo solicitado —producidos por el Instituto tecnológico de Toulouse para el ministerio de educación nacional— eran «documentos administrativos» en el sentido del artículo L300-2 del «Código de relaciones entre el público y la administración».

En consecuencia, la sucesión de estas tres decisiones de la CADA ponía claramente de manifiesto que los programas informáticos en general, y más específicamente los algoritmos y códigos fuente que los integran, se hallan bajo el ámbito de cobertura del sistema francés de transparencia[49]. Posición que, por lo demás, como hemos comprobado, se había visto ratificada jurisprudencialmente.

Con todo, el legislador francés creyó conveniente elevar de forma expresa esta lectura amplia de la noción de «documentos administrativos» a la propia legislación, y, así, el artículo 2 de la Ley nº 2016/132, de 7 de octubre de 2016, para una República digital, vino a modificar el artículo L300-2 del «Código de relaciones entre el público y la administración» para incorporar explícitamente al código fuente[50].

Antes de dar por terminadas estas líneas referentes al tratamiento de la cuestión en Francia, resulta conveniente anotar un asunto complementario al del acceso directo a los algoritmos o códigos fuente, a saber, que la legislación francesa también recoge

[48] Tribunal Administratif de Paris (5ème section — 2ème chambre). N°1508951/5-2. Lecture du 10 mars 2016.

[49] Y, más concretamente, las dos últimas decisiones las utiliza la CADA sistemáticamente como referencia en este tipo de asuntos, convirtiéndose casi en una cláusula de estilo. Véanse, por ejemplo, *Avis* 20180276, de 19 de abril de 2018; *Avis* 20182093, de 6 de septiembre de 2018; *Avis* 20203492, de 19 de noviembre de 2020; *Avis* 20204274, de 10 de diciembre de 2020; *Avis* 21210021, de 15 de abril de 2021.

[50] «Sont considérés comme documents administratifs, au sens des titres Ier, III et IV du présent livre, quels que soient leur date, leur lieu de conservation, leur forme et leur support, les documents produits ou reçus, dans le cadre de leur mission de service public, par l'Etat, les collectivités territoriales ainsi que par les autres personnes de droit public ou les personnes de droit privé chargées d'une telle mission. Constituent de tels documents notamment les dossiers, rapports, études, comptes rendus, procès-verbaux, statistiques, instructions, circulaires, notes et réponses ministérielles, correspondances, avis, prévisions, codes sources et decisions».

explícitamente la exigencia de que las Administraciones ofrezcan a los interesados información sobre el funcionamiento de los sistemas automatizados de toma de decisiones. Con ello, la legislación francesa viene a dar cumplimiento en el ámbito del sector público a las obligaciones de transparencia que impone al respecto el Reglamento General de Protección de Datos —a las que tuvimos ocasión de aproximarnos páginas atrás—, aunque ampliando notablemente su radio de acción, habida cuenta de que se proyectan también a las decisiones no totalmente automatizadas y a los casos en que los afectados por la decisión son personas jurídicas.

Así es; la recién citada Ley nº 2016/132, para una República digital, añadiría el artículo L311-3-1 al «Código de relaciones entre el público y la administración», en cuya virtud «una decisión individual adoptada sobre la base de un tratamiento algorítmico deberá incluir una declaración explícita en la que se informe al interesado. Las reglas que definen este tratamiento, así como las principales características de su aplicación, serán comunicadas por la administración al interesado si éste lo solicita».

Y el Decreto del Consejo de Estado nº 2017-330, de 14 de marzo de 2017, relativo a los derechos de las personas que sean objeto de decisiones individuales adoptadas sobre la base de un tratamiento algorítmico, fijaría las condiciones de aplicación de dicho artículo. Por una parte, incorporaría al «Código de relaciones entre el público y la administración» el artículo R311-3-1: «La mención explícita prevista en el artículo L. 311-3-1 indica la finalidad perseguida por el tratamiento algorítmico. Recuerda el derecho, garantizado por este artículo, a obtener la comunicación de las reglas que definen este tratamiento y las principales características de su aplicación, así como las modalidades de ejercicio de este derecho a la comunicación y de reclamar, en su caso, a la "Comisión de acceso a los documentos administrativos", tal como se define en este libro». Y, por otro lado, dicho Decreto introdujo asimismo el artículo R311-3-2: «La administración comunicará a la persona que sea objeto de una decisión individual adoptada con base en un tratamiento algorítmico, a petición de esta, de forma inteligible y siempre que no vulnere secretos protegidos por la ley, la siguiente información: «1º el grado y modo de contribución del tratamiento algorítmico a la toma de decisiones; 2º los datos tratados y sus fuentes; 3º los parámetros del tratamiento y, en su caso, su ponderación, aplicados a la situación del interesado; 4º las operaciones realizadas por el tratamiento».

Estas exigencias de transparencia, que entraron en vigor el 1 de septiembre de 2017, muy pronto demostraron su eficacia en la práctica, como lo acredita que ya el 30 de noviembre de dicho año la CADA estimara la pretensión de los solicitantes de acceder al sistema automatizado empleado por la Academia de Versalles en el procedimiento de selección del alumnado[51]. Otra muestra de la operatividad de esta reforma normativa proporciona el dictamen de la CADA de 10 de diciembre de 2020, que resolvió asimismo de modo favorable la petición, dirigida a la Academia de Poitiers, de

[51] *Avis* 20173235, de 30 de noviembre de 2017.

que se comunicara a la interesada las reglas y principales características de aplicación del algoritmo empleado para el examen de las solicitudes de traslado[52].

También en **Italia** se ha impuesto una lectura pro transparencia del concepto de «documento administrativo» establecido en la normativa reguladora del derecho de acceso, según la cual se entiende por tal «toda representación gráfica, fotocinematográfica, electromagnética o de cualquier otro tipo del contenido de los actos»[53].

A la hora de determinar si los algoritmos utilizados en la toma de decisiones podían reconducirse a dicha categoría, dos fueron las posiciones defendidas por la doctrina italiana. Por una parte, una tendencia —que era en principio mayoritaria— que concibe a los programas informáticos como simples herramientas técnicas, en las que sus desarrolladores se limitan a ejecutar las instrucciones del poder adjudicador contenidas en los actos administrativos establecidos a tal objeto; y, por otro lado, la tesis que considera que los programas informáticos son por sí mismos actos administrativos, en la medida en que expresan la voluntad de la administración condicionada al acaecimiento de hechos exactamente identificados en el correspondiente programa[54].

A la segunda de las posiciones referidas se ha inclinado con claridad la jurisprudencia recaída al respecto.

Determinante en la conformación de esta línea jurisprudencial ha sido sin duda la Sentencia del Tribunal Administrativo Regional para el Lazio (Sección tercera bis), de 22 de marzo de 2017 (Nº 3769), que abordó la pretensión del recurrente de conocer el sistema algorítmico utilizado por el Ministerio de Educación en materia de movilidad del personal docente[55]. Lo cierto es que la Administración interpelada había facilitado al solicitante cierta información sobre el procedimiento algorítmico, pero a juicio del Tribunal la mera descripción del algoritmo y de su funcionamiento no podía considerarse una respuesta suficiente, puesto que únicamente conociendo su código fuente podía valorarse adecuadamente su funcionalidad o los eventuales errores de programación. Así, pues, el grueso de la argumentación se centró en torno a la alegación del Ministerio de que el código fuente del programa en cuestión no podía asimilarse a un «documento administrativo» en el sentido del art. 22.1.d) de la Ley 241/90; disposición que —según el Ministerio— identifica las formas en que puede manifestarse un

---

[52] *Avis* 20204274.

[53] Según reza el artículo 22.1.d) de la Ley n. 241, de 7 de agosto de 1990, reguladora del derecho de acceso a los documentos administrativos, se entiende «d) per «documento amministrativo», ogni rappresentazione grafica, fotocinematografica, elettromagnetica o di qualunque altra specie del contenuto di atti, anche interni o non relativi ad uno specifico procedimento, detenuti da una pubblica amministrazione e concernenti attivita' di pubblico interesse, indipendentemente dalla natura pubblicistica o privatistica della loro disciplina sostanziale».

[54] Reproduzco la síntesis de las posiciones doctrinales expuesta por Mancosu, G., «Les algorithmes publics déterministes au prisme du cas italien de la mobilité des enseignants», en: *Rivista italiana di informática e diritto*, Fascicolo 1-2019, p. 77.

[55] Véase, por ejemplo, el comentario de Iaselle, M., «Diritti di accesso all'algoritmo, TAR Lazio apre nuovi scenari», *Altalex* 17 de mayo de 2017 (https://www.altalex.com/documents/news/2017/05/17/diritto-di-accesso-algoritmo).

acto administrativo, pero entendiéndose que el objeto del acceso sólo puede serlo el acto que por su naturaleza sea calificable como administrativo, lo que no es predicable del código fuente.

El Tribunal, sin embargo, tras una detenida y muy pedagógica argumentación, terminaría reconociendo que «el software que gestiona el algoritmo» es directamente reconducible a la categoría de «acto administrativo electrónico»[56] en el contexto del reiterado art. 22.1.d) de la Ley 241/90. Conclusión a la que llega tras rechazar expresamente la tesis estricta defendida por la doctrina en relación con el «acto administrativo electrónico», según la cual únicamente puede calificarse como tal el «acto administrativo en forma electrónica». A juicio del órgano judicial, por el contrario, también responde a tal naturaleza el «acto de elaboración electrónica», esto es, el acto administrativo cuyo contenido es elaborado a través de un sistema informático, con independencia de que el documento final resultante del proceso de elaboración pueda adoptar cualquier forma permitida en el ordenamiento[57].

Entre otras argumentaciones, la calificación del software como acto administrativo informático la fundamentó el órgano judicial en consideraciones tales como que es con el software como se concreta la voluntad final de la Administración, y es con él, en definitiva, como la Administración constituye, modifica o extingue las situaciones jurídicas individuales incluso si el mismo no produce efectos directos hacia el exterior; y, en fin, apuntó asimismo el Tribunal que el software termina por identificarse y concretar el propio procedimiento.

De interés son también otras consideraciones vertidas en la Sentencia, señaladamente la de que el hecho de que el software sea difícilmente comprensible para una persona no experta no es motivo para denegar su acceso directo al mismo. Pues, como razona el Tribunal, por una parte, esta circunstancia no es sino consecuencia de la elección de la Administración de recurrir a este instrumento para la gestión de un procedimiento de su competencia; y, por otro lado, en lo concerniente a su comprensión y a la verificación de su corrección, el destinatario del acto puede, en particular, recurrir legítimamente a la actividad profesional de un informático competente en la materia[58].

A partir de esta Sentencia del TAR Lazio se ha consolidado en la jurisprudencia la tesis de que los algoritmos son reconducibles al concepto de acto administrativo. Así, el Consejo de Estado (Sección Sexta) vendría ya a sumarse a esta posición en su Sen-

---

[56] Viola, L., «L'intelligenza artificiale nel procedimento e nel processo amministrativo: lo stato dell'arte», *federalismi.it*. *Rivista di Diritto Pubblico italiano, comparato, europeo*, núm. 21, 2018, p. 2 y ss.

[57] Sobre esta distinción entre «acto administrativo en forma electrónica» y «acto de elaboración electrónica», consúltese Giurdanella, C.; Guarnaccia, E., *Elementi di diritto amministrativo elettronico*, Halley, Matelica, 2005, pp. 13-14.

[58] Para un análisis más detallado de esta relevante Sentencia, puede consultarse Noto la Diega, G., «Against the Dehumanisation of Decision-Making — Algorithmic Decisions at the Crossroads of Intellectual Property, Data Protection, and Freedom of Information», en: *Journal of Intellectual Property, Information Technology and E-Commerce Law (JIPITEC)*, 9, 2018, apartados 97-99.

tencia 2270/2019, de 8 de abril, (N. 04477/2017 REG.RIC.), en donde afirma categóricamente: «l'algoritmo, ossia il *software*, deve essere considerato a tutti gli effetti come un "atto amministrativo informatico"»[59].

Comoquiera que sea, el relativamente amplio número de Sentencias del Consejo de Estado que se ocupan del empleo de algoritmos en el sector público abordan de forma mayoritaria el tema de la transparencia, no exclusivamente desde la perspectiva del puro y directo conocimiento de los mismos derivado del ejercicio del derecho de acceso a la información pública, sino desde un enfoque más general[60] que, a menudo, el Consejo vincula expresamente con la normativa reguladora de la protección de datos personales. En este sentido, la Sentencia del Consejo de Estado (Sección Sexta), de 13 de diciembre de 2019, n. 8472 (N. 02936/2019 REG.RIC), insiste en la relevancia del principio de transparencia en este ámbito (FJ 13.1), con continuas referencias a la regulación de la materia que realiza el Reglamento General de Protección de Datos (FFJJ 13.2, 13.3 y 14)[61]. Normativa europea de la que infiere, entre otros, el «principio de cognoscibilidad», que en última instancia reclama que la fórmula técnica en que consiste el algoritmo sea explicada de forma comprensible[62]. Este hilo argumental viene sosteniéndose ininterrumpidamente por el Consejo de Estado en sus resoluciones dictadas hasta la fecha (Sentencias 2270/2019, 8472/2019, 8473/2019, 8474/2019, 881/2020 y 1206/2021)[63].

III.1.2. *El estado de la cuestión en el ordenamiento español*

a) El acceso directo a los algoritmos y a los códigos fuente

En el caso de España, la asunción de la tesis de que los algoritmos utilizados en la toma de decisiones constituyen «información pública» a los efectos de la legislación reguladora de la transparencia se ha visto sin duda facilitada por los amplios términos con que el artículo 13 LTAIBG define dicho concepto: «Se entiende por información

[59] Véase el comentario a esta Sentencia de Chiacchio, M. G., «L'utilizzo dell'algoritmo nelle procedure valutative della PA (Commento a Consiglio di Stato, Sez. VI, Sent. 8 aprile 2019, N. 2270)», en: *European Journal of Privacy Law & Technologies* 2019/2, pp. 137-143.

[60] Sencillamente, el algoritmo está sujeto a los principios rectores de la actividad administrativa establecidos en el artículo 1 de la Ley 241/1990, entre los que se encuentra el principio de transparencia.

[61] Sobre esta Sentencia, véase Vestri, G., «La inteligencia artificial ante el desafío de la transparencia algorítmica. Una aproximación desde la perspectiva jurídico-administrativa», en: *Revista Aragonesa de Administración Pública*, núm. 56, 2021, pp. 379-380 y 386.

[62] Esta argumentación a partir de la normativa de la Unión Europea en materia de protección de datos también se halla presente en la Sentencia del Tribunal Administrativo Regional de la Campania (Sección tercera), de 14 de noviembre de 2022, n. 7003.

[63] Acerca de esta línea jurisprudencial, consúltese Rum, A. L., «Il provvedimento amministrativo adottato mediante algoritmo: il ruolo dell'intelligenza artificiale nel proceso decisionale della P.A.», en: *Il Diritto Amministrativo. Rivista Giuridica*, Año XV, n. 02, Febbraio 2023.

pública los contenidos o documentos, cualquiera que sea su formato o soporte, que obren en poder de alguno de los sujetos incluidos en el ámbito de aplicación de este título y que hayan sido elaborados o adquiridos en el ejercicio de sus funciones». Concepción amplia de la noción de información pública que —como no podía ser de otra manera dada su condición de norma básica— se incorporó a las diferentes leyes autonómicas reguladoras de la transparencia.

Y, de hecho, fue una autoridad de control autonómica —la Comisión de garantía del derecho de acceso a la información pública catalana, en adelante GAIP— la que por vez primera abordó el examen de solicitudes de información cuyo objeto era acceder a algoritmos. La ocasión se le presentó con motivo de las diversas reclamaciones formuladas por el mismo ciudadano a propósito de la misma pretensión: conocer el algoritmo matemático que determinaba el orden de posiciones en los tribunales correctores de las pruebas de acceso a la universidad. La GAIP en la Resolución de 21 de septiembre de 2016 (Reclamación 124/2016) reconocería el derecho de acceso del reclamante, pero, tras responder la Administración que no existía el pretendido «algoritmo matemático», el interesado volvería a concretar su pretensión, llegando finalmente a solicitar directamente el código fuente del programa informático. La Resolución 200/2017, de 21 de junio, resolvería de este modo la cuestión en su fundamento jurídico segundo:

> «Se tiene que reconocer el derecho de la persona reclamante a acceder al código fuente del programa informático empleado por el Consejo Interuniversitario en la designación de los miembros de los tribunales correctores de las PAU, por razones similares a las que llevaron, a la Resolución de esta Comisión de 21 de septiembre de 2016, a estimar la Reclamación 124/2016 y declarar el derecho a conocer el algoritmo matemático implementado por el mencionado programa informático. El código fuente de un programa informático empleado por la Administración en la designación de los miembros de tribunales evaluadores constituye información pública a los efectos del artículo 2.b de la Ley 19/2014, del 29 de diciembre, de transparencia, acceso a la información pública y buen gobierno (LTAIPBG). Según este precepto, se entiende por información pública «la información elaborada por la Administración y la que esta tiene en su poder como consecuencia de su actividad o del ejercicio de sus funciones, incluida la que le suministran los otros sujetos obligados de acuerdo con el que establece esta ley». Esta definición incluye toda la información que la Administración elabore o tenga en su poder en ejercicio de sus funciones, con independencia del lenguaje o forma en que se exprese. La información pública incluye así, no solo aquella que se expresa en lenguaje natural (en palabras, que es la más habitual), sino también la expresada mediante fotografías, videos, planos, señales, etc. o mediante otros lenguajes, como el matemático o, en este caso, el informático. El artículo 19.1 LTAIPBG confirma esta noción amplia de información pública cuando dispone que «el derecho de acceso a la información pública incluye cualquier forma o soporte en

> que esta información haya sido elaborada o en que se conserve». Lo mismo se desprende del artículo 13 de la Ley básica estatal 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno, cuando establece que «se entiende por información pública los contenidos o documentos, cualquiera que sea su formato o soporte, que obren en poder de alguno de los sujetos incluidos en el ámbito de aplicación de este título y que hayan sido elaborados o adquiridos en el ejercicio de sus funciones»[64].

La cita, aunque larga, ha merecido la pena, porque revela que, desde una fecha temprana, la GAIP asumió con naturalidad con base en su tenor literal la viabilidad de la legislación de transparencia para conocer los algoritmos utilizados en el proceso de toma de decisiones, por más que difícilmente pudieran catalogarse como «documentos» en sentido estricto. Y, así, aunque no constituyera el acceso a ningún algoritmo o código fuente el objeto de la controversia, en la Resolución 93/2019, de 22 de junio, se hace referencia a esta cuestión de modo incidental cuando se aborda con carácter general en su fundamento jurídico tercero el «alcance material del concepto de información pública como objeto del derecho de acceso»:

> «[…] el concepto de información trasciende el tradicional de documentos y es sustancialmente equivalente al de conocimiento, por lo que el derecho de acceso se proyecta, ciertamente, sobre los documentos en poder de la Administración, pero también sobre el otro conocimiento que esté en poder de la Administración municipal, tales como bases de datos informáticas, algoritmos o conocimiento material no formalizado en ningún documento o registro determinado […]»[65].

Habría que esperar más tiempo para que se plantease una cuestión de semejante tenor ante el CTBG. Sería específicamente con ocasión de la reclamación presentada por la Fundación Civio ante la decisión del Ministerio para la Transición Ecológica de denegar su pretensión de acceder al código fuente relativo a la aplicación telemática del bono social. Entre otras razones, el Ministerio rechazó la solicitud al sostener que el código fuente «no se considera información pública según el artículo 13 de la Ley de transparencia al no ser ni "contenidos" ni "documentos", sino programas informáticos» (Resolución 701/2018, de 18 de febrero de 2019, Antecedente 3). Sin embargo, el CTBG no entró directamente a argumentar sobre el particular, sino que resolvió examinando la pertinencia de la aplicación de los límites que asimismo había invocado el Ministerio para desestimar la solicitud, dando así por sentado que, en efecto, el código fuente debía considerarse información pública a los efectos de la LTAIBG.

---

[64] En relación con esta Resolución, véase Ponce Solé, *op. cit.*, nota 24, p. 43.

[65] Sobre la doctrina de la GAIP al respecto, Cerrillo i Martínez, A., «La transparencia de los algoritmos que utilizan las administraciones públicas», en: Camp Batalla, R. (ed.), *Anuario de Transparencia Local*, Vol. 3/2020, Fundación Democracia y Gobierno Local, Madrid/Barcelona, 2021.

Fue, por tanto, en la Resolución 58/2021 cuando, al elucidar la pretensión de acceder al algoritmo empleado para el cálculo de las pensiones, el CTBG por vez primera argumentaría expresamente la cobertura de esta suerte de peticiones en el marco del artículo 13 LTAIBG en línea con lo sostenido por la GAIP:

> «Existe unanimidad en considerar que la noción de «información pública» empleada por su artículo 13 ha superado la enteca concepción que del derecho de acceso se contemplaba en el artículo 37.1 de la hoy derogada Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, dando un relevante salto cualitativo y cuantitativo respecto del régimen de acceso inmediatamente precedente, en cuanto el objeto del derecho ya no son sólo los documentos, sino que incluye también la información no documentalizada, extendiendo el ámbito material del derecho desde la noción de documento a la de información en poder del sujeto obligado, con independencia de cuáles sean sus características técnicas (formato) o el material en el que se registre (soporte)» (FJ 4º).

A partir de entonces, se trata de una cuestión no controvertida y, por tanto, se parte de la premisa de que los algoritmos y códigos fuente constituyen información pública a los efectos de la legislación reguladora de la transparencia sin necesidad de proceder a una detallada justificación de esta calificación (así, por ejemplo, las Resoluciones del CTBG 253/2021, FJ 4º y 7/2023, FJ 3º).

Por lo demás, la divulgación directa e inmediata del algoritmo o su código fuente constituye, en opinión de la propia autoridad independiente de control, la fórmula idónea para asegurar la finalidad sustancial perseguida por nuestro sistema de transparencia. Así se reconoce de forma inequívoca en la Resolución 58/2021 del Consejo de Transparencia y Buen Gobierno:

> «En el contexto actual de progresivo desarrollo e implantación la administración electrónica y uso creciente de la inteligencia artificial, los algoritmos están adquiriendo una relevancia decisiva, a la vez que se incrementa su complejidad. Pueden sustentar la toma de decisiones públicas o, directamente, ser fuente de decisiones automatizadas con consecuencias muy relevantes para las personas. Esta evolución está generando una creciente demanda ciudadana de transparencia de los algoritmos utilizados por las Administraciones públicas como condición inexcusable para preservar la rendición de cuentas y la fiscalización de las decisiones de los poderes públicos y, en último término, como garantía efectiva frente a la frente a la arbitrariedad o los sesgos discriminatorios en la toma de decisiones total o parcialmente automatizadas.
>
> Mientras no se instauren otros mecanismos que permitan alcanzar los fines señalados con garantías equivalentes —como podrían ser, por ejemplo, auditorías independientes u órganos de supervisión—, el único recurso eficaz a tales efectos

> es el acceso al algoritmo propiamente dicho, a su código, para su fiscalización tanto por quienes se puedan sentir perjudicados por sus resultados como por la ciudadanía en general en aras de la observancia de principios éticos y de justicia» (FJ 5º; véase asimismo la Resolución 7/2023, FJ 4º).

Pero, obviamente, no es ésta la única vía que puede ser transitada al objeto de conseguir arrojar alguna luz sobre los sistemas automatizados de toma de decisiones empleados por las Administraciones públicas. En principio, nada impide que la ciudadanía no pretenda tanto acceder, sin más, al entero algoritmo como lograr que se le ofrezca alguna información sobre su funcionamiento.

b) La pretensión de conocer el funcionamiento del sistema algorítmico

Ciertamente, con base en la LTAIBG (artículo 13: «contenidos o documentos»), cabe también barajar la posibilidad de que se solicite de la Administración, no ya directamente el acceso al propio algoritmo o a su código fuente, sino que proporcione determinada información sobre el funcionamiento del mismo. En el caso de que el solicitante de la información sea la persona afectada por la decisión administrativa, es evidente que nos encontramos con un supuesto muy próximo al derecho de recibir «información significativa sobre la lógica aplicada» [art. 15.1.h) RGPD] o al pretendido «derecho a la explicación» que cabría derivar de este precepto en conexión con el artículo 22.3 y el Considerando 71 RGPD, según tuvimos ocasión de comprobar páginas arriba. Aunque, naturalmente, en el marco de la legislación de transparencia no opera ninguna de las relevantes restricciones que condicionan estos derechos de información bajo la normativa reguladora del derecho a la protección de datos personales, a saber, circunscribirse a las personas físicas y a las decisiones totalmente automatizadas.

Y, sin embargo, las posibilidades de que prospere este tipo de peticiones de información pueden encontrar un serio obstáculo en la causa de inadmisión establecida en el art. 18.1.c) LTAIBG («información para cuya divulgación sea necesaria una acción previa de reelaboración»).

Como es sabido, a propósito de este motivo de inadmisión el Consejo de Transparencia y Buen Gobierno elaboró el Criterio Interpretativo 7/2015, de 12 de noviembre, en el que se apuntan dos principales líneas orientadoras para identificar los casos de «reelaboración»: 1º) cuando la información tenga que «[e]laborarse expresamente para dar una respuesta, haciendo uso de diversas fuentes de información»; y 2º) cuando la Administración interpelada «carezca de los medios técnicos que sean necesarios para extraer y explotar la información concreta que se solicita, resultando imposible proporcionar la información solicitada». En lo concerniente al primero de los criterios mencionados, cabe apuntar que, si bien en una primera fase prevaleció una aplicación

de esta causa de inadmisión apegada a su tenor literal, lo cierto es que —impulsada por los pronunciamientos judiciales recaídos al respecto[66]— se ha abierto paso otra línea interpretativa que, soslayando la concurrencia de la pluralidad de las fuentes, se centra en valorar si atender la petición supone la elaboración de un informe *ex novo*. Por consiguiente, cuando satisfacer la pretensión del solicitante requiere una labor de confeccionar *ex profeso* un documento, siempre que vaya más allá de la mera agregación o suma de datos, podrá fundadamente invocarse esta causa de inadmisión[67].

Así, pues, salvo —claro está— que la explicación del funcionamiento del sistema algorítmico la tenga ya documentada la Administración, muy probablemente solicitudes de esta índole podrían ser inadmitidas a trámite con base en el art. 18.1.c) LTAIBG.

Y se trata de una alternativa que puede resultar de suma utilidad, pues, como comprobaremos al examinar los límites al derecho de acceso, algunos de ellos muestran una gran virtualidad cuando lo que pretende el solicitante es acceder al entero algoritmo o a su núcleo esencial, el código fuente.

Para dejar expedita la vía a la tramitación de solicitudes cuyo objetivo sea la explicación del funcionamiento algorítmico, parece que no queda otra opción que seguir el modelo francés y, por tanto, reconocer explícitamente en la normativa este tipo de pretensiones. Según adelantamos líneas arriba, la Ley nº 2016/132, de 7 de octubre de 2016, para una República digital, incorporó el artículo L311-3-1 al «Código de relaciones entre el público y la administración», en cuya virtud el afectado por una decisión tomada con base en un tratamiento algorítmico puede solicitar «[l]as reglas que definen este tratamiento, así como las principales características de su aplicación». Y el Decreto del Consejo de Estado nº 2017-330, de 14 de marzo de 2017, que desarrolló dicho artículo L311-3-1, añadiría al «Código de relaciones entre el público y la administración» el artículo R311-3-2, que precisa del siguiente modo el alcance de la infor-

---

[66] A partir de la Sentencia de la Audiencia Nacional 29/2017, de 24 de enero de 2017 (Nº recurso 63/2016), en cuyo FJ 4º se afirma que «el mencionado art.18.1.c permite la inadmisión de una solicitud cuando la información que se solicita requiere una elaboración y tarea de confección por no ser fácilmente asequible acceder a ella».

[67] Para más detalles sobre la evolución experimentada en la aplicación de este motivo de inadmisión, véase el muy documentado trabajo de Guichot, E.; Barrero Rodríguez, C., *El derecho de acceso a la información pública*, Tirant lo Blanch, Valencia, 2020, pp. 572-604. Como es obvio, la Administración podrá libremente dar una explicación sobre el funcionamiento de la aplicación informática objeto de la solicitud de información, con independencia de que la tenga ya documentada o la elabore *ex profeso* para satisfacer la pretensión del solicitante. A este respecto cabe mencionar la Resolución del CTBG 7/2023, que trajo causa de una petición de acceder al código fuente asociado al algoritmo que calcula los días cotizados utilizado por el SEPE; petición a la que la Administración respondió ofreciendo una explicación sobre el criterio empleado para el cálculo de los días de cotización. El CTBG concluiría en su FJ 6º estimando la reclamación, «a fin de que el órgano requerido añada a la información ya aportada copia del código fuente asociado al algoritmo de cálculo de los días cotizados, entendiendo como tal la explicación del conjunto de reglas internas (técnico-jurídicas) de la aplicación informática utilizada para dicho cálculo» (crítico en relación con esta argumentación se muestra Huergo Lora, A., «El derecho de transparencia en el acceso a los códigos fuente», en: *Anuario de Transparencia Local 5/2022*, Fundación Democracia y Gobierno Local, Madrid, 2023, p. 63).

mación a suministrar: «La administración comunicará a la persona que sea objeto de una decisión individual adoptada con base en un tratamiento algorítmico, a petición de esta, de forma inteligible y siempre que no vulnere secretos protegidos por la ley, la siguiente información: «1º el grado y modo de contribución del tratamiento algorítmico a la toma de decisiones; 2º los datos tratados y sus fuentes; 3º los parámetros del tratamiento y, en su caso, su ponderación, aplicados a la situación del interesado; 4º las operaciones realizadas por el tratamiento».

En resumidas cuentas, a nuestro juicio, sería una iniciativa plausible que se llevasen unas previsiones similares a la —tantas veces anunciada como aplazada— futura reforma de la LTAIBG; e, incluso, dando un paso más, que la capacidad de presentar solicitudes de esta naturaleza no se circunscribiese a los concretos interesados, sino que se ampliase a titulares cualificados del derecho de acceso, como la prensa y las entidades especializadas en la esfera de la transparencia.

c) La publicidad activa

Tal y como adelantamos al comienzo de este trabajo, la Carta de Derechos Digitales expresa en términos inequívocos la conveniencia de potenciar la transparencia algorítmica en el pilar de la publicidad activa[68].

No debe de ser motivo de sorpresa esta apelación a mejorar esta proyección de la transparencia, habida cuenta de la reducida presencia que tiene hasta la fecha en nuestro ordenamiento jurídico. E incluso, paradójicamente, en algún aspecto cabe afirmar que la transparencia algorítmica ha vivido mejores tiempos en el pasado. En efecto, hoy por hoy se carece de un precepto como el que incorporaba ya en su versión inicial la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, en su artículo 45.4: «Los programas y aplicaciones electrónicos, informáticos y telemáticos que vayan a ser utilizados por las Administraciones Públicas para el ejercicio de sus potestades, habrán de ser previamente aprobados por el órgano competente, quien deberá difundir públicamente sus características»[69]. Divulgación pública obligatoria de las «características» de los

[68] Según establece el segundo apartado de su artículo XVIII («Derechos digitales de la ciudadanía en sus relaciones con las Administraciones Públicas»): «El principio de transparencia y de reutilización de datos de las Administraciones públicas guiará la actuación de la Administración digital, de conformidad con la normativa sectorial. En particular, se garantizará el derecho de acceso a la información pública, se promoverá la publicidad activa y la rendición de cuentas y se velará por la portabilidad de los datos y la interoperabilidad de los formatos, sistemas y aplicaciones, en los términos que prevea el ordenamiento jurídico vigente».

[69] Ninguna obligación semejante se refleja ahora en el artículo 41 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, al regular la actuación administrativa automatizada. Su artículo 157.2 sí prevé que las aplicaciones desarrolladas por las Administraciones o que hayan sido objeto de contratación y de cuyos derechos de propiedad intelectual sean titulares *puedan* ser declaradas «como de

programas y aplicaciones informáticas que evidentemente podría haber supuesto, al menos sobre el papel, un notable avance en el conocimiento de su funcionamiento por parte de la ciudadanía[70].

De hecho, en la redacción inicial del Capítulo II del Título I de la LTAIBG (dedicado al a la «Publicidad activa») no era posible hallar ninguna referencia de la que se pudiera derivar una obligación de llevar a los portales de transparencia información sobre algoritmos[71]. Algún avance al respecto[72] se produjo, sin embargo, con ocasión de la aprobación de la Ley Orgánica 3/2018, de Protección de Datos y garantía de derechos digitales, toda vez que su artículo 31.2 impone a las diferentes Administraciones, entre otros integrantes del sector público, que hagan «público un inventario de sus actividades de tratamiento accesible por medios electrónicos en el que constará la información establecida en el artículo 30 del Reglamento (UE) 2016/679 y su base legal». Y a fin de cohonestar esta disposición con la LTAIBG, la Disposición final undécima de la LO 3/2018 procedió a su modificación añadiendo un nuevo artículo 6 bis, que viene a incorporar expresamente al listado de obligaciones de publicidad activa la exigencia de publicar el «inventario de actividades de tratamiento».

---

fuentes abiertas, cuando de ello se derive una mayor transparencia en el funcionamiento de la Administración Pública o se fomente con ello la incorporación de los ciudadanos a la Sociedad de la información».

Sobre este tema puede ser de interés mencionar el régimen de las condiciones de licenciamiento de las aplicaciones informáticas establecido en el Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica (tras su modificación por el 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). El artículo 16 del Real Decreto 4/2010 tiene por objeto regular las «condiciones de licenciamiento de las aplicaciones informáticas, documentación asociada, y cualquier otro objeto de información cuya titularidad de los derechos de la propiedad intelectual sea de una Administración Pública y permita su puesta a disposición de otra Administración y de los ciudadanos» (apartado primero); y sobre este particular el art. 16.2 establece que «[l]as Administraciones Públicas utilizarán para las aplicaciones informáticas, documentación asociada, y cualquier otro objeto de información declarados como de fuentes abiertas aquellas licencias que aseguren que los programas, datos o información cumplen los siguientes requisitos: […] b) Permiten conocer su código fuente». Y el apartado cuarto de este artículo 16 dispone finalmente: «A efectos de facilitar el establecimiento de las condiciones de licenciamiento, las Administraciones Públicas incluirán en los pliegos de cláusulas técnicas de aquellos contratos que tengan por finalidad el desarrollo de nuevas aplicaciones informáticas, los siguientes aspectos: a) Que la Administración contratante adquiera los derechos completos de propiedad intelectual de las aplicaciones y cualquier otro objeto de información que se desarrollen como objeto de ese contrato».

[70] Gutiérrez David, M. E., *op. cit.*, nota 10, p. 178.

[71] Aunque no faltaron notables esfuerzos hermenéuticos espoleados por la razonable finalidad de paliar la opacidad existente en este ámbito. Así, se apuntó que los algoritmos y códigos fuente podían considerarse «información cuyo conocimiento sea relevante para garantizar la transparencia de su actividad relacionada con el funcionamiento y control de la actuación pública» (art. 5.1 LTAIBG), debiendo en consecuencia publicarse en las correspondientes sedes electrónicas o páginas web (Ponce Solé, J., *op. cit.*, nota 23, p. 45).

[72] En este sentido, Cotino Hueso, L., «SyRI, ¿a quién sanciono? Garantías frente al uso de inteligencia artificial y decisiones automatizadas en el sector público y la sentencia holandesa de febrero de 2020», *La Ley Privacidad, Wolters Kluwer* nº 4*,* mayo 2020.

Aunque suponga un cierto progreso en la transparencia de los tratamientos automatizados, no deja de ser un paso muy limitado habida cuenta de que la obligación de publicidad se circunscribe a la información mencionada en el artículo 30 RGPD (fines del tratamiento; descripción de las categorías de interesados y de los datos personales; categorías de destinatarios; descripción general de las medidas de seguridad, etc.). Así, pues, no cabe derivar de la LTAIBG la exigencia de que se divulguen en el portal de transparencia las especificaciones técnicas de los algoritmos ni una explicación detallada de su funcionamiento[73].

Salvo error de quien esto escribe, ha sido la Comunidad Autónoma valenciana la que más decididamente ha apostado por fortalecer la transparencia algorítmica en las sedes electrónicas o páginas web del sector público. Así es; la todavía reciente nueva Ley 1/2022, de 13 de abril, de Transparencia y Buen Gobierno de la Generalitat Valenciana, incluye en el bloque de la «información de relevancia jurídica» que necesariamente debe difundirse telemáticamente la siguiente: «La relación de sistemas algorítmicos o de inteligencia artificial que tengan impacto en los procedimientos administrativos o la prestación de los servicios públicos con la descripción de manera comprensible de su diseño y funcionamiento, el nivel de riesgo que implican y el punto de contacto al que poder dirigirse en cada caso, de acuerdo con los principios de transparencia y explicabilidad» [art. 16.1.l)].

En cualquier caso, parece evidente que los límites a la transparencia pueden tener una mayor operatividad cuando se proyectan sobre la publicidad activa que cuando se aplican a propósito del ejercicio del derecho de acceso, debido a la mayor difusión que alcanza la información en cuestión. Ciertamente, el hecho de que esta esté disponible en los correspondientes portales, sedes electrónicas o páginas web potencia y multiplica el riesgo de afectación de los derechos o intereses jurídicos protegidos por los límites. Así, ha tomado ya carta de naturaleza a nivel jurisprudencial la apreciación de que la mayor capacidad difusora de las nuevas tecnologías constituye un factor relevante para resolver los conflictos entre derechos y la libertad de información (véase, por ejemplo, la STC 58/2018, FJ 7º y, por citar una decisión del Tribunal Europeo de Derechos Humanos, la Sentencia de 28 de junio de 2018, caso *M.L. y W.W. contra Alemania*, §§ 91, 97, 102). Y en esta línea es de destacar la Sentencia del Tribunal de Justicia (Gran Sala), de 1 de agosto de 2022 (asunto C-184/20), en donde se resolvió

[73] Conviene en cualquier caso apuntar que el «Reglamento de actuación y funcionamiento del sector público por medios electrónicos» (aprobado por el Real Decreto 203/2021, de 30 de marzo) incluye como contenido obligatorio de las sedes electrónicas la «[r]elación actualizada de las actuaciones administrativas automatizadas vinculadas a los servicios, procedimientos y trámites» disponibles; y precisa que «[c]ada una se acompañará de la descripción de su diseño y funcionamiento, los mecanismos de rendición de cuentas y transparencia, así como los datos utilizados en su configuración y aprendizaje». [artículo 11.1.i)]. Con este Real Decreto sólo vienen a atemperarse la manifiesta insuficiencia de transparencia de la que adolece el artículo 41 de la Ley 40/2015 (Cotino Hueso, L., «Qué concreta transparencia e información de algoritmos e inteligencia artificial es la debida», en: *Revista Española de la Transparencia*, núm. 16, primer semestre de 2023, p. 27).

una cuestión prejudicial sobre la normativa lituana que obliga a publicar en Internet los datos contenidos en las declaraciones de intereses privados de personas que trabajan como servidores públicos, así como de los directivos de asociaciones que reciben fondos públicos. En efecto, entre los factores a tener en cuenta al evaluar la gravedad de la injerencia en el derecho invocado como límite de la transparencia, el TJUE apuntó que debía tomarse en consideración «la naturaleza y el modo concreto del tratamiento de los datos de que se trata, en particular el número de personas que tienen acceso a ellos y el modo en que acceden» (apartado 99).

Aunque se trata de una línea jurisprudencial usualmente empleada en los casos de colisión entre transparencia y el derecho a la protección de datos personales, no hay ningún motivo para soslayarla en relación con otros límites que pueden entrar en juego cuando se pretende el acceso a los algoritmos.

III.2. Los límites usualmente invocados para restringir la publicidad de la información algorítmica

Por más que sea bien conocido, no parece impertinente recordar que, según se desprende de la lectura conjunta del primer y segundo apartado del artículo 14 LTAIBG, la aplicación de los límites se articula como un proceso argumentativo que se despliega en tres fases o momentos sucesivos[74]. En primer término, debe examinarse si los «contenidos o documentos» (art. 13 LTAIBG) a los que se quiere acceder inciden realmente en la materia definitoria del límite en cuestión, pues, de no llegarse a la conclusión de que la información pretendida guarda relación con el sector de la realidad objeto del límite, habría que descartar sin más la aplicación del mismo.

Pero en el caso de que se aprecie su aplicabilidad, es preciso identificar acto seguido el riesgo de un perjuicio concreto, definido y evaluable para los intereses tutelados por el límite en el supuesto de concederse el acceso, así como argumentar la existencia de una relación de causalidad entre el perjuicio y la divulgación de la información solicitada. Es importante destacar que debe tratarse de un riesgo real, actual y concreto para tales intereses, no bastando la exposición de meras conjeturas ni la mención de remotas o hipotéticas posibilidades de que se irrogue un perjuicio con motivo de la divulgación de la información[75].

---

[74] He seguido muy de cerca la formulación que suele emplear el Consejo de Transparencia y Protección de Datos de Andalucía (así, entre otras, las Resoluciones 81/2016, FJ 6º; 120/2016, FJ 3º, 31/2017, FJ 4º; 52/2017, FJ 4º; 143/2019, FJ 5º; 300/2020, FJ 4º).

[75] Véase, por ejemplo, la Resolución 143/2019 del Consejo de Transparencia y Protección de Datos de Andalucía (FJ 7º), que se hace eco de la doctrina sentada por el Tribunal de Justicia de la Unión Europea: «Pues bien, según viene puntualizando de modo constante la jurisprudencia acuñada en el marco de la Unión Europea, para que pueda legítimamente restringirse el derecho de acceso ha de invocarse el riesgo de un menoscabo al interés protegido por el límite que «debe ser razonablemente previsible y no puramente hipotético» [Sentencia de 15 de septiembre de 2016 (*Herbert Smith Freehills/Consejo*), apartado 33; Sentencia de 17 de octubre de 2013

Y finalmente, una vez superado este *test*, aún habría de determinarse, atendiendo a las circunstancias concurrentes en el caso concreto, si los beneficios derivados de la evitación del perjuicio han de prevalecer sobre los intereses públicos o privados que pueda conllevar la difusión de la información[76].

Conviene tener presente estas diferentes etapas en que se desenvuelve la aplicación de los límites en el marco de la legislación de transparencia, porque —como veremos acto seguido— no siempre se distinguen con nitidez en relación con el que constituye el principal límite que se invoca cuando de conocer los algoritmos se trata, a saber, el derecho a la propiedad intelectual.

III.2.1 *El límite de la propiedad intelectual*

Así es; la LTAIBG incluye expresamente este derecho en el listado de límites al derecho de acceso. «El derecho de acceso —dice su artículo 14.1— podrá ser limitado cuando acceder a la información suponga un perjuicio para: […] j) El secreto profesional y la propiedad intelectual e industrial».

Como acabamos de recordar, el primer paso en la aplicación de los límites a los casos concretos consiste en constatar que el acceso a los «contenidos o documentos» objeto de la solicitud de información (en nuestro caso, el algoritmo) incide materialmente en el interés jurídico protegido por el límite en cuestión. Tarea que conduce inevitablemente a la cuestión de determinar si y en qué medida los algoritmos utilizados por las Administraciones públicas se encuentran bajo la cobertura de la normativa reguladora de la propiedad intelectual. De esto tendremos ahora que ocuparnos.

a) Los algoritmos forman parte del ámbito materialmente protegido por el derecho a la propiedad intelectual

Como sucede con tantos sectores de la realidad, la regulación de la propiedad intelectual es un asunto asumido en primer término por el legislador europeo. Y con

(*Consejo/Access Info Europe*), apartado 31; Sentencia de 21 julio de 2011 (*Suecia/ MyTravel y Comisión*), apartado 76; Sentencia de 1 de julio de 2008 (*Suecia y Turco/Consejo*), apartado 43; asimismo, la Sentencia de 13 de abril de 2005 (*Verein für Konsumenteninformation/Comisión*), apartado 69]».

[76] Para expresarlo en términos familiares desde la perspectiva de la teoría general de los derechos fundamentales, esta tercera y última fase se halla muy próxima a la que constituye también la última etapa en la aplicación del principio de proporcionalidad, a saber, el «principio de proporcionalidad en sentido estricto». Según se desprende de la jurisprudencia constitucional recaída al respecto, este integrante del genérico principio de proporcionalidad se traduce en la máxima de que debe lograrse un equilibrio entre las ventajas y perjuicios que inevitablemente se generan cuando se limita un derecho para salvaguardar otro derecho o bien jurídicamente protegido. Exigencia que supone, en suma, que debe procederse a una valoración confrontada de los intereses contrapuestos, lo cual requiere tomar en consideración todas las circunstancias relevantes del caso concreto (para más detalles, consúltese Medina Guerrero, M., *La vinculación negativa del legislador a los derechos fundamentales*, McGraw Hill, Madrid, 1996, pp. 131-136).

independencia de la aplicación a los programas informáticos —como a cualquier otra obra protegida— de determinados preceptos de la Directiva 2001/29/CE[77], estos cuentan con un régimen específico acuñado en la Directiva 2009/24/CE del Parlamento Europeo y del Consejo, de 23 de abril de 2009, sobre la protección jurídica de programas de ordenador[78].

En efecto, el artículo 1 de esta última Directiva impone, en su apartado primero, a los Estados miembros que protejan «mediante derechos de autor los programas de ordenador como obras literarias tal como se definen en el Convenio de Berna para la protección de las obras literarias y artísticas». Y acota a continuación el ámbito material sobre el que debe proyectarse tal protección: por una parte, extiende la noción de «programas de ordenador» a su documentación preparatoria (art. 1.1)[79], y proyecta la tutela a «cualquier forma de expresión de un programa de ordenador» (art. 1.2). Delimitación del ámbito protegido que también realiza la Directiva de forma negativa, ya que explícitamente excluye de la esfera de los derechos de autor a las «ideas y principios en los que se base cualquiera de los elementos de un programa de ordenador, incluidos los que sirven de fundamento a sus interfaces» (art. 1.2)[80].

Pues bien, entre las diversas «formas de expresión» de los programas de ordenador protegidas[81] se encuentran el código fuente y el código objeto[82], tal y como reconocería expresamente el TJUE ya bajo la anterior Directiva 91/250/CEE. Así, en la Sentencia de la Sala Tercera de 22 de diciembre de 2010 (asunto C393/09) *Bezpečnostní softwarová asociace*, se declararía que «el código fuente y el código objeto de un programa de

[77] Directiva 2001/29/CE del Parlamento Europeo y del Consejo de 22 de mayo de 2001 relativa a la armonización de determinados aspectos de los derechos de autor y derechos afines a los derechos de autor en la sociedad de la información. Directiva que ya expresamente quiso dejar constancia del mantenimiento de la regulación específica sobre los programas informáticos: «Salvo en los casos mencionados en el artículo 11, la presente Directiva dejará intactas y no afectará en modo alguno las disposiciones comunitarias vigentes relacionadas con: a) la protección jurídica de los programas de ordenador…» (artículo 1.2).

[78] Directiva que derogó la Directiva 91/250/CEE del Consejo, de 14 de mayo de 1991, sobre la protección jurídica de programas de ordenador.

[79] Como precisa el Considerando 7: «A los efectos de la presente Directiva, el término «programa de ordenador» incluye programas en cualquier forma, incluso los que están incorporados en el hardware. Este término designa también el trabajo preparatorio de concepción que conduce al desarrollo de un programa de ordenador, siempre que la naturaleza del trabajo preparatorio sea tal que más tarde pueda originar un programa de ordenador».

[80] Aunque la «expresión» de dichas ideas y principios sí deben ser objeto de tutela, según explicita el Considerando 11: «De acuerdo con este principio de derechos de autor, en la medida en que la lógica, los algoritmos y los lenguajes de programación abarquen ideas y principios, estos últimos no están protegidos con arreglo a la presente Directiva. De acuerdo con la legislación y jurisprudencia de los Estados miembros y los convenios internacionales en la materia, la expresión de dichas ideas y principios debe protegerse mediante derechos de autor».

[81] Véase Schneider, J., *op. cit.*, nota 33, pp. 1037-1038.

[82] Sobre la diferenciación entre ambos conceptos puede consultarse Fernández Masiá, E., «Comentario al artículo 96», en: Palau Ramírez, F.; Palao Moreno, G. (dir.), *Comentarios a la Ley de Propiedad Intelectual*, Tirant lo Blanch, Valencia, 2017, pp. 1201-1202.

ordenador son formas de expresión de éste, que merecen por tanto la protección del derecho de autor sobre los programas de ordenador en virtud del artículo 1, apartado 2, de la Directiva 91/250» (apartado 34). E insistiría acto seguido: «En consecuencia, el objeto de la protección conferida por esa Directiva abarca el programa de ordenador en todas sus formas de expresión, que permiten reproducirlo en diferentes lenguajes informáticos, tales como el código fuente y el código objeto» (apartado 35).

Declaración de la tutela tanto del código objeto como del código fuente que sería poco después ratificada por la STJUE (Gran Sala) de 2 de mayo de 2012 (asunto C406/10) *SAS Institute Inc.* y *World Programming Ltd* (apartado 35). Pero la Gran Sala, dando un paso más, revelaría otras facetas relativas a los programas de ordenador que asimismo gozan de protección: «De acuerdo con la segunda frase del séptimo considerando de la Directiva 91/250, el término «programa de ordenador» también designa el trabajo preparatorio de concepción que conduce al desarrollo de un programa, siempre que su naturaleza sea tal que más tarde pueda originar un programa de ordenador» (apartado 36). «Por tanto —concluiría su razonamiento el Tribunal—, el objeto de la protección de la Directiva 91/250 engloba las formas de expresión de un programa de ordenador así como los trabajos preparatorios de concepción que pueden llevar respectivamente a la reproducción o a la creación ulterior de tal programa […]» (apartado 37)[83].

En consonancia con este marco normativo europeo, el Texto Refundido de la Ley de Propiedad Intelectual (Real Decreto Legislativo 1/1996, de 12 de abril; en adelante, TRLPI) menciona expresamente a los programas de ordenador entre las obras originales objeto de propiedad intelectual [artículo 10.1.i)] y recuerda las directrices marcadas por la Directiva que delimitan su ámbito de protección: la extensión de la noción de programas de ordenador a la documentación preparatoria (art. 96.1), la proyección de la tutela a «cualquier forma de expresión de un programa de ordenador» (art. 96.3) y, en fin, la exclusión de «las ideas y principios en los que se basan cualquiera de los elementos de un programa de ordenador» (art. 96.4).

El Texto Refundido, sin embargo, a diferencia de la Directiva 2009/24, puntualiza que la protección dispensada a los programas de ordenador también se extiende

[83] Sentencia que permitiría asimismo avanzar en los aspectos que quedaban al margen de la protección de la Directiva: «39 Sobre la base de estas consideraciones, procede señalar que […] ni la funcionalidad de un programa de ordenador ni el lenguaje de programación o el formato de los archivos de datos utilizados en un programa de ordenador para explotar algunas de sus funciones constituyen una forma de expresión de tal programa en el sentido del artículo 1, apartado 2, de la Directiva 91/250. 40 En efecto, tal como el Abogado General señala en el punto 57 de sus conclusiones, admitir que el derecho de autor pudiera proteger la funcionalidad de un programa de ordenador supondría ofrecer la posibilidad de monopolizar las ideas, en perjuicio del progreso técnico y del desarrollo industrial. […] 42 En cuanto al lenguaje de programación y al formato de los archivos de datos utilizados en un programa de ordenador para interpretar y ejecutar programas de aplicación escritos por los usuarios así como para leer y escribir datos en un formato de archivos de datos específico, se trata de elementos de ese programa mediante los que los usuarios explotan algunas de las funciones de éste».

a la «documentación técnica y los manuales de uso» de los programas (art. 96.1). Mantiene así la ampliación de la tutela establecida en el artículo 96.2 de la Ley de Propiedad Intelectual de 1987 (Ley 22/1987, de 11 de noviembre); una continuación que se ha criticado porque, si podía tener algún sentido en dicho momento, ha dejado de tenerlo tras el cambio del paradigma de protección acuñado en el marco normativo europeo[84].

Quizá por ello esta última vertiente del derecho apuntada en el art. 96.1 TRLPI no parece haberse asumido en su integridad por el CTBG en la Resolución 701/2018, de 18 de febrero de 2019, en donde ciñó el alcance del mismo a lo previsto expresamente en la Directiva: «Este derecho de propiedad intelectual contemplado en la Directiva no comprende, sin embargo, las especificaciones técnicas del programa ni el resultado de las pruebas realizadas para comprobar que la aplicación implementada cumple la especificación funcional, que han sido igualmente solicitados. Las primeras pueden incluir aspectos, entre otros, como si es un sistema operativo de código abierto, cómo realiza el almacenamiento de datos, cuál es su lenguaje de programación o si incluye herramientas para depuración de memoria y análisis del rendimiento del software. Existen multitud de especificaciones técnicas de programas de ordenador expuestas al público en Internet» (Fundamento Jurídico 5).

Comoquiera que sea, lo que sí resulta evidente es que los programas de ordenador y todos los integrantes en los que se expresan (algoritmos subyacentes a los programas, códigos fuente, etc.) forman parte del ámbito material protegido por el derecho a la propiedad intelectual.

Llegados a la conclusión de que los algoritmos utilizados por las Administraciones sí se hallan bajo la cobertura de la normativa reguladora de la propiedad intelectual, hay que dar un paso más y determinar si el solo acceso a los mismos resulta vedado por la misma. O formulada la cuestión desde otra perspectiva: se trata de averiguar si el límite de la propiedad intelectual comprende también la facultad de la Administración de impedir el mero y simple conocimiento del algoritmo por parte del solicitante de información que no tiene en absoluto la pretensión de utilizarlo ni explotarlo comercialmente.

b) El límite de la propiedad intelectual comprende el mero acceso al algoritmo

Más allá de los supuestos en que están involucrados los sistemas algorítmicos de toma de decisiones, lo cierto es que con alcance general la delimitación del alcance del derecho a la propiedad intelectual constituye uno de los límites que más problemas conceptuales está planteando a la hora de su aplicación por las autoridades de control.

[84] Aparicio Vaquero, J. P., «Comentario al Título VII del Libro I (`Programas de ordenador´)», en Bercovitz Rodríguez-Cano, R. (Coord.), *Comentarios a la Ley de Propiedad Intelectual*, 4ª edición, Tecnos, Madrid, 2017, pp. 1386 y 1411-1412.

Como se ha cuidado de subrayar repetidamente la literatura especializada, a menudo estas autoridades de control parten de la premisa de que la función del límite no sería tanto proyectarse en la fase de acceso a la información, sino en garantizar que no se haga una utilización posterior de la misma contraria a los intereses del autor de la obra que se condensarían en sus derechos de explotación. Así, con base en la actuación de dichas autoridades, se ha afirmado que «el respeto al derecho de propiedad intelectual afecta no tanto al acceso a la información en sí misma como a la utilización de la misma por el solicitante, en el sentido de que no podrá reproducirla o destinarla con fines económicos sin la autorización previa del titular de los derechos de autor»[85]. O se ha escrito abundando en esta línea: «Parece más bien que los derechos de autor jugarían aquí no para prohibir el acceso, sino para impedir, conforme a su propia normativa, una reproducción y un posterior uso inconsentido de la información obtenida para fines lucrativos diferentes al del escrutinio público, como prevé el Derecho de la Unión Europea […]»[86].

Esta síntesis doctrinal se ha construido fundamentalmente a partir de las resoluciones de la autoridad de control catalana (GAIP), resultando determinante al respecto su Dictamen 1/2016, de 11 de mayo[87]. En su FJ 2.7, tras recordar la distinción entre derechos morales y derechos de explotación de la propiedad intelectual y apuntar que la titularidad de tales derechos puede recaer en personas diferentes, seguiría argumentando:

«El acceso a un documento protegido por el derecho de propiedad intelectual no afectará previsiblemente a los derechos morales de su creador, pero, según como se haga el acceso, puede afectar a sus derechos de explotación. Dicho de otra manera, la propiedad intelectual protege de la explotación del bien creado por parte de terceras personas; por tanto, es compatible con la consulta o simple uso del bien que no interfiera con los derechos de explotación. La propiedad intelectual no puede operar como límite en el acceso, sino como límite a su utilización o explotación por parte de la persona solicitante. Si tenemos en cuenta que entre los derechos de explotación se encuentra la reproducción y el aprovechamiento económico, lo que sería incompatible con este derecho sería un acceso que comportase la reproducción del bien o un perjuicio para los derechos económicos de explotación.

»De acuerdo con estas consideraciones, se puede afirmar que sería claramente incompatible con los derechos de explotación de la propiedad intelectual un acceso a la información que comportase su reproducción con finalidades de aprovechamiento económico. Más dudas puede comportar una simple reproducción por una sola vez,

---

[85] Fernández Ramos. S.; Pérez Monguió, J. M., *El derecho al acceso a la información pública en España*, Thomson Reuters Aranzadi. Cizur Menor, 2017, p. 184.

[86] Guichot, E.; Barrero Rodríguez, C., *op. cit.*, nota 67, p. 392.

[87] Además de los trabajos citados anteriormente, véase Gutiérrez David, M. E., «El derecho de acceso a la información pública contractual y sus límites», en: Cotino, L.; Boix, P. (coordinadores), *Los límites al derecho de acceso a la información pública*, Tirant lo Blanch, Valencia, 2021, pp. 285-286.

sin finalidades de aprovechamiento económico; en estos casos, la ponderación puede ser más fácilmente favorable al acceso, especialmente si este se fundamenta en derechos o intereses adicionales al derecho de acceso».

Pese a que esta resolución de la GAIP desliza la idea de que «el derecho de propiedad intelectual no afectará *previsiblemente* a los derechos morales de su creador» (la cursiva, obviamente, es nuestra), lo cierto es que en la práctica la argumentación se centra exclusivamente en examinar la afectación de los derechos de explotación, fomentando así la imagen de que los derechos morales quedan expulsados apriorística e incondicionalmente de la materia protegida por el derecho a la propiedad intelectual tutelado en el artículo 14.1.j) LTAIBG.

De ahí que, por lo general y en la práctica, en este tipo de controversias la duda a despejar no sea tanto si se va o no a conceder el acceso, sino cuál sea la modalidad de acceso que puede reconocerse sin menoscabo de los derechos de explotación del autor de la obra.

Y así, como sostuvo el citado Dictamen de la GAIP 1/2016, se entiende que «es claramente compatible con el derecho de propiedad intelectual un acceso limitado a consulta o vista sin reproducción» (FJ 2.7). Doctrina establecida al responder una consulta que sería en lo sucesivo aplicada a las reclamaciones de derecho al acceso; sencillamente, en estos casos habría siempre que conceder el acceso, aunque subordinándolo a condicionantes orientados a evitar que se produzca un perjuicio de los derechos de explotación. Baste reseñar como ejemplo la Resolución 261/2017, de 16 de julio, en cuyo FJ 2º puede leerse: «La decisión del Ayuntamiento de permitir el acceso presencial al proyecto técnico limitando la obtención de copia electrónica fundamentada en la cautela frente a los derechos de propiedad intelectual de su autor se ajusta a los criterios que establecía el Dictamen 1/2016 de esta Comisión, que recomendaba *no aplicar el límite al acceso*, sino en todo caso a los formatos que hiciesen posible una difusión incontrolada…» (de nuevo, es nuestro el énfasis).

E incluso la vía de la consulta presencial puede rodearse de cautelas adicionales, como la adopción de las medidas pertinentes para evitar el uso de dispositivos móviles que permitan obtener copia del documento en cuestión (el repetido Dictamen de la GAIP 1/2015, FJ 2.7). Aunque en otras ocasiones se ha considerado factible dar acceso a la copia de la información pretendida, pues se ha considerado suficiente con la advertencia expresa al solicitante de la responsabilidad en que podía incurrir por un mal uso de la misma (Resolución de la GAIP 17/2015, de 23 de diciembre, FJ 5, en relación con el acceso a proyectos docentes).

Mas volviendo de nuevo al específico tema de la transparencia algorítmica, es de notar que esta línea doctrinal del «acceso condicionado» se ha extendido también a aquellos supuestos en que lo pretendido era conocer el código fuente o, más genéricamente, un algoritmo: «[…] se tiene que declarar el derecho de la persona reclamante a que le sea facilitado el código fuente solicitado, por correo electrónico, tal como pidió. Atendida la finalidad de control de la petición de acceso, se restringe el acceso a esta

finalidad y no se permite la difusión o la utilización del código fuente para otras finalidades sin la autorización expresa de la Administración de la Generalitat» (GAIP, Resolución 200/2017, de 21 de junio, FJ 3). Y en sentido similar ya se había declarado en la Resolución de 21 de septiembre de 2016: «[…] dada la finalidad de control de la petición de acceso, parece prudente restringir el acceso a este fin y no permitir la difusión o utilización del algoritmo sin la autorización expresa del Consejo Interuniversitario o de quien, eventualmente, ostente la titularidad del derecho de propiedad inmaterial en cuestión» (FJ 3).

Pero con independencia de cuál pueda ser la operatividad práctica de esta fórmula del «acceso condicionado» pergeñada para tutelar los derechos de explotación[88], es difícil asumir la percepción que esta construcción fomenta en la práctica, a saber, que el puro y simple acceso —sin pretensión de aprovechamiento económico— no forma materialmente parte del derecho a la propiedad intelectual protegido en el art. 14.1.j) LTAIBG.

Y en esta última línea inciden algunas de las decisiones del CTBG. Así, en la Resolución 464/2022, de 21 de noviembre, en donde se trataba de acceder a los exámenes realizados en determinadas oposiciones, tras hacerse eco de diversos preceptos del TRLPI —entre otros, su art. 14—, declaró lo siguiente: «De este sucinto marco normativo se desprende, en primer lugar, la posibilidad de formular una distinción entre los derechos morales del creador —atribución o reconocimiento de autoría, divulgación, preservación de la integridad— que son inalienables y los derechos de explotación, que incluyen la reproducción y el aprovechamiento económico que puede ser objeto de cesión. Y en segundo lugar, cabe señalar que el bien jurídico protegido por la propiedad intelectual consiste, en definitiva, en la protección de la explotación del bien creado por parte de terceras personas. Esto es, la propiedad intelectual no puede operar como un límite al acceso de la información de que se trate, sino como límite a su utilización o explotación por parte del solicitante de la misma» (FJ 6º). Y aunque es cierto que a continuación el CTBG argumenta en torno al test de daño para llegar a la conclusión de que, al no haberse demostrado o acreditado el eventual perjuicio originado, no cabía «apreciar la concurrencia del límite», no es menos verdad que el pasaje transcrito refleja la idea de que el solo acceso queda al margen de la protección que dispensa a su titular o beneficiario el límite del derecho a la propiedad intelectual.

No es este ciertamente un resultado que parezca asumible a la luz del modo en que se caracteriza el derecho a la propiedad intelectual en nuestro ordenamiento. Según la conceptúa el artículo 2 TRLPI, la propiedad intelectual se halla «integrada por derechos de carácter personal y patrimonial, que atribuyen al autor la plena disposición y el derecho exclusivo a la explotación de la obra, sin más limitaciones que las establecidas en la Ley». Distinción entre estos dos bloques de derechos subjetivos constitutivos del genérico derecho a la propiedad intelectual que se refleja explícitamente en el Ca-

[88] Dudas acerca de que el acceso condicionado al código fuente sea siempre una solución adecuada ha manifestado Gutiérrez David, M. E., *op. cit.*, nota 10, p. 174.

pítulo III del Título II del Libro Primero de la TRLPI, al dedicar su Sección 1ª al «Derecho moral» y la Sección 2ª a los «Derechos de explotación»[89].

Pues bien, entre las numerosas posibilidades de actuación del autor que el legislador incluye al delimitar el contenido del derecho moral en el artículo 14 TRLPI[90], a nosotros únicamente interesa apuntar la que aparece en primer lugar: «1.º Decidir si su obra ha de ser divulgada y en qué forma»; entendiendo por divulgación de una obra, tal y como puntualiza el artículo 4 TRLPI, «toda expresión de la misma que, con el consentimiento del autor, la haga accesible por primera vez al público en cualquier forma». Con base en estas disposiciones, resulta evidente que el derecho de divulgación comprende esencialmente la capacidad del autor de decidir si se permitirá el acceso al público a su obra por vez primera[91], aunque también le corresponde determinar «el momento y la forma o condiciones en que ha de divulgarse»[92].

En suma, aunque se trate única y estrictamente del puro y simple acceso a la información —sin que haya el menor atisbo de utilización o empleo posterior de la obra protegida— siempre entrará en juego el límite del art. 14.1.j) LTAIBG, al afectarse el referido «derecho moral» a la divulgación integrante del genérico derecho a la propiedad intelectual. Pues ciertamente, como con tino se ha afirmado, «la lesión del derecho a decidir la divulgación genera daño por sí misma con independencia de la lesión por los derechos de explotación que de dicho acto pueda derivarse»[93].

Con el solo acceso al algoritmo se está, pues, incidiendo materialmente en la propiedad intelectual a cuya tutela se incardina este límite. Pero, como ya sabemos, para rechazar justificadamente el acceso es además preciso que el mismo irrogue un daño real y, especialmente en estos supuestos, que la decisión denegatoria sea el resultado de una adecuada ponderación entre los intereses protegidos por el límite y los beneficios que pueda conllevar la difusión de la información.

Y, como el improbable lector quizá haya ya adivinado, en dicha ponderación puede resultar un factor relevante la circunstancia de que el sistema algorítmico se haya

---

[89] Subraya la separación e «independencia» del derecho moral frente a los derechos patrimoniales Plaza Penadés, J., «Comentario al artículo 14», en: Rodríguez Tapia, J. M. (Dir.), *Comentarios a la Ley de Propiedad Intelectual*, 2ª edición, Civitas/Thomson Reuters, Cizur Menor, 2009, p. 154.

[90] Plaza Penadés señala que «la legislación española contiene la regulación más amplia y extensa del derecho moral de autor de cuantas se conocen actualmente» (*ibid.)*.

[91] La distinción entre derechos morales y patrimoniales es habitual en los ordenamientos de la Europa continental, que suelen reconocer explícitamente entre los primeros al derecho a la divulgación. Así, la Ley alemana reguladora del derecho a la propiedad intelectual también contempla en el §12 el denominado «derecho a la primera divulgación» —*Erstveröffentlichungsrecht*— (véase al respecto Mecklenburg, W.; Pöppelmann, B. H., *Informationsfreiheitsgesetz*, Deutscher Journalisten-Verband *et al.*, Berlin, 2007, p. 89). Igualmente en Francia el Código de la propiedad intelectual se hace eco de dicha distinción y específicamente del derecho a la divulgación (artículos L111-1 y L121-7-1; véanse al respecto las siguientes decisiones de la CADA: *Avis* 20180226 y *Avis* 20180376).

[92] Martínez Espín, P., «Comentario al artículo 14», en Bercovitz Rodríguez-Cano, R. (Coord.), *Comentarios a la Ley de Propiedad Intelectual*, 4ª edición, Tecnos, Madrid, 2017, p. 232.

[93] Plaza Penadés, J., *op. cit.*, nota 89, p. 163.

creado directamente por la propia Administración o, por el contrario, que sea obra de un tercero realizada por encargo de la misma.

c) Titularidad y ejercicio de los derechos de propiedad intelectual en relación con los programas creados por las Administraciones públicas

Muy habitualmente, tanto en España como en general en la órbita jurídica en la que nos insertamos, las Administraciones no se encargan directamente de crear en su integridad sus propios sistemas automatizados de toma de decisiones, sino que encomiendan la tarea de elaborar los algoritmos o programas a entidades privadas[94]. En estos casos frecuentes, máxime si la Administración no aparece como cesionaria de los derechos de explotación[95], es cuando el límite del derecho a la propiedad intelectual adquiere su máxima virtualidad y, consiguientemente, opera con mayor intensidad.

Aunque, ciertamente, los principales problemas en torno a la aplicabilidad de este límite se suscitan en aquellos casos en que es la propia Administración la creadora del programa. De hecho, lo cierto es que es controvertida con carácter general —más allá del concreto tema que nos ocupa— la posibilidad de que una autoridad pública apele a su propio derecho a la propiedad intelectual para negarse a dar una información generada por ella misma, al considerarse desde cierta perspectiva que únicamente es dable que esgrima este límite en relación con las obras creadas por terceros[96].

Y, como se ha destacado por un sector de la doctrina, lo debatido de la cuestión se refleja en la oscilante práctica seguida al respecto por el CTBG, ya que, frente a decisiones que toman en consideración el límite cuando se trata de proyectos de investigación realizados en centros públicos, en los restantes supuestos se tiende a soslayar la aplicación de la propiedad intelectual[97].

En efecto, en algunas de sus decisiones muestra la proclividad a excluir que entre en juego el límite cuando la información es elaborada por personal al servicio de la Administración. Así, en la Resolución 42/2017, de 25 abril, en la que se abordaba el posible acceso a las soluciones de un tribunal calificador, entre otras razones, se denegó la aplica-

---

[94] Boix Palop, A., «Transparencia en la utilización de inteligencia artificial por parte de la Administración», *El Cronista del Estado Social y Democrático de Derecho*, núm. 100, septiembre-octubre 2022, p. 96.

[95] Cesión que, obviamente, puede entrañar un coste para la Administración. En esta línea, en los Estados Unidos se ha criticado la opción de que se traspase el derecho de propiedad intelectual a los Estados por la sencilla razón de que no es necesario para una prestación de bienes y servicios eficaz y económicamente eficiente (sobre estas posiciones críticas, consúltese Bloch-Wehba, H., *op. cit.*, nota 29, p. 1307).

[96] Así, se ha sostenido que las propiedades intelectual e industrial, en cuanto derechos de naturaleza privada, constituyen un límite que se refiere a derechos de terceros, que no de la propia Administración pública [Messia de la Cerda Caballero, J. A., «Comentario al artículo 14 i) y j)», en: Troncoso Reigada, A. (dir.), *Comentario a la Ley de transparencia, acceso a la información pública y buen gobierno*, Civitas/Thomson Reuters, Madrid, 2017, p. 943].

[97] Para un examen más detallado del diferente sentido de algunas Resoluciones del CTBG, consúltese Guichot, E.; Barrero Rodríguez, C., *op. cit.*, nota 67, pp. 389-391.

ción del límite sobre la base de que los trabajos de los miembros del tribunal, en cuanto «empleados públicos de la Administración», «no gozan tampoco de la protección de la propiedad intelectual, ya que no les pertenecen en este sentido los trabajos realizados bajo su condición de tales» (FJ 8º). Y en la Resolución 530/2018, de 30 de noviembre, concerniente al acceso a los enunciados de unas pruebas y las plantillas correctoras, abundaría sobre el particular: «resulta evidente que no puede ser de aplicación el límite de la propiedad intelectual, ya que los enunciados de esas pruebas y sus plantillas correctoras pertenecen a la Administración con carácter general, no a los funcionarios que las idearon ni a los participantes en las mismas y, por ello, deben ser públicos» (FJ 5º)[98].

Esta tendencia a soslayar el límite de la propiedad intelectual cuando se trata de una obra propia de la Administración también se trasluce, ocasionalmente, en algunas decisiones de las autoridades de control concernientes específicamente al acceso al código fuente. Así parece vislumbrarse al menos, por citar algún ejemplo, en el siguiente pasaje de la Resolución de la GAIP 200/2017, de 21 de junio: «Tampoco se ha invocado el límite relativo a los derechos de propiedad intelectual o industrial […], seguramente porque, como se ha señalado en el fundamento jurídico anterior, el programa informático en cuestión es de titularidad de la Generalitat» (FJ 2º).

En suma, según se desprende de estas resoluciones, cuando la obra es realizada por el personal al servicio de la Administración en el desempeño de sus tareas y, por tanto, se entiende información propia de ésta, el derecho a la propiedad intelectual no opera en relación con las concretas personas físicas autoras de la obra, pero tampoco se considera que la Administración pueda invocarlo para denegar el acceso a la información pretendida. Sencillamente, a la luz de las citadas resoluciones, el solo hecho de catalogarse la información como perteneciente a la Administración conlleva *per se*, sin considerar siquiera la aplicabilidad del límite, que deba ser pública[99].

Un adecuado abordaje de estas controversias exige, sin embargo, afrontar en primer término la cuestión de si las Administraciones pueden ser titulares o ejercitar el derecho a la propiedad intelectual en relación con la información generada por ellas mismas, y específicamente en lo que a este trabajo concierne respecto de los sistemas algorítmicos creados en su seno.

En línea de principio, la Directiva 2009/24 deja un amplio margen de libertad a los Estados miembros para regular la titularidad de los derechos sobre los programas de ordenador. Con independencia de que volvamos más adelante sobre algún otro de sus

[98] La Resolución sería anulada por la Sentencia 120/2019 del Juzgado Central de lo Contencioso Administrativo núm. 5, de 5 de noviembre, al considerar que la solicitud de información incurría en la causa de inadmisión del artículo 18.1.e) LTAIBG.

[99] En esta línea, en el recurso contencioso-administrativo presentado por la Fundación Civio respecto del acceso al código fuente del sistema BOSCO, se sostiene que este límite únicamente puede ser alegado por la Administración cuando se trate de una propiedad intelectual de titularidad ajena, toda vez que la finalidad de esta limitación no es sino tutelar derechos de un tercero (Presno Linera, M. A., *Derechos fundamentales e inteligencia artificial*, Marcial Pons, Madrid, 2022, p. 80).

preceptos, procede ahora recordar lo que establece su artículo 2 («Titularidad de los derechos») en su primer apartado: «1. Se considerará autor del programa de ordenador a la persona física o grupo de personas físicas que lo hayan creado o, cuando la legislación de los Estados miembros lo permita, a la persona jurídica que sea considerada titular del derecho por dicha legislación. Cuando la legislación de un Estado miembro reconozca las obras colectivas, la persona física o jurídica que según dicha legislación haya creado el programa, será considerada su autor». Y a continuación su artículo 3, relativo a los «beneficiarios de la protección», dispone lo siguiente: «La protección se concederá a todas las personas físicas y jurídicas que cumplan los requisitos establecidos en la legislación nacional sobre derechos de autor aplicable a las obras literarias».

Así, pues, la Directiva habilita a los Estados incluso para determinar si atribuye la condición de autor de un programa a una persona jurídica. Habilitación de la que haría uso el legislador español, tal y como se refleja en el artículo 97 TRLPI[100]:

> «1. Será considerado autor del programa de ordenador la persona o grupo de personas naturales que lo hayan creado, o la persona jurídica que sea contemplada como titular de los derechos de autor en los casos expresamente previstos por esta Ley.
>
> »2. Cuando se trate de una obra colectiva tendrá la consideración de autor, salvo pacto en contrario, la persona natural o jurídica que la edite y divulgue bajo su nombre. […]
>
> »5. La protección se concederá a todas las personas naturales y jurídicas que cumplan los requisitos establecidos en esta Ley para la protección de los derechos de autor».

De los dos primeros apartados del artículo 97 TRLPI se desprende que las personas jurídicas no es sólo que puedan ser «meros» titulares o beneficiarios de determinados derechos sobre los programas de ordenador, sino que incluso pueden recibir la consideración de *autores* de los mismos, alejándose así palmariamente del tradicional Derecho de Autor español en el que únicamente las personas físicas podían tener tal condición[101]. Lo cierto es que la recepción en nuestro ordenamiento de la atribución de la autoría a las personas jurídicas —propia del *copyright* anglosajón— tuvo en un sector de la doctrina el efecto del estallido de un trueno en un cielo sereno[102].

---

[100] Con ocasión de la adaptación de nuestra legislación a la Directiva 91/250 CE ya se dieron claros pasos al respecto con alcance general. Así, el artículo 5 TRLPI, tras considerar «autor a la persona natural que crea alguna obra…», dispone acto seguido que «de la protección que esta Ley concede al autor se podrán beneficiar personas jurídicas en los casos expresamente previstos en ella». Y el artículo 8 contempla explícitamente, en relación con «los derechos sobre la obra colectiva», que pueden corresponder a la persona jurídica que la edite y la divulgue bajo su nombre.

[101] Aparicio Vaquero, J. P., *op. ci.*, nota 84, pp. 1418-1419.

[102] Como «cataclismo conceptual» describe Rodríguez Tapia la situación provocada por tal recepción [«Comentario al artículo 97», en: Rodríguez Tapia, J. M. (Dir.), *Comentarios a la Ley de Propiedad Intelectual*, 2ª edición, Civitas/Thomson Reuters, Cizur Menor, 2009, p. 592].

La principal consecuencia que se deriva de la incorporación a nuestro ordenamiento de esa ficción jurídica de raíz anglosajona es que conlleva necesariamente la atribución a las personas jurídicas —junto a los derechos de naturaleza económica— de los derechos morales sobre el programa de ordenador[103]. Pues de la autoría se sigue inescindiblemente, como se cuida de destacar generalizadamente la doctrina[104], la titularidad de los derechos morales, por más que esto suponga un «contrasentido» desde la perspectiva clásica de nuestro Derecho, en el que los derechos morales son, por definición, intransferibles[105].

Así, pues, y sobre la base de que nada autoriza a entender que queden excluidas las personas jurídico-públicas del artículo 97 TRLPI, en la medida en que los programas de ordenador creados por el personal al servicio de las Administraciones son reconducibles en la mayoría de las ocasiones a la categoría de «obra colectiva» en el sentido del art. 97.2 TRLPI[106], a ellas corresponde en su condición de «autoras» tanto los derechos de explotación como los derechos morales sobre los programas (entre los cuales se encuentra, como ya sabemos, el derecho a «decidir si su obra ha de ser divulgada y en qué forma» *ex* art. 14 1º TRLPI)[107]. Todo ello sin olvidar la even-

[103] Es más; quizá sea esta la única finalidad objetiva que persigue reconocer a las personas jurídicas la condición de autor. Como ha escrito Ángel Carrasco Parera con su exuberancia y agudeza habituales: «La segunda violencia que se practica sobre el sistema afecta al concepto de autoría. Si se lee el galimatías del art. 97, lo que se saca en claro […] es que la empresa con cuya personal y medios se fabrica el programa tiene los derechos de propiedad intelectual; como es lógico. Pero al tener que meter este cadáver en el ataúd del *copyright* es como si no le cupieran lo brazos; la ley se ve obligada a hablar de `autoría´, término improcedente en este terreno propio de los programas; y como no sabe qué hacer con la autoría, comete el atropello de `considerar´ autor a la persona jurídica o a la empresa bajo cuya estructura organizativa se haya diseñado el programa. Ante esta bárbara `consideración´ (bastedad propia de la horda) preguntamos para qué sirve discutir aquí de autoría, de qué sirve llamar autor a la persona jurídica titular de la empresa. Y descubrimos (¿lo descubrió el legislador también?) que no tiene otro sentido que el de hacerle titular de derechos morales de autor» (Introducción al libro de Fernández Masía, E., *La protección de los programas de ordenador en España*, Tirant lo Blanch, Valencia, 1996, p. 22).

[104] Baste citar: Aparicio Vaquero, J. P., *op. cit.*, nota 84, p. 1423; Fernández Masía, E., *op. ci.*, nota 82, pp. 1210-1211; Plaza Penadés, J., *op. cit.*, nota 89, pp. 161-162; Vendrell Cervantes, C., «Comentario al artículo 14», en: Palau Ramírez, F./Palao Moreno, G. (dir.), *Comentarios a la Ley de Propiedad Intelectual*, Tirant lo Blanch, Valencia, 2017, p. 272.

[105] Fernández Masiá, E., *op. cit.*, nota 82, p. 1211.

[106] En esta línea, Aparicio Vaquero, J. P., *op. cit.*, nota 84, p. 1432.

[107] Por el contrario, según cabe inferir de la Resolución 253/2021, de 19 de noviembre de 2021, el CTBG parece partir de la idea de que las administraciones públicas no ostentan el derecho de propiedad intelectual sobre los algoritmos y programas que crean: «En el caso de esta reclamación, la administración no aclara quién es el creador del código fuente de la aplicación informática, si la propia administración o un tercero con quien ha contratado. El Real Decreto Legislativo 1/1996, de 12 de abril, define al autor en su artículo 5 como «la persona natural que crea alguna obra literaria, artística o científica». Por lo tanto, si la administración es la autora del código fuente no cabe considerar afectada la propiedad intelectual, puesto que ésta no es un derecho que corresponda a una administración pública, sino únicamente a personas físicas y en casos muy concretos, que no resultan de aplicación al supuesto de esta reclamación, a personas jurídicas» (FJ 6º).

tual aplicabilidad a los programas elaborados por las Administraciones del artículo 6.2 TRLPI, el cual, en relación con las obras divulgadas en forma anónima, prevé que los derechos de propiedad intelectual (incluyendo los derechos morales) se ejercitarán por las personas jurídicas que las saquen a la luz con el consentimiento de los correspondientes autores.

Por último, a fin de completar el panorama normativo en lo concerniente al desenvolvimiento del derecho a la propiedad intelectual cuando se elaboran programas de ordenador en el seno de la Administración, ha de tenerse presente lo dispuesto en el artículo 97.4 TRLPI: «Cuando un trabajador asalariado cree un programa de ordenador, en el ejercicio de las funciones que le han sido confiadas o siguiendo las instrucciones de su empresario, la titularidad de los derechos de explotación correspondientes al programa de ordenador así creado, tanto el programa fuente como el programa objeto, corresponderán, exclusivamente, al empresario, salvo pacto en contrario»[108]. Pues bien, aunque hay acuerdo generalizado acerca de que el precepto resulta directamente de aplicación a los programas elaborados para la Administración por contratados laborales, dista mucho de ser pacífica la tesis de que pueda extenderse a los programas creados en el marco de una relación funcionarial[109]. Se trata en cualquier caso de una controversia de una limitada repercusión práctica a los efectos de este trabajo, ya que, con independencia de que la disposición no abarque la totalidad de los derechos sobre el programa sino «únicamente» los derechos de explotación, los programas de ordenador creados por los funcionarios entran en el ámbito de cobertura del art. 97.2 TRLPI según apuntamos líneas arriba.

Y, sin embargo, con lo dicho hasta ahora aún no se han zanjado todos los interrogantes planteados en torno al binomio propiedad intelectual/programas elaborados por las Administraciones, pues todavía queda por examinar cuál sea el alcance de las «exclusiones» a las que hace referencia el artículo 13 TRLPI: «No son objeto de propiedad intelectual las disposiciones legales o reglamentarias y sus correspondientes proyectos, las resoluciones de los órganos jurisdiccionales y los actos, acuerdos, deliberaciones y dictámenes de los organismos públicos, así como las traducciones oficiales de todos los textos anteriores».

En primer término, y aun cuando pueda parecer una obviedad, no está de más apuntar que, dado que no excluye *sic et simpliciter* a la totalidad de las creaciones realizadas por las instituciones y organismos públicos, sino que menciona únicamente algunos supuestos, la disposición no viene sino a ratificar la capacidad general que

---

[108] Precepto que sigue muy de cerca lo establecido en el artículo 2.3 de la Directiva 2009/24: «Cuando un trabajador asalariado cree un programa de ordenador en el ejercicio de las funciones que le han sido confiadas, o siguiendo las instrucciones de su empresario, la titularidad de los derechos económicos correspondientes al programa de ordenador así creado corresponderá, exclusivamente, al empresario, salvo pacto en contrario».

[109] Aparicio Vaquero, J. P., *op. cit.*, nota 84, p. 1432; Fernández Masiá, E., *op. cit.*, nota 82, p. 1214.

tienen las Administraciones públicas para ostentar la titularidad del derecho de propiedad intelectual sobre sus obras[110].

Pero, como adelantamos, la principal controversia suscitada por este artículo 13 TRLPI se centra en determinar si los programas y algoritmos elaborados por las Administraciones forman parte, o no, del listado de exclusiones que contiene. Una cuestión que fue planteada abiertamente en el recurso interpuesto por la Fundación Civio contra la Resolución del CTBG 701/2018, que consideró cubiertos por el derecho a la propiedad intelectual determinados aspectos de una aplicación telemática. Según se refleja en el Fundamento de Derecho Primero de la Sentencia que resolvió el recurso, la Fundación alegó la «vulneración de lo dispuesto en los artículos 13 y 31 bis del Texto Refundido de la Ley de Propiedad Intelectual, dado que el límite del artículo 14.1.j) de la LTAIBG puede aducirse por la administración cuando el código objeto de petición pudiera ser de titularidad de un tercero, pero nunca y en ningún caso cuando la titularidad de dicho código es de una Administración pública, puesto que nada hay en la legislación que permita ocultar la motivación de los actos con los que se nos gobierna» (Sentencia 143/2021 del Juzgado Central de lo Contencioso Administrativo nº 8, de 30 de diciembre de 2021).

Alegación que sería rechazada por el Juzgado en los siguientes términos: «[…] hay que tener en cuenta que el código fuente de la mencionada aplicación informática no está dentro de las exclusiones de la propiedad intelectual, mencionadas en el artículo 13 del Real Decreto Legislativo 1/1996, de 12 de abril, de propiedad intelectual, precepto invocado por la entidad recurrente, pues dicho código no es una norma ni un acto administrativo» (Fundamento Cuarto).

A mi juicio, considerar que los programas y algoritmos forman parte de los supuestos excluidos sólo puede fundamentarse en una interpretación sumamente expansiva del artículo 13 TRLPI, difícilmente sostenible dada su naturaleza de norma excepcional[111]. Ciertamente, los programas de ordenador no son reconducibles —sin retorcer los propios términos empleados por la norma— a ninguna de las categorías mencionadas en el artículo 13 TRLPI —«disposiciones reglamentarias», «actos, acuerdos, deliberaciones y dictámenes»—, por lo que no parece factible concluir que los algoritmos de creación pública queden al margen del ámbito material protegido por el derecho de propiedad intelectual en virtud de la reiterada disposición. Por otro lado, de abrazarse esa interpretación expansiva, se facilitaría una explotación económica ilimitada de los programas y algoritmos públicos por parte de terceros.

---

[110] Véase en relación con el §5 de la Ley de Propiedad Intelectual alemana —una disposición, con alguna variante, semejante a nuestro art. 13 TRLPI—, Wegener, B. W., *Zum Verhältnis des Rechts auf freien Zugang zu Umweltinformationen zum Urheberrecht —Gutachten—*, Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit, mayo 2010, §§ 83-94.

[111] «Como toda norma excepcional, no es susceptible de interpretación extensiva o aplicación analógica» [Bercovitz Rodríguez-Cano, R., «Comentario al artículo 13», en Bercovitz Rodríguez-Cano, R. (Coord.), *Comentarios a la Ley de Propiedad Intelectual*, 4ª edición, Tecnos, Madrid, 2017, p. 224].

En realidad, lo que subyace tras esa lectura extensiva del artículo 13 TRLPI es la convicción de que los sistemas automatizados de toma de decisiones son comparables estructuralmente con los reglamentos[112], razón por la cual habría que extender a los mismos las garantías de las que disfrutan las normas reglamentarias[113]. Un enfoque que, llevado hasta sus últimas consecuencias, conduce a entender que hay una plena equiparación material entre los algoritmos y las normas, resultando por ende de aplicación dicha disposición a aquéllos: «El código fuente y los algoritmos, al igual que la ley y la jurisprudencia en aplicación del artículo 13 del Texto Refundido de la Ley de Propiedad Intelectual, deben ser de dominio público»[114].

Es difícil no coincidir con la valoración de que deberían ampliarse determinadas garantías propias de los reglamentos a los procesos de toma de decisiones algorítmicas. Pero el cumplimiento de este «deber» incumbe en primer término y sobre todo al legislador, que habrá de emprender las reformas normativas que sean pertinentes a tal objeto. Creo, sin embargo, que su silencio no puede ser suplido con una interpretación forzada de los términos literales empleados por la normativa vigente, haciéndoles decir lo que en realidad no dicen. En fin, según entiendo, no es posible sostener que los algoritmos utilizados para la toma de decisiones administrativas queden excluidos del ámbito del derecho a la propiedad intelectual en virtud del art. 13 TRLPI.

A modo de recapitulación de cuanto llevamos dicho acerca de la posibilidad de que se invoque el límite del derecho a la propiedad intelectual respecto de los programas de ordenador que han creado las propias Administraciones públicas, conviene destacar lo siguiente:

— En su consideración de autoras de los programas en cuanto obra colectiva (art. 97.2 TRLPI), son titulares tanto de los derechos morales como de los derechos de explotación sobre los mismos. Asimismo, cabe plantearse la aplicabilidad del concepto de «obra anónima» (art. 6.2 TRLPI) al supuesto que nos ocupa —los programas de ordenador de creación pública—, en cuyo caso la Admi-

[112] Martini, M.; Nink, D., *op. cit.*, nota 15, p. 10.

[113] Por lo que hace a la literatura española, véase por todos Boix Palop, A., «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* Vol.1, 2020, p. 224 y ss. Enfoque de Boix que es compartido por Balaguer Callejón, F., para quien los algoritmos «si materialmente realizan las mismas funciones que los reglamentos, deben estar sometidos a similares garantías» (*La constitución del algoritmo*, Fundación Manuel Giménez Abad de Estudios Parlamentarios y del Estado Autonómico, Zaragoza, 2022, p. 39).

[114] De la Cueva, J., «Código fuente, algoritmos y fuentes del Derecho», *El notario del siglo XXI: revista del Colegio Notarial de Madrid,* núm. 77, 2018 (http://www.elnotario.es/index.php/hemeroteca/revista-77/opinion/opinion/8382-codigo-fuente-algoritmos-y-fuentes-del-derecho; fecha de la última consulta: 16 de diciembre de 2022)]. Valoración que el autor ha reiterado en «La importancia del código fuente», en: Capilla Roncero, F. *et al.* (dirs.), *Derecho digital: Retos y cuestiones actuales*, Thomson Reuters Aranzadi, 2018.

nistración, aun no ostentando la titularidad, puede ejercitar en nombre propio los derechos morales y los derechos de explotación.

— Una vez constatado que, en efecto, los programas de ordenador de creación pública entran bajo el ámbito de cobertura material del límite del derecho a la propiedad intelectual, procede ya determinar si el acceso a los mismos o a algunos de sus elementos integrantes entraña un riesgo actual, real, no meramente hipotético. Y aquí, por su propia naturaleza, es necesario diferenciar entre las dos categorías de derechos que componen el genérico derecho a la propiedad intelectual.

  a) Por lo que hace a los derechos de explotación (cuyo contenido, en lo fundamental, se delimita en el art. 99 TRLPI), puede llegarse a la conclusión de que la vía del «acceso condicionado» es una fórmula a la que cabe recurrir para armonizar el derecho de acceso y el derecho a la propiedad intelectual, toda vez que está orientada a minimizar —o, en el mejor de los casos, erradicar— el riesgo de afectación de los intereses económicos inherentes a los derechos de explotación.

  b) Diferente es la valoración que puede hacerse cuando se trata del específico derecho moral a decidir si la «obra ha de ser divulgada y en qué forma» (art. 14 1º TRLPI), puesto que el acceso no consentido a la misma entraña *per se* un daño actual al interés jurídico protegido por este derecho, que no es otro que la capacidad de disponer libremente si la obra se expone, o no, a la consideración del público en general, con independencia de los eventuales efectos económicos que la exposición pueda conllevar. Por consiguiente, dado que el mero acceso supone ya la irrogación de un perjuicio real y no meramente hipotético, de nada vale la fórmula del «acceso condicionado» para enervar la virtualidad del límite.

— Pero esto no supone que quede ya blindado, opacado, el algoritmo en cuestión. Aún quedaría por resolver el tercer paso del *test*, a saber: que la aplicación de este límite esté «justificada y proporcionada a su objeto y finalidad de protección», debiendo atenderse a «las circunstancias del caso concreto, especialmente a la concurrencia de un interés público o privado superior que justifique el acceso» (art. 14.2 LTAIBG). Previsiblemente, dada la relevancia que tiene para la generalidad de la ciudadanía —y para el concreto afectado en particular— que se revele el algoritmo al objeto de conocer el proceso de toma de decisiones administrativas —núcleo duro del sistema de transparencia—, es de esperar que de forma absolutamente mayoritaria el resultado de la ponderación no será otro que el de estimar la solicitud de acceso. A menos que la Administración exponga y acredite otras consideraciones que justifiquen la retención de la información, como podría ser, por ejemplo, que el conocimiento del algoritmo permita a los ciudadanos eludir su aplicación. Pero sobre esto tendremos que volver más adelante (apartado III.2.4), ya que cabe plantearse como

hipótesis de trabajo si, acaso, la Administración no encuentra también alguna defensa frente a esta práctica de sortear la decisión algorítmica en otros límites previstos en la LTAIBG.

d) Los programas elaborados por particulares para las Administraciones públicas

En el caso nada infrecuente —más bien habitual— de que la Administración emplee algoritmos creados por una empresa externa, puede suceder que no disponga de la información pretendida sobre los mismos[115]. Circunstancia que, como es sabido, no puede servir de justificación de alcance general para rechazar *sic et simpliciter* la correspondiente solicitud, toda vez que la legislación reguladora de la transparencia impone al sector privado, en determinadas circunstancias, la obligación de que suministre a la Administración toda la información necesaria que le permita cumplir con las exigencias establecidas en aquella legislación. Las posibilidades de este mecanismo encuentran, sin embargo, un sustancial condicionante que opera como un notable obstáculo para la transparencia en los supuestos que nos ocupan: «Esta obligación se extenderá a los adjudicatarios de contratos del sector público en los términos previstos en el respectivo contrato» (art. 4 LTAIBG)[116].

Los términos contractuales se han erigido, pues, prácticamente desde el arranque mismo de la legislación reguladora del derecho a acceder a la información, como la principal rémora de la transparencia en la generalidad de los países cuando de software se trata.

Así se refleja de modo paradigmático en la experiencia de los Estados Unidos. Tal y como señamos *supra* en el epígrafe III.1.1, el hecho de que el programa esté bajo el control de la Administración constituye un requisito esencial para catalogar la información como *agency record* y, por ende, resultar accesible con base en la *Freedom of Information Act*. Consiguientemente, dado que lo usual es que la Administración obtenga el uso del software a través de un acuerdo contractual que limita específicamente su utilización y reserva el resto de las facultades de disposición a la empresa creadora

[115] Cerrillo i Martínez, A., «Actividad administrativa automatizada y utilización de algoritmos», en Castillo Blanco, F. A. *et al.* (dirs.), *Las políticas de buen gobierno en Andalucía (I): Digitalización y transparencia*, Instituto Andaluz de Administración Pública, Sevilla, 2022, p. 271. En este sentido, asimismo Vestri, G., *op. cit.*, nota 62, p. 384.

[116] Algunas leyes autonómicas reguladoras de la transparencia incorporan la exigencia de que los pliegos de cláusulas administrativas particulares o documento contractual equivalente especifiquen dicha obligación (así, por ejemplo, artículo 4.2 de la Ley andaluza). La nueva ley valenciana 1/2022, dando un paso más, precisa que dichos documentos deben asimismo recoger «los medios para su cumplimiento y los mecanismos de control y seguimiento» (art. 5.2), añadiendo a continuación: «Sin perjuicio de ello, la no inclusión de esta obligación en estos instrumentos no exime de su cumplimiento» (véase Fernández Ramos, S., «Derecho de acceso: Dos novedades autonómicas en 2022 y una tercera que no pudo ser», en: *Revista Española de la Transparencia*, núm. 15, julio-diciembre 2022, pp. 39-40).

del programa, la cuestión se centra en determinar en los casos concretos si la Administración ostenta el suficiente control sobre el mismo para poder considerarlo *agency record* a los efectos de la FOIA[117]. Y lo cierto es que, a la larga, ha terminado prevaleciendo una lectura jurisprudencial estricta de cuándo un archivo está bajo el control de la Administración. En efecto, se tiende a considerar que no hay «control» si la Administración no tiene unas posibilidades no restringidas de usar la aplicación informática de que se trate[118]. Y, en aplicación de esta doctrina, en el caso resuelto en la Sentencia *Gilmore v. US Dept. of Energy*[119], en el que la Administración no disponía de una licencia de uso exclusivo del programa CLERVER, se consideró que el Departamento involucrado carecía del suficiente control sobre el mismo para considerarlo un *agency record* a efectos de la ley reguladora del derecho de acceso a la información.

Pero también en países como Francia, tan sensibilizados con garantizar la transparencia en los sistemas de toma de decisiones algorítmicas, este límite juega un papel determinante en este tipo de supuestos. Así es; los dictámenes de la CADA que atienden a la solicitud de acceder a códigos fuente suelen reconocerlo con la salvedad de que haya terceros que ostenten derechos de propiedad intelectual sobre los códigos (véanse, por ejemplo, el *Avis* 20144578, de 8 de enero de 2015, y el *Avis* 20161990, de 23 de junio de 2016).

En lo que a España concierne, es de notar que la regla general, en línea de principio, es que la contratación de servicios con empresas privadas conlleve la cesión de los derechos de propiedad intelectual a la Administración[120] según se desprende del artículo 308.1 de la Ley de Contratos del Sector Público:

> «Salvo que se disponga otra cosa en los pliegos de cláusulas administrativas o en el documento contractual, los contratos de servicios que tengan por objeto el desarrollo y la puesta a disposición de productos protegidos por un derecho de propiedad intelectual o industrial llevarán aparejada la cesión de este a la Administración contratante. En todo caso, y aun cuando se excluya la cesión de los derechos de propiedad intelectual, el órgano de contratación podrá siempre autorizar

[117] Así se planteó ya abiertamente en el Informe elaborado en el año 1990 por el Departamento de Justicia sobre la noción de documento electrónico en el marco de la FOIA (*Department of Justice Report on «Electronic Record» FOIA Issues*, FOIA Issues, Part II. FOIA Update Vol. XI, Nº 3, 1990. Issue D: Status of Computer Software).

[118] *Tax Analysts v. United States Dept. of Justice,* 913 F. Supp. 599 (D.D.C.1996).

[119] 4 F. Supp. 2d 912 (N.D. Cal. 1998).

[120] Regla general que ocasionalmente ha sido utilizada por las autoridades de control al argumentar sobre la posible aplicabilidad de este límite a la concreta controversia enjuiciada. Valga como ejemplo la Resolución del CTBG 253/2021, de 19 de noviembre: «Si el autor es una persona física o jurídica con la que ha contratado la Comunidad de Madrid, lo habitual en estos casos es que la primera ceda los derechos de propiedad intelectual en favor de la segunda. […] Por lo tanto, parece razonable concluir con que no se ha producido tal cesión en el caso que ocupa esta reclamación, toda vez que si la cesión hubiera tenido lugar la Comunidad de Madrid lo indicaría así expresamente en su resolución y alegaciones como argumento concluyente para afirmar la concurrencia del límite de la propiedad intelectual» (FJ 6º).

> el uso del correspondiente producto a los entes, organismos y entidades pertenecientes al sector público.»

En el caso de que en los pliegos o en el correspondiente documento contractual no se disponga otra cosa y, por tanto, se produzca tal cesión del derecho a la propiedad intelectual sin ningún condicionante, este límite operaría en idénticos términos a como lo hace cuando el programa informático es creado directamente por la propia Administración.

Sin embargo, en la práctica es habitual que los contratistas establezcan cláusulas de confidencialidad o faciliten a la Administración aplicaciones cerradas que no permiten el acceso al código fuente[121]. En estos supuestos, ante la pretensión del solicitante de que se ponga en su conocimiento información sobre el algoritmo, a la Administración no le queda sino confiar en que la empresa se avenga voluntariamente a atender tal petición y le transmita la información pertinente. Frente a la más que probable respuesta denegatoria del contratista, nuestro marco normativo regulador de la transparencia no ofrece, hoy por hoy, ningún mecanismo que asegure el acceso a estos algoritmos.

La superación de la opacidad en estos supuestos sólo parece factible —como lo atestigua alguna experiencia de Derecho Comparado[122]— si se introducen las reformas normativas precisas que impongan específicas obligaciones de transparencia en este ámbito, de tal manera que el derecho de acceder a información sobre los algoritmos no quede enteramente al albur de la libertad negocial.

III.2.2. *El límite de los intereses económicos y comerciales*

A menudo, la invocación del derecho a la propiedad intelectual para justificar la denegación del acceso a los algoritmos se ve acompañada por la apelación al límite de los «intereses económicos y comerciales» [art. 14.1.h) LTAIBG]. Cosa lógica, por lo demás, toda vez que frecuentemente los intereses protegidos por ambos límites son prácticamente coincidentes cuando de empresas se trata[123]. Así sucede palmariamente cuando lo que está en juego son los derechos de explotación de la propiedad intelec-

---

[121] Así, entre otros, Ponce Solé, J., *op. cit.*, nota 23. Sencillamente, como ha reprochado Boix Palop, en numerosas ocasiones se aceptan «las condiciones de uso impuestas por los desarrolladores de manera acrítica» (*op. cit.*, nota 94, p. 96).

[122] Muy interesante es, sin duda, una Ley del Estado de Washington aprobada el año 2019 en la que, entre otros aspectos, se incorporan apreciables medidas tendentes a potenciar la transparencia de los sistemas automatizados de decisiones [H.R. 1655, 66th Leg., Reg. Sess. (Wash. 2019)]. Ciñéndonos estrictamente al asunto que ahora nos ocupa, a fin de asegurar que la Administración esté siempre en condiciones de explicar las decisiones basadas en sistemas algorítmicos, la Ley contempla que la Administración pueda requerir al contratista la elaboración de tal explicación (https://app.leg.wa.gov/billsummary?BillNumber=1655&Year=2019).

[123] En este sentido, Guichot. E.; Barrero, C., *op.cit.*, nota 67, p. 347.

tual, pero también el solo y mero acceso al código fuente puede incidir tanto en el ámbito material tutelado por el art. 14.1.j) LTAIBG como en el que es objeto de protección en el límite que ahora nos ocupa, habida cuenta de que los secretos empresariales son una parte esencial integrante del mismo. Y parece evidente que el código fuente será, por lo general, un «secreto empresarial»[124] —o «secreto comercial» (*trade secret*), para decirlo en los términos empleados usualmente en la esfera anglosajona y de creciente utilización en el marco normativo de la Unión Europea—.

La estrecha conexión entre los intereses protegidos por ambos límites se pone de manifiesto en la propia jurisprudencia del Tribunal de Justicia de la Unión Europea. Desde su punto de vista, cuando se esgrime el secreto empresarial frente a una pretensión de acceder a información, entran en juego tanto el derecho a la propiedad intelectual como el derecho a la libertad de empresa, consagrados respectivamente por los artículos 17.2 y 16 de la Carta de Derechos Fundamentales de la Unión Europea [en este sentido, véase la Sentencia del Tribunal de Justicia (Sala Quinta), de 23 de noviembre de 2016, *Bayer CropScience SANV y Stichting De Bijenstichting* (asunto C442/14), apartado 97 y ss.][125].

Y, de hecho, ha sido tradicionalmente el secreto comercial el principal argumento esgrimido en algunos de los países de nuestro entorno para denegar el acceso a los algoritmos empleados por las empresas[126].

En este sentido, por mencionar uno de los países pioneros en legislar en materia de derecho de acceso a la información pública —los Estados Unidos—, hay una coincidencia absolutamente generalizada en señalar que el secreto comercial constituye el más relevante límite que impide la transparencia algorítmica; máxime cuando, carentes habitualmente las Administraciones de los recursos precisos para desarrollar ellas mismas las herramientas para la toma de decisiones automatizadas, deben recurrir al sector privado para que le suministren los sistemas necesarios[127]. Acuerdos con las empresas que frecuentemente se ven acompañados con garantías de que el contenido de los sistemas han de ser tratados como secretos comerciales.

---

[124] Schneider, J., *op. cit.*, nota 33, p. 1051.

[125] Y en el caso de los Estados Unidos, la relación del secreto comercial se hace directamente con el derecho a la propiedad sin más, de tal suerte que la divulgación pública de un secreto comercial por parte de la Administración puede suponer una privación de la propiedad privada sujeta a una justa compensación de acuerdo con la Quinta Enmienda de la Constitución [Sentencia del Tribunal Supremo *Ruckelshaus v. Monsanto Co.*, 467 U.S. 986 (1984), 1002-1004]. Véase Menell, P. S., «Tailoring a Public Policy Exception to Trade Secret Protection», en: *California Law Review,* Vol. 105, Nº 1 (February 2018), p. 12. En lo que a España concierne, nótese que el Capítulo III de la Ley 1/2019, de 20 de febrero, de Secretos Empresariales, versa precisamente sobre «El secreto empresarial como objeto del derecho de propiedad».

[126] Con alcance general, se ha señalado fundadamente que es el secreto comercial la «más común forma de protección utilizada por las empresas» (Pooley, J., «Trade secrets: The other IP right», en; *WIPO Magazine*, 3/2013, p. 2).

[127] Baste apuntar Bloch-Wehba, H., *op. cit.*, nota 29, p. 1272; Busuioc, M., «Accountable Artificial Intelligence: Holding Algorithms to Account», *Public Administration Review*, Vol. 00, Iss. 00, p. 5 (DOI: 10.1111/puar.13293); Diakopoulos, N., *op. cit.*, nota 30.

En efecto, estos últimos se hallan tutelados en la Exención 4 de la FOIA, que establece que no tienen que divulgarse los secretos comerciales, ni la información comercial o financiera obtenida de una persona que sea privilegiada o confidencial (*trade secrets and commercial or financial information obtained from a person and privileged or confidential*). De conformidad con la jurisprudencia recaída al respecto, puede catalogarse como confidencial a los efectos de esta excepción aquella información cuya divulgación probablemente genere alguno de los siguientes efectos: 1) mermar la capacidad del gobierno para obtener en el futuro información necesaria; o 2) causar un daño sustancial a la posición competitiva de la persona de la que se ha obtenido la información. Así, pues, es suficiente con que se acredite que hay una competencia efectiva y la probabilidad de que se irrogue un perjuicio sustancial para que una información comercial se considere bajo el ámbito de cobertura de la Excepción 4 [*GC Micro Corp. v. Defense Logistics Agency,* 33 F.3d 1109, 1112-1113 (9th Cir.1994), citando *National Parks & Conservation Ass›n v. Morton,* 498 F.2d 765, 770 (D.C.Cir.1974)].

Y en la ponderación entre el interés público inherente a la divulgación de la información y el interés perseguido por el legislador al establecer la excepción, el único interés público a valorar es el de si su difusión puede servir a la finalidad esencial de la FOIA de contribuir significativamente al conocimiento público de las funciones o actividades del gobierno[128]. En cualquier caso, la tendencia es apreciar la concurrencia de esta excepción y, por ende, denegar las solicitudes de información en que estén involucrados softwares desarrollados por empresas privadas[129].

Pero esta operatividad del límite no es exclusiva del ámbito estadounidense, pues también ha dado muestra de su eficacia en instituciones de países tan proclives a la transparencia como Francia. Así se pone de manifiesto en el Dictamen de la CADA 20142953, de 16 de octubre de 2014, en donde se resolvía la pretensión de acceder al programa informático desarrollado por una sociedad privada para el Consejo General del Ródano. La CADA acordaría dar el acceso al programa, pero procediendo previamente a la ocultación de los aspectos cubiertos por el «secreto en materia comercial e industrial» mencionado en el artículo 6 de la Ley 78-753, de 17 de julio de 1978[130].

---

[128] *United States Dep't of Defense v. Federal Labor Relations Auth.*, 510 U.S. 487, 495, 114 S. Ct. 10006, 127 L. Ed. 2d 325 (1994); *Bibles v. Oregon Natural Desert Ass'n,* 519 U.S. 335, 117 S. Ct. 795, 795, 136 L. Ed. 2d 825 (1997).

[129] En esta línea, *Gilmore v. US Dept. of Energy*, 4 F. Supp. 2d 912 (N.D. Cal. 1998).

[130] Y, acto seguido, precisaría el Dictamen el alcance de lo protegido por este límite: «Se recuerda a estos efectos que están amparados por el secreto industrial y comercial las menciones relativas a una de las tres categorías siguientes: a) El secreto de los procesos. Se trata de información que permite conocer las técnicas de fabricación o el contenido de las actividades de investigación y desarrollo de las empresas, como la descripción de los materiales utilizados; b) El secreto de la información económico-financiera. Esta categoría incluye información relacionada con la situación económica de una empresa, su salud financiera o el estado de su crédito, como el volumen de negocios, los documentos contables, el personal y, en general, toda la información que pueda revelar el nivel de actividad; c) El secreto de las estrategias comerciales. Esta categoría incluye información sobre precios y prácticas comerciales como el inventario detallado de una tienda, la lista de sus proveedores, el monto de los descuentos otorgados a ciertos clientes, etc.»

Antes de abordar el examen del régimen jurídico hoy vigente regulador del límite *ex* artículo 14.1.h) LTAIBG, quizá no sea inoportuno señalar que, al preservar la Administración los intereses económicos y comerciales de las empresas contratistas, de modo tangencial pueden ser también sus propios intereses objetivos los que se estén tutelando.

Como agudamente ha argumentado el Tribunal Supremo al interpretar la Exención 4 de la FOIA: «cuando el Congreso aprobó la FOIA, buscaba un "equilibrio viable" entre la divulgación y otros intereses gubernamentales —intereses que pueden incluir proporcionar a las partes privadas garantías suficientes sobre el tratamiento de su información particular para que cooperen en los programas federales y proporcionen al gobierno información vital para su trabajo.» [*Food Marketing Institute v. Argus Leader Media*, 139 S. Ct. 2356, 2366 (2019)]. «La propia existencia de la exención 4 anima a los proveedores a facilitar voluntariamente información comercial o financiera útil a la Administración y ofrece a esta la garantía de que la información solicitada será fiable». [*Critical Mass Energy Project v. NRC*, 975 F.2d 871, 878 (D.C. Cir. 1992)]. Por consiguiente, como adelantamos líneas arriba, una de las finalidades de la Exención 4 es evitar que la divulgación de determinada información produzca el indeseado efecto de «mermar la capacidad del gobierno para obtener en el futuro información necesaria». Pues, según se reconocería en *Gilmore v. US Dept. of Energy* refiriéndose específicamente al acceso a un programa informático, pocas dudas hay que albergar acerca de que «las empresas estarán menos dispuestas a crear empresas conjuntas con el gobierno para desarrollar tecnología si esta puede distribuirse libremente a través de la FOIA.» [4 F. Supp. 2d 912 (N.D. Cal. 1998)]. En suma, reina en los Estados Unidos casi la plena certidumbre de que tutelar los algoritmos creados por las empresas como secreto comercial incentiva que estas creen modelos predictivos para aplicaciones públicas[131].

a) La aplicabilidad de la categoría de «secreto comercial» a los algoritmos

En la actualidad, sin embargo, como también sucede con el derecho a la propiedad intelectual, es un asunto que está primariamente regulado por el legislador europeo, a saber, por la Directiva (UE) 2016/943 del Parlamento europeo y del Consejo, de 8 de junio de 2016, relativa a la protección de los conocimientos técnicos y la información empresarial no divulgados (secretos comerciales) contra su obtención, utilización y revelación ilícitas. Como se reconoce en su Considerando 3, el objetivo central de la Directiva es elevar con alcance general el nivel de tutela del que hasta entonces gozaba el secreto comercial: «Los secretos comerciales son una de las modalidades de protec-

[131] Brauneis, R.; Goodman, E. P., «Algorithmic Transparency for the Smart City», en: *The Yale Journal of Law & Technology*, Vol. 20, 103, 2018, p. 159.

ción de la creación intelectual y de los conocimientos técnicos innovadores que las empresas más suelen utilizar, pero también es la modalidad menos protegida por el actual marco jurídico de la Unión contra la obtención, utilización o revelación ilícitas por terceros».

Directiva que pronto fue valorada como un paso muy relevante en el incremento de la protección del secreto empresarial en relación con los algoritmos en particular[132]. Pues lo que resultó evidente desde el principio es que los sistemas de toma de decisiones algorítmicas se hallaban bajo el ámbito de cobertura de la Directiva, e incluso ésta venía a asegurar y eliminar todo tipo de incertidumbre que pudiera existir sobre el particular.

En efecto, los algoritmos son claramente reconducibles a la noción de secreto comercial consagrado en la Directiva [artículo 2.1)][133], puesto que no suelen ser generalmente conocidos ni fácilmente accesibles, tienen valor comercial y las personas que los controlan tienden a adoptar las medidas pertinentes para preservar su secreto. En este sentido, se ha destacado que cuando los algoritmos se ponen a disposición de terceros, estos quedan obligados a mantener la confidencialidad al respecto. Como sucede con los programas informáticos corrientes, las empresas pueden conceder licencia sobre el código objeto, mantener secreto el código fuente y prohibir la ingeniería inversa (o descompilación) del código objeto a través de una específica cláusula contractual[134]. En suma, no cabe dudar de que las empresas suelen utilizar los instrumentos jurídicos necesarios para restringir el acceso y preservar la confidencialidad de los algoritmos, quedando por ende bajo el ámbito de cobertura de la Directiva.

Debe notarse, por otra parte, que la tutela que brinda esta Directiva reguladora de los secretos comerciales es más extensa que la que proporciona la Directiva 2009/24/CE sobre la protección jurídica de los programas de ordenador. Como señalamos *supra* [epígrafe III.2.1.a)], esta última se proyecta a «cualquier forma de expresión de un programa de ordenador» (art. 1.2), pero excluye expresamente a las «ideas y principios en los que se base cualquiera de los elementos de un programa de ordenador, incluidos los que sirven de fundamento a sus interfaces». Restricción que conlleva que queden al margen del derecho a la propiedad intelectual «ideas» tales como la funcionalidad de un programa de ordenador, el lenguaje de programación o el formato de los archi-

---

[132] Así, por ejemplo, Scheja, K., *op. cit.*, nota 19, *passim*.

[133] Según establece su artículo 2: «A los efectos de la presente Directiva se entenderá por: 1) «secreto comercial»: la información que reúna todos los requisitos siguientes: a) ser secreta en el sentido de no ser, en su conjunto o en la configuración y reunión precisas de sus componentes, generalmente conocida por las personas pertenecientes a los círculos en que normalmente se utilice el tipo de información en cuestión, ni fácilmente accesible para estas; b) tener un valor comercial por su carácter secreto; c) haber sido objeto de medidas razonables, en las circunstancias del caso, para mantenerla secreta, tomadas por la persona que legítimamente ejerza su control».

[134] Maggiolino, M., «EU Trade Secrets Law and Algorithmic Transparency» (March 31, 2019), en: *Bocconi Legal Studies Research Paper* No. 3363178, p. 8 [Disponible en SSRN: https://ssrn.com/abstract=3363178; o bien en htpps://dx.doi.org/10.2139/ssrn.3363178].

vos de datos utilizados en un programa de ordenador para explotar algunas de sus funciones[135].

Este flanco abierto parece quedar, sin embargo, resguardado con la Directiva (UE) 2016/943, pues las «ideas» en general son reconducibles al concepto amplio de secreto comercial del que parte la misma. En efecto, al regular la obtención ilícita de un secreto comercial, su artículo 4.2.a) hace referencia a «cualquier documento, objeto, material, sustancia o fichero electrónico, que se encuentre legítimamente bajo el control del poseedor del secreto comercial y que contenga el secreto comercial o a partir del cual este se pueda deducir»[136].

Ahora bien, este extenso ámbito de protección del secreto comercial delimitado por la Directiva (UE) 2016/943 no se configura como un espacio absoluto e incondicionado. Antes al contrario, la propia Directiva contempla en su artículo 1.2 que la misma no afectará: «a) al ejercicio del derecho a la libertad de expresión e información recogido en la Carta, incluido el respeto a la libertad y al pluralismo de los medios de comunicación; b) a la aplicación de las normas de la Unión o nacionales que, por motivos de interés público, exijan a los poseedores de secretos comerciales divulgar información, incluidos secretos comerciales, o comunicarla a las autoridades administrativas y judiciales para el ejercicio de las funciones de esas autoridades». Y, en consonancia con esta disposición, su artículo 5 («Excepciones») establece que «[l]os Estados miembros garantizarán que se deniegue la solicitud de las medidas, procedimientos y recursos previstos en la presente Directiva cuando la presunta obtención, utilización o revelación del secreto comercial haya tenido lugar en cualquiera de las circunstancias siguientes: a) en ejercicio del derecho a la libertad de expresión e información recogido en la Carta, incluido el respeto a la libertad y al pluralismo de los medios de comunicación. […] d) con el fin de proteger un interés legítimo reconocido por el Derecho de la Unión o nacional.»

Con independencia del ejercicio de la libertad de información[137], la Directiva confiere, además, un cierto margen de maniobra a los legisladores nacionales para ar-

---

[135] STJUE (Gran Sala) de 2 de mayo de 2012 (asunto C406/10) *SAS Institute Inc.* y *World Programming Ltd*, apartado 39.

[136] Consúltese al respecto Maggiolino, M., *op. cit.*, nota 135, p. 6; Noto la Diega, G., «Against the Dehumanisation of Decision-Making — Algorithmic Decisions at the Crossroads of Intellectual Property, Data Protection, and Freedom of Information», en: *Journal of Intellectual Property, Information Technology and E-Commerce Law (JIPITEC)*, 9, 2018, apartado 37 [última consulta: 17/02/2023].

[137] Como es sabido, existe una estrecha conexión entre el derecho a la libertad de información y el derecho de acceso a la información pública establecido por las leyes reguladoras de la transparencia. Vínculo tan íntimo, que el TEDH viene sosteniendo que, en determinadas circunstancias, cuando es un periodista quien ejerce el derecho de acceso, cabe entender que lo que entra en juego es el derecho a recibir y comunicar información consagrado en el artículo 10 del Convenio. Y en aplicación del mandato hermenéutico contenido en el art. 10.2 CE, algunas autoridades de control asumen también que el derecho de acceso a la información pública enraizado en el art. 105 b) CE pasa a operar, en este supuesto, como el derecho fundamental consagrado en el artículo 20.1.d) CE [así, por ejemplo, véanse las Resoluciones del Consejo de Transparencia y Protección de Datos de Andalucía 10/2017 (FJ 2º) y 330/2019 (FJ 6º)].

monizar el secreto comercial con razones de interés público o de interés legítimo, que podrían llevar a justificar el levantamiento del velo del secreto. Y así sucede palmariamente con las exigencias de transparencia que los Estados miembros puedan establecer a fin de alcanzar un mejor control de la toma de decisiones de las Administraciones por parte de la ciudadanía. El propio Considerado 11 de la Directiva lo reconoce en términos inequívocos:

> «La presente Directiva no debe afectar a la aplicación de las normas de la Unión o nacionales que exigen la divulgación de información, incluidos los secretos comerciales, o su comunicación a las autoridades públicas. Tampoco debe afectar a la aplicación de las normas que permiten a las autoridades públicas recabar información para el ejercicio de sus funciones, ni a las normas que permiten o exigen a tales autoridades públicas cualquier otra divulgación de información pertinente. Tales normas incluyen, en particular, las relativas a la divulgación por las instituciones y órganos de la Unión, o por las autoridades públicas nacionales, de información sobre empresas que obre en su poder en virtud del Reglamento (CE) nº 1049/2001 del Parlamento Europeo y del Consejo, del Reglamento (CE) nº 1367/2006 del Parlamento Europeo y del Consejo, de la Directiva 2003/4/CE del Parlamento Europeo y del Consejo, *o de otras normas sobre el acceso público a documentos o las obligaciones en materia de transparencia de las autoridades públicas nacionales*.» (el énfasis es nuestro)

A partir de la aprobación de esta Directiva, y a falta aún de su transposición en el ordenamiento interno, se contaba ya con un firme referente normativo que permitió a las autoridades de control delimitar el concepto de «secreto comercial» a los efectos de la aplicación del límite *ex* art. 14.1.h) LTAIBG. Baste como muestra la Resolución 120/2016 del Consejo andaluz de Transparencia y Protección de Datos, que efectuó una aproximación a la noción de secreto comercial que partía —como no podía ser de otra manera— del sistema conceptual de dicha Directiva 2016/943:

> «[…] de la repetida Directiva cabe inferir determinados elementos estructurales del concepto «secreto comercial», los cuales, por lo demás, ya se habían asumido con anterioridad en otros países de nuestro entorno [así, la Sentencia del Tribunal Constitucional federal alemán, de 14 de marzo de 2006, número marginal 87, *BVerfGE* 115, 205 (230)]. Por una parte, la información que se quiere mantener secreta debe versar sobre hechos, circunstancias u operaciones que guarden conexión directa con la actividad económica propia de la empresa. Por otro lado, debe tratarse de una información que no tenga carácter público, esto es, que no sea ya ampliamente conocida o no resulte fácilmente accesible para las personas pertenecientes a los círculos en que normalmente se utilice ese tipo de información. En tercer término, debe haber una voluntad subjetiva de mantener alejada del conocimiento público la información en cuestión. Y, finalmente, dado que no

> basta con la concurrencia de este elemento subjetivo, también es necesaria la existencia de un legítimo interés objetivo en mantener secreta la información de que se trate. Interés objetivo que, obviamente, debe tener naturaleza económica, y que cabrá identificar —por ceñirnos a lo que a este caso concierne— cuando la revelación de la información refuerce la competitividad de los competidores de la empresa titular del secreto, debilite la posición de ésta en el mercado o le cause un daño económico al hacer accesible a los competidores conocimientos exclusivos de carácter técnico o comercial.» (FJ 5º).

La transposición de la Directiva se llevaría a efecto con la aprobación de la Ley 1/2019, de 20 de febrero, de Secretos Empresariales, la cual, sin embargo, no hace uso de la libertad de configuración habilitada por el legislador europeo a favor de los Estados miembros para que ajusten el secreto comercial a las exigencias de la transparencia pública. En este sentido, la Ley 1/2019 no supone ningún avance en la concreción de la libertad de información o del «interés legítimo» como causas legitimadoras de la divulgación del secreto empresarial, limitándose a recordar las previsiones generales ya contenidas en la Directiva[138].

El panorama jurídico interno apenas experimentó, pues, cambio sustantivo alguno en lo tocante a la posibilidad de acceder a la información sobre los programas informáticos elaborados por las empresas para el sector público. Como hemos señalado al examinar el límite del derecho a la propiedad intelectual, la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, contempla como regla general que «los contratos de servicios que tengan por objeto el desarrollo y la puesta a disposición de productos protegidos por un derecho de propiedad intelectual o industrial llevarán aparejada la cesión de este a la Administración contratante»; regla que, sin embargo, se condiciona a la circunstancia de que «se disponga otra cosa en los pliegos de cláusulas administrativas o en el documento contractual».

Pero, aun en la hipótesis de que proceda a la cesión del derecho de propiedad intelectual, las empresas pueden instar la confidencialidad cuando consideren que pueden resultar afectados los secretos técnicos o comerciales, tal y como establece expresa-

[138] Según establece en el apartado tercero del artículo 2: «En todo caso, no procederán las acciones y medidas previstas en esta ley cuando se dirijan contra actos de obtención, utilización o revelación de un secreto empresarial que hayan tenido lugar en cualquiera las circunstancias siguientes: a) En ejercicio del derecho a la libertad de expresión e información recogido en la Carta de los Derechos Fundamentales de la Unión Europea, incluido el respeto a la libertad y al pluralismo de los medios de comunicación; […] «d) Con el fin de proteger un interés legítimo reconocido por el Derecho europeo o español. En particular, no podrá invocarse la protección dispensada por esta ley para obstaculizar la aplicación de la normativa que exija a los titulares de secretos empresariales divulgar información o comunicarla a las autoridades administrativas o judiciales en el ejercicio de las funciones de éstas, ni para impedir la aplicación de la normativa que prevea la revelación por las autoridades públicas europeas o españolas, en virtud de las obligaciones o prerrogativas que les hayan sido conferidas por el Derecho europeo o español, de la información presentada por las empresas que obre en poder de dichas autoridades».

mente el artículo 133.1 de la Ley de Contratos del Sector Público: «Sin perjuicio de lo dispuesto en la legislación vigente en materia de acceso a la información pública y de las disposiciones contenidas en la presente Ley relativas a la publicidad de la adjudicación y a la información que debe darse a los candidatos y a los licitadores, los órganos de contratación no podrán divulgar la información facilitada por los empresarios que estos hayan designado como confidencial en el momento de presentar su oferta. El carácter de confidencial afecta, entre otros, a los secretos técnicos o comerciales, a los aspectos confidenciales de las ofertas y a cualesquiera otras informaciones cuyo contenido pueda ser utilizado para falsear la competencia, ya sea en ese procedimiento de licitación o en otros posteriores».

Se trata de un marco normativo que ha permitido que habitualmente los contratos, los pliegos o las cláusulas de confidencialidad incluidas en las propuestas de los contratistas excluyan el acceso al algoritmo o al código fuente[139]. Naturalmente, en última instancia depende de las Administraciones públicas avenirse a aceptar las restricciones de la transparencia sugeridas por las empresas, o bien imponer un menor nivel de opacidad de los algoritmos que el pretendido por aquéllas. Ciertamente, no puede sino suscribirse la apreciación de que las Administraciones «deberían mejorar la redacción de los pliegos y, en particular, incluir cláusulas específicas de transparencia donde se determine concretamente qué información relativa a los algoritmos deberá o podrá hacerse pública a fin de garantizar el conocimiento público de los algoritmos, de su configuración o de su funcionamiento»[140].

Pero no es menos cierto que, mientras el marco normativo en materia de contratación no se modifique, no puede con base en la legislación de transparencia jurídicamente imponerse a las Administraciones que establezcan como condición *sine qua non* para proceder a la contratación la introducción de tales cláusulas de salvaguarda de la transparencia.

b) Los intereses económicos y comerciales propios de la Administración protegidos por el artículo 14.1.h) LTAIBG

Aunque el límite que nos ocupa tiene su más habitual proyección en la esfera del sector privado, las Administraciones también pueden apelar al art. 14.1.h) LTAIBG para tutelar sus propios intereses económicos y comerciales, y no sólo los de los terce-

[139] Ponce Solé, J., *op. cit.*, nota 23, nota a pie de página número 62.

[140] Cerrillo i Martínez, A., *op. cit.*, nota 65, p. 50. Y en la misma línea ha escrito Huergo Lora: «El hecho de que el modelo algorítmico haya sido elaborado por una empresa (contratista de la Administración) y esté protegido como secreto empresarial, no autoriza a la Administración a denegar el acceso a la información. La Administración contratante deberá adoptar en el pliego las cláusulas necesarias para poder después enseñar a terceros los elementos del modelo o de la aplicación necesarios para hacer visible y controlable su funcionamiento» (*op. cit.*, nota 12, p. 86).

ros concernidos por la petición de información[141]. A esta dirección apunta expresamente el CTBG en el Criterio Interpretativo 1/2019, de 24 de septiembre, en donde se afirma que «el perjuicio a los intereses económicos y comerciales puede venir referido tanto al sujeto al que se dirige la solicitud de información o que debe publicarla por tratarse de publicidad activa (por ejemplo, el caso de una sociedad mercantil participada en más del 50% por una Administración Pública) como a un tercero del que una Administración Pública posea información […]»[142].

Ahora bien, en línea con la necesidad de interpretar restrictivamente los límites plenamente consolidada en la jurisprudencia recaída sobre nuestra legislación de transparencia, la tendencia doctrinal preponderante es ceñir la aplicación de este límite a aquellos sujetos públicos que ejerzan una actividad empresarial, pues sólo estos tienen unos intereses económicos o comerciales que proteger. Así, pues, bajo este prisma, únicamente el sector público empresarial podría recurrir a este límite en salvaguarda de sus propios intereses[143].

Dando por bueno este enfoque doctrinal, y salvando —claro está— el ámbito recién mencionado, en vano la Administración podrá apelar al artículo 14.1.h) LTAIBG para denegar la información sobre el algoritmo —o parte del mismo— que ella misma haya elaborado[144].

III.2.3. *El límite de la seguridad pública*

En ocasiones, ante la pretensión de acceder a aplicaciones informáticas o algoritmos, se esgrime el límite de la «seguridad pública» arguyéndose la vulnerabilidad que supondría para las propias aplicaciones su conocimiento por terceros. De este modo, el límite del artículo 14.1.d) LTAIBG se identifica, sin más, con la «seguridad informática».

Esta es la posición a la que parece escorarse la única resolución judicial que hasta la fecha ha abordado directamente esta cuestión, a saber, la Sentencia 143/2021 del Juzgado Central de lo Contencioso Administrativo nº 8, de 30 de diciembre de 2021, que vino a desestimar el recurso interpuesto por la Fundación

---

[141] Así, siquiera como *obiter dictum*, ya en la Resolución del Consejo de Transparencia y Protección de Datos de Andalucía 42/2016, FJ 8º.

[142] Véase su epígrafe II.3.2 («Sujetos»).

[143] En este sentido, Guichot, E.; Barrero Rodríguez, C., *op. cit.*, nota 67, pp. 350-351. Incluso de modo más estricto, Fernández Ramos y Pérez Monguió sostienen que el límite resulta particularmente de aplicación respecto de «las sociedades mercantiles del sector público que concurran en el mercado […] En cambio, es más cuestionable la alegación de este límite por entidades de Derecho Público, como las entidades públicas empresariales» (*op. cit.*, nota 85, p. 178).

[144] Asimismo, en opinión de Danielle Keats Citron, la excepción de los «secretos comerciales» de la FOIA es inaplicable a la parte del código fuente confeccionada por personal de la Administración («Technological Due Process», en: *Washington University Law Review,* Vol. 85 Issue 6, 2008, pp. 1292-1293).

Civio contra la Resolución CTBG 701/2018. Sencillamente, en lo que concierne al punto que ahora nos interesa, el Juzgado se limitó a transcribir sin ulterior argumentación el informe remitido por la Administración en el que se sostenía que la revelación del código fuente haría a la aplicación sensible a los ataques dadas sus vulnerabilidades, dando así por sentado que la noción de «seguridad pública» abarca sin más e incondicionalmente la seguridad informática (Fundamento de Derecho Cuarto).

A nuestro juicio, sin embargo, esta plena equiparación supone una lectura expansiva y, por ende, insostenible del límite, máxime cuando soslaya la noción de «seguridad pública» que cabe inferir de la Constitución. En efecto, para la delimitación del ámbito material del art. 14.1.d) LTAIBG, la mejor doctrina parte de la noción constitucional de «seguridad pública», que la identifica con protección de personas y bienes, vinculándola así, por tanto, con la garantía del orden ciudadano; circunstancia que no entraña que se circunscriba a la acción de las fuerzas y cuerpos de seguridad del Estado, sino también a otros ámbitos, como sucede con la preservación del normal funcionamiento de determinadas infraestructuras críticas[145].

Esta aproximación material a la noción de «seguridad pública» es la que con carácter general siguen mayoritariamente las autoridades de control. Baste mencionar como ejemplo la Resolución del Consejo de Transparencia de Andalucía 3/2017 (FJ 4º), que se apoyó en la doctrina elaborada por el Tribunal Constitucional al respecto al interpretar el art. 104.1 CE y el título competencial del Estado *ex* art.149.1.29ª CE: «[…] según la jurisprudencia constitucional, por seguridad pública ha de entenderse la "actividad dirigida a la protección de personas y bienes y al mantenimiento de la tranquilidad y el orden ciudadano", la cual incluye "un conjunto plural y diversificado de actuaciones, distintas por su naturaleza y contenido, aunque orientadas a una misma finalidad tuitiva del bien jurídico así definido" (baste citar las SSTC 33/1982, FJ 3º, 154/2005, FJ 5º y, más recientemente, la STC 184/2016, FJ 3º). Actividades de protección entre las que hay que incluir, lógicamente, de forma predominante, las que corresponden a las Fuerzas y Cuerpos de seguridad a que se refiere el art. 104.1 CE (STC 104/1989, FJ 3º).»

«Sin embargo —proseguía el FJ 4º de la citada Resolución 3/2017—, aunque tal protección se lleve a cabo preferentemente mediante la actividad policial propiamente dicha, su ámbito puede extenderse más allá de las intervenciones de la llamada «policía de seguridad». En este sentido, la jurisprudencia constitucional ha subrayado la relación que guarda con la «seguridad pública» la materia «protección civil» (STC

[145] Guichot, E.; Barrero Rodríguez, C., *op. cit.*, nota 67, pp. 168-169; asimismo, Fernández Ramos, S.; Pérez Monguió, J. M., *op.cit.*, nota 85, pp. 262-268. Sobre la aplicación natural de este límite a los algoritmos empleados por las fuerzas y cuerpos de seguridad del Estado en el ámbito de la policía predictiva, véase Rivero Ortega, R., «Algoritmos, inteligencia artificial y policía predictiva del Estado vigilante», en: *Revista General de Derecho Administrativo*, núm. 62, 2023, apartado 5 («Garantías adaptadas a la protección de la seguridad»).

155/2013, FJ 3º); razón por la cual, en principio, también sería operativo el límite del art. 14.1 d) LTAIBG en relación con este sector material.»

Por otra parte, también es reconducible al límite de la seguridad pública la información atinente a «la acreditación de la identidad de los ciudadanos», ya que constituye «una premisa para que los poderes públicos puedan cumplir su función de perseguir los delitos y garantizar a la vez la seguridad ciudadana y la paz social» [STC 10/2023, FJ 4º (i)][146]. Y, en fin, es cierto que la ciberseguridad también es susceptible de conectarse genéricamente con el límite *ex* art. 14.1 d) LTAIBG, pero cabe esa identificación «con la seguridad nacional o con la seguridad pública cuando se trata de la protección ordinaria de las redes y las infraestructuras de telecomunicaciones» (STC 142/2018, FJ 5º)[147].

Y esta aproximación constitucionalmente adecuada a la noción de «seguridad pública» es la que subyace tras las decisiones de las autoridades de control que han debido abordar la aplicabilidad de este límite cuando de acceso a algoritmos se trata. Así, la GAIP, en la Resolución 200/2017, a propósito del programa informático destinado a determinar la composición de los tribunales de las pruebas de acceso a la Universidad, argumentaría lo siguiente sobre este particular: «Este código fuente se tiene que limitar a recoger y aplicar correctamente las variables antes mencionadas (requerimientos de paridad entre hombres y mujeres y de porcentajes mínimos de profesores universitarios y de bachillerato, etc.), de forma reglada, sin que su conocimiento por terceros ponga en peligro la población ni ningún colectivo en particular. Si lo que se trata es de evitar que el código fuente pueda ser manipulado por terceros, esto no se garantiza impidiendo su conocimiento, sino adoptando las medidas de seguridad necesarias para evitar que terceras personas puedan acceder —presencialmente o de forma remota— a los ordenadores y sistemas informáticos que lo utilizan».

Y también a esta dirección parece apuntar el CTBG, aunque de forma más críptica, en la Resolución 701/2018, de 18 de febrero de 2019, que consideró que no resultaba de aplicación este límite a la petición de acceder al código fuente de la aplicación utilizada para comprobar que los solicitantes del bono social satisfacen los requisitos para ser catalogados como consumidores vulnerables. En efecto, tras apuntar que la Administración se había ceñido a invocar los límites de la seguridad nacional y la seguridad pública sin una mínima argumentación[148], concluiría el Consejo: «Teniendo en

[146] La STC 10/2023 resolvió un recurso de inconstitucionalidad interpuesto contra el Real Decreto-Ley 14/2019, de 31 de octubre, por el que se adoptaron medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones.

[147] Con carácter general, cabría considerar que entra en juego este límite cuando la divulgación de la información «pueda afectar a la seguridad de las instalaciones calificadas como estratégicas o críticas» [FJ 5º de la Sentencia de la Audiencia Nacional, de 17 de junio de 2020 (Núm. de Recurso: 70/2019; Roj: SAN 1377/2020), aunque refiriéndose a la garantía de la confidencialidad *ex* art. 14.1. k) LTAIBG que es lo que había invocado la entidad recurrente].

[148] De «inconsistente apelación a la seguridad de la Administración» califica Presno Linera la invocación de este límite en relación con el código fuente del sistema BOSCO (*Derechos fundamentales e inteligencia artificial*, Marcial Pons, Madrid, 2022, p. 80).

cuenta la ausencia de argumentos, *la naturaleza de la información solicitada* y las restricciones con la que los Tribunales de Justicia entienden que deben aplicarse los límites al derecho de acceso a la información, este Consejo de Transparencia no comparte que los límites aludidos sean de aplicación» (FJ 4º; el énfasis es nuestro)[149].

Ciertamente, es difícil no compartir esta posición tendente a rehuir la pura y simple equiparación mecánica entre seguridad informática y seguridad pública al objeto de denegar toda pretensión de acceso en materia de algoritmos. Pues, aun en la hipótesis de que existieran eventuales riesgos de vulnerabilidad, la aplicación del límite, lejos de operar como estímulo para que la Administración procurase la mejora de la seguridad informática, podría tener el efecto contrario, al primarse su falta de diligencia con la opacidad de sus sistemas algorítmicos. Como oportunamente ha apuntado un sector de la doctrina a propósito del caso del bono social, «los riesgos de seguridad por acceso a un algoritmo de esta naturaleza debieran ser inexistentes y, si efectivamente se pudieran dar, es responsabilidad de la Administración evitarlos por otros medios que no supongan eliminar la posibilidad de acceder a conocer cómo se realiza en la práctica el cálculo»[150].

En consecuencia, la razonable aplicación del límite *ex* art. 14.1.d) LTAIBG a la pretensión de acceder a algoritmos debe circunscribirse a aquellos casos en que se afecte la materia «seguridad pública» en el sentido constitucional antes referido, pues, de lo contrario, este límite se convertiría en un caballo de Troya para la transparencia algorítmica.

En lo concerniente al tratamiento de la seguridad como causa impeditiva del acceso a los programas informáticos, resulta de interés la experiencia francesa. Como muestra de una aplicación del límite de la «seguridad pública» ceñida a su noción material, cabe mencionar el dictamen de la CADA 20163619, de 20 de octubre, relativo a la pretensión de acceder a la aplicación móvil SAIP, que utilizaba el Ministerio de Interior para enviar a través de los teléfonos móviles notificaciones de alerta tras la sospecha de un ataque o hechos excepcionales de seguridad civil. Dada su evidente conexión con el ámbito material tutelado por el límite, la Comisión secundó la alegación del Ministerio de que facilitar el código fuente facilitaría los ataques contra la aplicación, hasta el punto de llegar a neutralizarla, por lo que denegó el acceso al mismo.

Pero es de notar que, a partir de la Ley nº 2016-1321, de 7 de octubre de 2016, por una República digital, se incorporó específicamente en el Código de Relaciones entre el Público y la Administración como límite del acceso «la seguridad de los sistemas de información de las administraciones», que vendría así a sumarse a la «seguridad pública» y a la «seguridad de las personas» que ya aparecían en la anterior versión del

[149] Se ha reprochado a esta Resolución que no entrase a valorar las vulnerabilidades concretas de la aplicación alegadas por la Administración (Gutiérrez David, M. E., *op. cit.*, nota 10, p. 171).

[150] Boix Palop, A., *op. cit.*, nota 94, p. 95.

Código[151]. Una muestra de la operatividad práctica de la ampliación del límite a la «seguridad de los sistemas de información» proporciona el Dictamen de la CADA de 15 de abril de 2021 (*Avis* 21210021), toda vez que fue determinante para que se rechazara la pretensión de que se comunicasen los códigos fuentes producidos y utilizados por la plataforma de datos de salud «Health Data Hub».

III.2.4. *La eventual aplicabilidad de otros límites*

a) La defensa de la Administración frente al riesgo de eludir el algoritmo

Antes de dar por concluido este apartado referente a los límites establecidos en la legislación de transparencia, no parece impertinente dedicar siquiera unas líneas a una de las principales consecuencias perniciosas que la apertura de los algoritmos puede entrañar para una correcta y eficaz toma de decisiones por las autoridades públicas: que el conocimiento de su funcionamiento permita a los potenciales destinatarios de sus decisiones «burlar» el algoritmo al objeto de eludir la correspondiente normativa que resulte de aplicación. Así es; en cuanto se hace público el modelo algorítmico, los eventuales afectados pueden detectar los indicadores utilizados y, consecuentemente, están en condiciones de sortearlos. En suma, es un lugar común en la literatura especializada señalar que, si se accede a la totalidad del algoritmo empleado por la Administración pública, se abre la posibilidad de erosionar la eficacia del sistema automatizado de decisiones[152].

Dos son los principales ámbitos materiales que la generalidad de la doctrina tiende a identificar como especialmente sensibles en relación con estos problemas de *gaming* o elusión del algoritmo[153]. Por una parte, la esfera penal, en donde resultan evidentes los efectos perversos derivados del conocimiento de los algoritmos conectados con las técnicas de investigación o los programas de policía predictiva[154]. En especial, se ha puesto

---

[151] Tras esta modificación, el artículo L-311-5, apartado 2º d) del Código impide que se pueden comunicar los documentos administrativos cuyo conocimiento pueda atentar: «d) A la sûreté de l'Etat, à la sécurité publique, à la sécurité des personnes ou à la sécurité des systèmes d'information des administrations». Y en «la seguridad de las personas o la seguridad de los sistemas de información de las administraciones» se fundamentó la CADA en el *Avis* 20200496, de 12 de marzo de 2020, para confirmar la decisión del Ministerio del Interior de denegar el código fuente de la aplicación ALICEM, que permite la autenticación de la propia identidad desde el teléfono móvil y da acceso a determinados servicios disponibles a través de FranceConnect.

[152] Diakopoulos, N., *op. cit.*, nota 30, p. 12.

[153] Obviamos por afectar fundamentalmente al sector privado otro de los ámbitos tradicionalmente sensibles a esta problemática: el de la calificación crediticia.

[154] Así, por traer como muestra un ejemplo utilizado en materia de terrorismo, si un potencial terrorista llega a conocer que uno de los indicadores es pagar en metálico los pasajes de avión, obviamente resulta muy fácil eludirlo [LAAT, P. B. de, «Algorithmic Decision-Making Based on Machine Learning from Big Data: Can Transparency Restore Accountability?», en: *Philos. Technol* 2017, p. 11 [https://doi.org/10.1007/s13347-017-0293-z].

el foco en aquellos algoritmos que se centran en delitos fácilmente resolubles debido a su simplicidad y al reducido número de factores de entrada con los que operan[155].

Por otro lado, la materia impositiva es asimismo un terreno abonado para que el acceso al funcionamiento de los algoritmos genere efectos indeseados. Conocer los aspectos específicos de las declaraciones de impuestos que se utilizan como posibles indicadores de fraude fiscal, permitiría lógicamente a los contribuyentes acomodar sus pautas de comportamiento y provocar, con ello, que tales indicadores perdieran su valor predictivo para la Administración tributaria[156]. En esta línea, por mencionar un ejemplo tomado del sistema fiscal automatizado alemán, usualmente se concede la deducción por donativos sin demasiada revisión, pero a partir de determinada cantidad crítica sí se realizan controles detallados al respecto, por lo que, como es obvio, acceder a este último dato facilitaría la utilización indebida de esta bonificación[157].

Pues bien, en numerosas ocasiones los sectores materiales antes indicados se hallan protegidos por específicos límites establecidos en las respectivas leyes reguladoras del derecho de acceso a la información pública.

En lo referente a la actuación en la esfera penal —y soslayando el ya examinado límite de la seguridad pública—, parece que lógicamente podría entrar en juego en nuestro caso el límite de la «prevención, investigación y sanción de los ilícitos penales, administrativos o disciplinarios» [art. 14.1.e) LTAIBG] para rechazar la pretensión de conocer eventuales sistemas automatizados destinados a la investigación o predicción delictiva[158].

---

[155] Oswald, M. *et al.*, *The UK Algorithmic Transparency Standard: A Qualitative Analysis of Police Perspectives*, 7 julio 2022, p. 17 (https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4155549). Se trata de un informe, realizado a partir de entrevistas con diferentes responsables de cuerpos policiales y otros departamentos, sobre los riesgos y ventajas de la transparencia en este ámbito. Es un trabajo elaborado en relación con el proyecto del Gobierno británico *Algorithmic Transparency Standard*; documento cuyo objetivo es proporcionar a las autoridades públicas una fórmula estandarizada para dar información sobre la forma en que emplean las herramientas algorítmicas para adoptar sus decisiones. La explicación que dio uno de los entrevistados respecto de dichos algoritmos utilizados para resolver delitos sencillos fue muy elocuente: «Si conocieras todo sobre esto [lo que hace el algoritmo], podrías cometer un delito siendo sólo cuidadoso con muy pocas pruebas».

[156] Kroll, J. A. *et al.*, «Accountable Algorithms», en: *University of Pennsylvania Law Review*, Vol. 165, 2017 p. 658.

[157] Martini, M.; Nink, D., *op. cit.*, nota 15, pp. 11-12.

[158] Conviene notar que, desde el punto de vista de la transparencia garantizada por el derecho a la protección de datos personales, existe en materia penal una normativa específica que se aleja notablemente —por razones obvias— del régimen general establecido en el Reglamento General de Protección de Datos. Es, en efecto, la Directiva (UE) 2016/680, de 27 de abril de 2016, la que se encarga de regular el tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales. Esta Directiva suprime la obligación del responsable del tratamiento de informar sobre las decisiones automatizadas (art. 13), a las que tampoco se extiende el derecho de acceso al afectado (art. 14); aspectos ambos que, como apuntamos *supra* en el epígrafe II.1, sí forman parte de las garantías de trasparencia del RGPD [art. 13.2.f) y art. 14.2.g); art. 15.1.h)]. Y lógicamente la Ley Orgánica 7/2021, de transposición de la referida Directiva, mantiene dichas decisiones (arts. 21 y 22).

Por lo que hace a Estados Unidos, resulta de aplicación en este ámbito la Exención 7 (E) de la FOIA, que excluye del derecho de acceso a «los archivos o la información compilada para fines de cumplimiento de la ley (*law enforcement*), pero únicamente en la medida en que la exposición de tales archivos o información… E) revelase «técnicas y procedimientos» o «directrices» para las investigaciones, y si de tal divulgación «pudiera razonablemente esperarse un riesgo de evasión de la ley». La principal cuestión suscitada en torno a esta exención es si debe ceñirse estrictamente a los supuestos de «investigación» —que conlleva las tareas de identificación de los posibles involucrados y de recopilación de pruebas sobre delitos *ya* cometidos—, quedando en consecuencia al margen de la misma los programas algorítmicos de policía preventiva, o si, por el contrario, también a estos podría extenderse su aplicación. Si bien hay diversos precedentes jurisprudenciales en los que se aplicó el límite respecto de determinadas medidas preventivas (aunque no atinentes a algoritmos), no faltan voces en la doctrina que consideran que aquellos programas de policía predictiva que ponen el acento en la disuasión antes que en la investigación se encuentran al borde de la exención o, lisa y llanamente, a extramuros de la misma[159]. Es de notar, por otro lado, que a esta Exención 7 (E) también se ha recurrido para retener información sobre las técnicas utilizadas para evaluar el cumplimiento de la legislación tributaria, toda vez que su revelación «puede posibilitar que los evasores fiscales eviten ser detectados» [*Palmarini v. Internal Revenue Service*, No. 17-3430, 2019 WL 1429547 (E.D. Pa. Mar. 29, 2019)][160].

Por su parte, la legislación federal alemana establece un específico límite en materia impositiva, ya que el § 3.1 d) de la *Informationsfreiheitsgesetz* excluye expresamente que pueda solicitarse información que entrañe perjuicios para las funciones de inspección o control de las autoridades fiscales. Y ello con independencia de que en la propia legislación sectorial se contemple de forma explícita la restricción de la publicidad al respecto, como hace el § 88 (5) de la *Abgabenordnung*, que dispone que «[l]os detalles de los sistemas de gestión de riesgos no podrán publicarse en la medida en que ello pueda poner en peligro la uniformidad y la legalidad de la tributación».

En lo que a nosotros concierne, este ámbito material parece hallarse bajo la cobertura del límite atinente a las «funciones administrativas de vigilancia, inspección y control» [art. 14.1.g) LTAIBG]. Nótese que la *Memoria Explicativa del Convenio del Consejo de Europa sobre el Acceso a los Documentos Públicos*, de 18 de junio de 2009 —Convenio cuya influencia en la conformación del sistema de límites establecido en la LTAIBG ha destacado alguna autoridad de control—, menciona concretamente a las inspecciones tributarias como uno de los ejemplos de este límite (véase el punto 27 de la Memoria). A esta dirección apunta inequívocamente la posición del CTBG sostenida en la Resolución 825/2019, de 13 de febrero de 2020: «[…] este Consejo de

[159] Brauneis, R.; Goodman, E. P., *op. cit.*, nota 131, pp. 160-161.

[160] Otras referencias jurisprudenciales sobre la aplicación de esta exención en materia impositiva proporciona Tal Z. Zarsky («Transparent Predictions», en: *University of Illinois Law Review*, Vol. 2013, No 4, 2013, p. 1512, nota 54).

Transparencia y Buen Gobierno —afirma en su FJ 4º— sí puede compartir el criterio de que proporcionar información detallada sobre el funcionamiento de unas aplicaciones creadas para el desarrollo de las funciones encomendadas a la AEAT —aplicación efectiva del sistema tributario estatal y aduanero— de tal manera que se proporcione el detalle de los instrumentos de los que dispone para el ejercicio de dichas funciones y, por lo tanto, el alcance y límites de sus posibilidades de actuación sí podría implicar un perjuicio, razonable y no meramente hipotético a sus actividades de investigación y supervisión y, por lo tanto, a *Las funciones administrativas de vigilancia, inspección y control (art. 14.1 g) de la LTAIBG)* que tiene encomendadas.»[161]

Pero con independencia de estas restricciones al acceso fundamentadas en límites directamente relacionados con los específicos sectores materiales antes referidos, la cuestión central que ahora debemos plantearnos es si cabe recurrir a algún otro límite general, de carácter transversal, que pueda utilizarse para hacer frente al *gaming* sean cuales fueren los ámbitos materiales afectados por el correspondiente algoritmo.

b) El límite de la confidencialidad o el secreto requerido en procesos de toma de decisión

En los Estados Unidos, se especuló con la posibilidad de proyectar a los programas de ordenador la Exención 2 de la FOIA, que excluye del acceso a aquellos documentos que están «relacionados únicamente con las reglas y prácticas internas de personal de una agencia» [*related solely to the internal personnel rules and practices of an agency*]. Debe notarse que la jurisprudencia ha interpretado que la excepción comprende dos tipos de información: por una parte, asuntos internos de naturaleza rutinaria o relativamente trivial, que no son objeto de un genuino y significativo interés público (a la que frecuentemente se denomina *«low 2» information*); y, por otro lado, aquellos otros asuntos más sustanciales cuya divulgación podría entrañar el riesgo de elusión de una exigencia legal (la conocida como *«high 2» information*). El origen último de la doctrina sobre este segundo tipo de información se remonta a la Sentencia del Tribunal Su-

[161] Sobre este particular, ha de tenerse presente lo dispuesto en el artículo 170.7 del Real Decreto 1065/2007, de 27 de julio, por el que se aprueba el Reglamento General de las actuaciones y los procedimientos de gestión e inspección tributaria y de desarrollo de las normas comunes de los procedimientos de aplicación de los tributos: «Los planes de inspección, los medios informáticos de tratamiento de información y los demás sistemas de selección de los obligados tributarios que vayan a ser objeto de actuaciones inspectoras tendrán carácter reservado, no serán objeto de publicidad o de comunicación ni se pondrán de manifiesto a los obligados tributarios ni a órganos ajenos a la aplicación de los tributos.» Determinar con exactitud cuál sea el alcance efectivo de esta disposición tras la aprobación de la LTAIBG merece un tratamiento específico cuyo abordaje excede del sentido y finalidad de este trabajo. Véanse al respecto Olivares Olivares, B., «Transparencia y aplicaciones informáticas en la Administración tributaria», en: *Crónica Tributaria*, núm. 174, 2000, pp. 97-98; Soto Bernabeu, L., «La importancia de la transparencia algorítmica en el uso de la inteligencia artificial por la Administración tributaria», en: *Crónica Tributaria*, núm. 179, 2021, p. 109.

premo, de 21 de abril de 1976, *Department of the Air Force v. Rose*[162], en donde, tras declarar que la exención cubría los asuntos internos de carácter trivial, dejó abierta la posibilidad de extender la misma a lo que luego sería conocido como *«high 2» information*[163]. Y a partir del año 1981, a raíz de la Sentencia del Tribunal de apelaciones para el Distrito de Columbia *Crooker v. ATF*[164], se asumiría durante más de treinta años la interpretación de que la Exención 2 abarcaba la información cuya divulgación podría suponer un riesgo para la elusión (*circumvention*) de la ley, y ello con independencia de que la misma estuviera relacionada o no con asuntos de personal. No es de extrañar, por tanto, que en el Informe elaborado en el año 1990 por el Departamento de Justicia sobre el «documento electrónico» en el marco de la FOIA, se barajase abiertamente la posibilidad de que la protección de la *circumvention* se aplicase a cualquier elemento del software —tales como códigos y otros componentes de seguridad— que se considerase susceptible de generar la elusión en caso de concederse el acceso[165].

El estado de la cuestión cambió sustancialmente el año 2011 con motivo de la Sentencia del Tribunal Supremo *Milner v. Department of the Navy*[166], puesto que redujo estrictamente el alcance de la exención a la información referente a relaciones con los empleados y recursos humanos. En su argumentación puso el acento en el tenor literal del precepto para llegar a dicha conclusión —concretamente en el hecho de que la palabra «personal» se emplea como adjetivo de «reglas y prácticas»—, de tal modo que la exención quedaría circunscrita a «las condiciones de empleo en las agencias federales —asuntos tales como contratación y despido, reglas sobre condiciones de trabajo y régimen disciplinario, remuneración y prestaciones»[167]. Esta es la línea jurisprudencial hoy vigente, de la que evidentemente poco cabe esperar en punto a la posibilidad de negar, con base en la Exención 2, información que permita «jugar» con el algoritmo al objeto de sortear obligaciones jurídicas o, sencillamente, lograr una decisión favorable a los intereses del afectado[168].

Otra de las previsiones de la FOIA sobre la que se ha especulado acerca de su aplicabilidad a las decisiones algorítmicas es el «privilegio del proceso de deliberación» (*deliberative process privilege*) contenido en la Exención 5, cuyo objetivo último es

---

[162] 425 U.S. 352 (1976).

[163] «En suma, creemos que, salvo que se trate de una situación en la que la divulgación pueda entrañar un riesgo de elusión de la regulación de la agencia, la Exención 2 no es aplicable a asuntos sujetos a un interés público [tan] genuino y significativo» (*Id.*, 369).

[164] 670 F.2d 1051 (D.C. Cir. 1981).

[165] *Department of Justice Report on «Electronic Record» FOIA Issues*, Part II. FOIA Update Vol. XI, Nº 3, 1990.

[166] 562 U.S. 562 (2011).

[167] *Idem*, 570.

[168] Así, por ejemplo, se ha considerado inaplicable la exención en relación con los códigos informáticos pertenecientes a una base de datos sensible [*Skinner v. DOJ*, 806 F. Supp. 2d 105, 112 (D.D.C. 2011)]. Sobre esta Sentencia y, en general, sobre esta Exención 2, consúltese *Department of Justice Guide to the Freedom Information Act. Exemption 2* (29 de septiembre de 2020).

«evitar un perjuicio en la calidad de las decisiones» que adopten las Administraciones[169]. Como se describiría gráficamente en *Wolfe v. Dep't of Health & Human Servs.*, el Congreso aprobó esta exención porque era consciente de que «la calidad de la toma de decisiones administrativas quedaría seriamente socavada si las agencias estuvieran obligadas a operar en una pecera»[170]. Pues bien, la jurisprudencia tradicionalmente ha exigido dos requisitos que deben cumplirse cumulativamente para que pueda invocarse exitosamente este privilegio: de un lado, la información pretendida debe haberse generado antes de que se adopte la decisión, y, en segundo término, ha de formar parte del proceso deliberativo en el que se hacen recomendaciones, se dan consejos o se expresan opiniones sobre las cuestiones objeto de la decisión en cuestión.

En lo concerniente a este último requisito, que es el que genera más controversia en la práctica, es de reseñar que la jurisprudencia sostiene que queda al margen de la exención la información sobre hechos, habida cuenta de que la divulgación de esta información factual no conlleva exponer las deliberaciones u opiniones del personal de la Administración. Naturalmente, en ocasiones es una tarea compleja distinguir entre el material meramente fáctico y el material genuinamente deliberativo, por lo que ha de descenderse al examen de los casos concretos para averiguar si los hechos están tan estrechamente integrados en el proceso deliberativo que su revelación puede causarle un perjuicio.

Así, por citar algunos ejemplos que guardan proximidad con el tema que nos ocupa, se han considerado cubiertos por la exención unos programas de ordenador usados en una investigación científica, al argumentarse que la autora del estudio modificaba regularmente el software durante el transcurso de la investigación para acomodarlo a la evolución de las hipótesis de las que inicialmente partía el trabajo, de tal suerte que los programas «reflejaban los procesos mentales de su creadora» y revelaban sus «deliberaciones y opiniones científicas». Sus deliberaciones y opiniones estaban, pues, «inextricablemente entrelazadas» con los hechos subyacentes[171]. Igualmente se ha entendido aplicable la exención a un modelo diseñado para medir la contaminación de las aguas subterráneas que se hallaba aún en fase de proyecto, ya que los datos a introducir en el modelo y el ajuste del mismo únicamente reflejaban en esta fase las opiniones del personal que lo desarrollaba, al no poder considerarse que representasen las opiniones definitivas de la agencia al respecto. Por consiguiente, concluiría el Tribunal en este caso, «aunque los datos introducidos en el modelo sean puramente factuales, la selección y ajuste de los datos forman parte del proceso deliberativo al que se aplica la exención 5»[172].

Por el contrario, en fecha más reciente, se ha negado la aplicación de la exención a un integrante del modelo OMEGA diseñado por la Administración para medir la emi-

---

[169] *NLRB v. Sears, Roebuck & Co.*, 421 U.S. 132, 151 (1975).

[170] 839 F.2d 768, 773 (D.C.Cir.1988) (en banc); citado en *Brennan Center for Justice at New York University School of Law v. United States Department of Justice*, 697 F.3d 184, 194 (2d Cir. 2012).

[171] *Cleary, Gottlieb, Steen & Hamilton v. HHS*, 844 F. Supp. 770, 782-783 (D.D.C. 1993).

[172] *Goodrich Corp. v. U.S. EPA*, 593 F. Supp. 2d 184, 189 (D.D.C. 2009).

sión de contaminantes de los vehículos a motor. Más específicamente, el objeto de la solicitud de información era el tercero de sus componentes, el «modelo central» (*core model)*, que estaba compuesto por una serie de algoritmos que efectuaban miles de cálculos en relación con los datos introducidos en el sistema al objeto de predecir la tecnología de reducción de emisiones que los fabricantes podrían incorporar para acomodarse a los estándares impuestos por la normativa medioambiental. En el marco del modelo OMEGA en su conjunto —argumentaría el Tribunal—, los puntos de vista subjetivos de la Administración se reflejaban en la determinación de los *inputs* que se introducían en el sistema, pero el *core model* se ceñía a realizar cálculos a partir de tales datos. Así, pues, en la medida en que el modelo central operaba como «una calculadora especializada, que utiliza los mismos algoritmos para realizar los mismos cálculos en cada ejecución de OMEGA», y en consecuencia sólo proporcionaba «una visión muy abstracta de las deliberaciones» de la Administración interpelada, no podía en modo alguno atribuirse carácter deliberativo al mismo. Sencillamente, el «modelo central» no proporcionaba ningún tipo de información al que la doctrina jurisprudencial suele atribuir un riesgo para la libre discusión de los asuntos en el seno de la Administración, como las opiniones, consejos o recomendaciones. En suma, concluiría el Tribunal, «aunque el modelo central puede reflejar en algunos aspectos las deliberaciones internas de la agencia, no puede preverse razonablemente que la divulgación de sus herramientas analíticas menoscabe la calidad de la toma de decisiones por parte de la agencia»[173].

Pues bien, no parece que en la práctica esta exención haya jugado hasta la fecha ningún papel relevante para la denegación de información sobre sistemas automatizados de toma de decisiones. Así, algún trabajo publicado en fecha aún reciente desvela que ningún tribunal ha respaldado el carácter deliberativo de ningún sistema automatizado, pese a que la Administración a menudo sostiene la pertinencia de aplicar la exención al considerar que el proceso de deliberación ha sido auxiliado o desarrollado por medios automatizados. Sencillamente, prevalece la apreciación de que el sistema algorítmico *per se* tiene un carácter fáctico y, por tanto, queda excluido de la exención[174]. Y en esta línea, otro estudio revela que ninguna de las solicitudes de información que los autores habían presentado sobre el particular se rechazaron con base en este «privilegio del proceso de deliberación», por lo que la eventual operatividad de la excepción respecto del acceso a los sistemas algorítmicos permanecía aún en el terreno de la especulación[175].

---

[173] *Nat. Res. Def. Council v. EPA*, 954 F.3d 150, 157-158 (2d Cir. 2020). La Sentencia se apoyaría, entre otros, en el precedente de *Petroleum Info. Corp. v. U.S. Dep't of Interior*: «La divulgación de materiales que no incorporen valoraciones de la agencia —por ejemplos, materiales relacionados con cálculos o mediciones estándares o rutinarios sobre los que la agencia no tiene una discreción significativa— es improbable que disminuya la franqueza (*candor)* de los funcionarios o perjudique de cualquier otra forma la calidad de las decisiones de la agencia» [976 F.2d 1429, 1435 (D.C. Cir. 1992)].

[174] Bloch-Wehba, H., *op. cit.*, nota 29, pp. 1302-1303.

[175] Brauneis, R.; Goodman, E. P., *op. cit.*, nota 131, p. 162.

Pasando ya al examen de nuestro marco jurídico regulador de la transparencia, el límite que mantiene cierto paralelismo con la analizada Exención 5 es el establecido en el artículo 14.1 k) LTAIBG: «La garantía de la confidencialidad o el secreto requerido en procesos de toma de decisión» [art. 14.1 k) LTAIBG]. Se trata de una limitación de cuyo enorme potencial expansivo ha alertado reiteradamente la doctrina, máxime si se vincula o combina con la causa de inadmisión del art. art. 18.1 b) LTAIBG («información que tenga carácter auxiliar o de apoyo»), con la cual guarda una clara relación. Sin embargo, atinadamente se ha impuesto una lectura restrictiva de este motivo de inadmisión a raíz del Criterio Interpretativo del Consejo de Transparencia y Buen Gobierno 6/2015, de 12 de noviembre, en el que, entre otras muchas consideraciones, se sostiene que todo examen sobre la pertinencia de aplicar dicho artículo 18.1.b) LTAIBG ha de estar presidido por la idea de que la finalidad de la LTAIBG es «evitar que se deniegue información que tenga relevancia en la tramitación del expediente o en la conformación de la voluntad pública del órgano, es decir, que sea relevante para la rendición de cuentas, el conocimiento de la toma de decisiones públicas y su aplicación». Línea hermenéutica que conduce casi necesariamente a la convicción de que no cabe proyectar esta causa de inadmisión a «aquella documentación que forme parte del procedimiento, que constituya la *ratio decidendi* de la Administración interpelada o contribuya, en fin, a la intelección de la decisión adoptada por ésta» (Resolución del Consejo de Transparencia y Protección de Datos de Andalucía 10/2020, FJ 3º)[176].

Como parece evidente, este límite tiene como finalidad primordial brindar protección a las deliberaciones en el seno de las instituciones y preservar, así, el normal desenvolvimiento del proceso de toma de decisiones. Para decirlo con los términos utilizados por la *Memoria Explicativa del Convenio del Consejo de Europa sobre el Acceso a los Documentos Públicos* (§ 34) en relación con el límite del artículo 3.1 k), el legislador quiso con este límite asegurar a las instituciones un cierto libre «espacio para pensar»[177].

Pues bien, de acuerdo con la interpretación que hoy puede darse por consolidada de este límite[178], el mismo está llamado a aplicarse cuando se satisfagan al unísono dos requisitos. Por una parte, un condicionante de orden cronológico o temporal según el cual debe tratarse de una solicitud de información que se produzca antes de que la decisión haya sido adoptada, bien porque se solicite en relación con un concreto procedimiento de toma de decisiones aún abierto, bien porque la divulgación de la información pueda condicionar los procesos que se pongan en marcha en el futuro[179].

---

[176] Del mismo Consejo, en esta misma línea, Resoluciones 117/2016, FJ 2º; 228/2018, FJ 3º; 34/2020, FJ 4º; 312/2020, FJ 4º.

[177] En este sentido, por ejemplo, la Resolución 112/2017 del Consejo de Transparencia y Protección de Datos de Andalucía (FJ 4º).

[178] Un análisis detallado del modo en que las autoridades de control de la transparencia están aplicando el límite ofrecen Guichot, E.; Barrero Rodríguez, C., *op. cit.*, nota 67, pp. 307-324.

[179] Así, ya en la Resolución del CTBG 35/2015, FJ 6º: «A juicio de este Consejo de Transparencia y Buen Gobierno, dicho límite sería de aplicación tanto cuando la concesión del acceso a la información solicitada pueda afectar al procedimiento de toma de decisiones mientras éste se esté llevando a cabo, esto

Y, en segundo término, el acceso a la información pretendida debe tener una influencia real en la decisión a tomar[180], esto es, ha de tratarse de «datos cuyo conocimiento anticipado podría perjudicar […], de forma razonable y no meramente hipotética, a las conclusiones del proceso» (Resolución CTBG 104/2019, FJ 5º). En suma, como sintetizó la Resolución CTBG 283/2016: «Puede entenderse que es correcto invocar este límite cuando se está en fase de tomar una decisión importante y su conocimiento público haría variar esa decisión o influir en ella de manera notoria y determinante, tanto en el transcurso de un procedimiento abierto como en situaciones futuras parecidas…» (FJ 5º).

Así definido el alcance y sentido del límite, parece indudable que no abarca aquellos supuestos de decisiones totalmente automatizadas, y muy señaladamente cuando el programa algorítmico se proyecta a una actividad estrictamente reglada de la Administración, puesto que la decisión únicamente depende de la constatación de que en el caso concreto se cumplen los requisitos exigidos por la normativa aplicable incorporados al programa[181]. No hay aquí margen de maniobra para la decisión a adoptar por el personal al servicio de la Administración y, por tanto, no hay que preservar ningún «espacio para pensar» que pueda verse interferido por el conocimiento previo del algoritmo por parte de terceros.

Aunque tampoco resulta asumible considerar incluido en el límite aquellos programas que sólo operan como un elemento más del que puede servirse la Administración, junto a otras consideraciones y factores, para llegar a una concreta decisión. Si acaso, a lo sumo, la garantía de la «confidencialidad o el secreto requerido en procesos de toma de decisión» podría proyectarse a esos otros argumentos, puntos de vista, observaciones u opiniones barajados por el personal de la Administración en el curso del proceso, los cuales, eventualmente, podrían llevar en última instancia a apartarse de la propuesta de decisión sugerida por el algoritmo. En esta hipótesis, y a fin de evitar todo riesgo de opacidad sobre el particular, sería conveniente juridificar la formula apuntada en la Carta de Derechos Fundamentales u otra semejante: «El interesado tendrá derecho a que se motive o se explique la decisión administrativa cuando esta se separe del criterio propuesto por un sistema automatizado o inteligente» [artículo XVIII, apartado 6 c)].

Pero, aun cuando —a efectos puramente dialécticos— se diera por buena la aplicabilidad de este límite a los programas algorítmicos en algunos supuestos, no parece

es, cuando la decisión aún no haya sido adoptada, […] como cuando dichos procesos de toma de decisiones pudieran verse comprometidos *a futuro*».

[180] Para decirlo en los términos de la recién citada Resolución 35/2015, que «el conocimiento de la información pudiera comprometer la decisión que finalmente se adopte» (FJ 6º).

[181] Huergo Lora, A., «El derecho de transparencia en el acceso a los códigos fuente», en: *Anuario de Transparencia Local 5/2022*, Fundación Democracia y Gobierno Local, Madrid, 2023, pp. 38-40. Asimismo, Jiménez-Castellanos Ballesteros, I., «Decisiones automatizadas y transparencia administrativa: nuevos retos para los derechos fundamentales», en: *Revista Española de la Transparencia*, núm. 16, enero-junio 2023, p. 195.

que resulte en ningún caso un instrumento *transversal* adecuado para combatir con alcance general el fenómeno de la elusión del algoritmo. Atendiendo a la necesaria interpretación restrictiva de los límites —tantas veces reclamada por la jurisprudencia—, resulta de casi imposible aceptación que el artículo 14.1 k) LTAIBG autorice *per se* a denegar información para eludir la eventualidad de que los potenciales afectados puedan modificar sus *futuras* conductas o respuestas que deban dar en un procedimiento como consecuencia del conocimiento del funcionamiento del algoritmo.

IV. UN BALANCE. LÍMITES Y POSIBILIDADES DE LA TRANSPARENCIA EN LA TOMA DE DECISIONES AUTOMATIZADAS

Hemos analizado hasta el momento los límites y las posibilidades que derivan de la legislación reguladora de la transparencia y del derecho a la protección de datos personales en punto a asegurar una adecuada información sobre los sistemas automatizados de toma de decisiones por parte de las Administraciones públicas. Y, salvando acaso la experiencia francesa, hemos constatado que con alcance general dista de lograrse un adecuado nivel de accesibilidad a este tipo de información en los países de nuestro entorno. De ahí que no sean infrecuentes las apelaciones a que se profundice en la transparencia en este ámbito adoptando las medidas legislativas necesarias para asegurarla. Llamadas al legislador que, incluso, proceden directamente de las propias autoridades independientes de control.

Especialmente significativa a este respecto ha sido la posición mantenida por las autoridades de control alemanas en materia de derecho de acceso a la información —que, al tiempo, son asimismo competentes en relación con el derecho a la protección de datos personales—, que el 16 de octubre de 2018 suscribieron el documento «La transparencia de la Administración en la utilización de algoritmos, indispensable para una protección real de los derechos fundamentales» (*Transparenz der Verwaltung beim Einsatz von Algorithmen für gelebten Grundrechtsschutz unabdingbar*). A partir de la premisa de que «la información sobre los algoritmos y los procedimientos de inteligencia artificial que resultan esenciales para la Administración deberían también ponerse a disposición de la opinión pública», dichas autoridades de control explícitamente «piden a los legisladores del Bund y de los Länder que obliguen a los organismos públicos a utilizar de modo transparente y responsable los algoritmos y los procedimientos de inteligencia artificial, incluso de forma más firme que lo han hecho hasta la fecha». Y prosigue el documento: «Es aconsejable anclar las correspondientes disposiciones de transparencia en las respectivas leyes de libertad de información o transparencia o en las leyes especializadas pertinentes. Las excepciones deben reducirse al mínimo».

Aunque un paso previo casi obligado para asegurar la accesibilidad a los procedimientos algorítmicos por parte de la ciudadanía, es que la propia Administración

cuente con la pertinente información: «Los organismos públicos deben garantizar una transparencia suficiente sobre los algoritmos utilizados. Para un uso controlable de la tecnología, deben disponer de información significativa, completa y generalmente comprensible sobre su propio tratamiento de datos. Esta información comprende sobre todo: —las categorías de los datos de entrada y de salida del procedimiento; —la lógica contenida en ellos, en particular las fórmulas de cálculo utilizadas, incluida la ponderación de los datos de entrada, la información sobre los conocimientos técnicos subyacentes y la configuración individual por parte de los usuarios; y — el alcance de las decisiones basadas en ellos y los posibles efectos de los procedimientos. En la medida de lo legalmente posible, esta información debe hacerse pública.» Pero no se agota aquí el nivel de transparencia que resulta aconsejable alcanzar desde la perspectiva de las autoridades de control alemanas: «Para garantizar una verificabilidad completa, el código fuente y, en su caso, otra información pertinente sobre los algoritmos o procedimientos de IA también deben ponerse a disposición de los organismos públicos respectivos. Los procedimientos de IA deben ponerse a disposición de las autoridades públicas respectivas y, si es posible, publicarse.»

Esta llamada a la necesaria profundización de la transparencia en el sector público es asimismo habitual, desde hace algún tiempo, en la literatura especializada de nuestro país[182]. Y lo cierto es que algún avance al respecto se ha experimentado ya en la práctica, poniéndose así de manifiesto que la pretensión de la Carta de Derechos Digitales de servir a modo de acicate o estímulo para extender la transparencia en el ordenamiento jurídico ha comenzado a dar sus primeros frutos.

En el plano de la publicidad activa, tal y como reseñamos *supra* en el apartado III.1.2.c), la Comunidad Autónoma valenciana ya ha procedido a incorporar en su legislación de transparencia concretas obligaciones sobre el particular[183]. Y con anterioridad el «Reglamento de actuación y funcionamiento del sector público por medios electrónicos» (que fue aprobado por el Real Decreto 203/2021, de 30 de marzo) estableció como contenido obligatorio de las sedes electrónicas la «[r]elación actualizada

[182] Algún paso significativo se dio ya de forma pionera en el ámbito privado con el Real Decreto Ley 9/2021, de 11 de mayo, por el que se modificó el texto refundido de la Ley del Estatuto de los Trabajadores para garantizar los derechos laborales de las personas dedicadas al reparto en el ámbito de plataformas digitales. Vino a ampliar el ámbito materialmente protegido del derecho fundamental a la libertad sindical al incorporar una nueva letra d) en el artículo 64.4 del Estatuto de los Trabajadores, en cuya virtud se incluye entre los derechos de información del Comité de Empresa el de «[s]er informado por la empresa de los parámetros, reglas e instrucciones en los que se basan los algoritmos o sistemas de inteligencia artificial que afectan a la toma de decisiones que pueden incidir en las condiciones de trabajo, el acceso y mantenimiento del empleo, incluida la elaboración de perfiles».

[183] La Ley 1/2022, de 13 de abril, de Transparencia y Buen Gobierno de la Generalitat Valenciana, incluye entre la información que ha de divulgarse telemáticamente: «La relación de sistemas algorítmicos o de inteligencia artificial que tengan impacto en los procedimientos administrativos o la prestación de los servicios públicos con la descripción de manera comprensible de su diseño y funcionamiento, el nivel de riesgo que implican y el punto de contacto al que poder dirigirse en cada caso, de acuerdo con los principios de transparencia y explicabilidad» [art. 16.1.l)].

de las actuaciones administrativas automatizadas vinculadas a los servicios, procedimientos y trámites» disponibles; añadiendo a continuación que «[c]ada una se acompañará de la descripción de su diseño y funcionamiento, los mecanismos de rendición de cuentas y transparencia, así como los datos utilizados en su configuración y aprendizaje» [artículo 11.1.i)]. Un avance este sin duda significativo, pero que habría tenido un mayor alcance y significado si se hubiera llevado directamente al texto de la LTAIBG[184].

Pero la que se ha valorado hasta la fecha como la más relevante medida normativa en pro de la transparencia en el sector público es la Ley 15/2022, de 12 de julio, integral para la igualdad de trato y la no discriminación[185]. Pese al específico ámbito sectorial al que se circunscribe la Ley, su artículo 23 (bajo el título «Inteligencia Artificial y mecanismos de toma de decisión automatizados») se expresa en términos genéricos y, por tanto, parece proyectarse con alcance general a la entera actividad administrativa. Ciertamente, la disposición merecería haber encontrado un más adecuado acomodo en la Ley 40/2015, de Régimen Jurídico del Sector Público, con lo que *pari passu* se habría paliado en cierto modo su muy limitada asunción de la transparencia algorítmica[186].

El primer apartado del recién mencionado artículo 23 comienza, además, enlazando directamente con la Carta: «En el marco de la Estrategia Nacional de Inteligencia Artificial, de la Carta de Derechos Digitales y de las iniciativas europeas en torno a la Inteligencia Artificial, las administraciones públicas favorecerán la puesta en marcha de mecanismos para que los algoritmos involucrados en la toma de decisiones que se utilicen en las administraciones públicas tengan en cuenta criterios de minimización de sesgos, transparencia y rendición de cuentas, siempre que sea factible técnicamente. En estos mecanismos se incluirán su diseño y datos de entrenamiento, y abordarán su potencial impacto discriminatorio. Para lograr este fin, se promoverá la realización de evaluaciones de impacto que determinen el posible sesgo discriminatorio.» Y su apartado segundo insiste en la idea de impulsar la transparencia en la toma de decisiones basadas en algoritmos: «Las administraciones públicas, en el marco de sus competencias en el ámbito de los algoritmos involucrados en procesos de toma de decisiones, priorizarán la transparencia en el diseño y la implementación y la capacidad de interpretación de las decisiones adoptadas por los mismos.»[187]

---

[184] En esta línea, Cerrillo i Martínez, A., «Doce propuestas para la mejora de la regulación de la transparencia en España», en: Bermúdez Sánchez, J. (coord.), *La reforma de la regulación de transparencia y buen gobierno en España*, Centro de Estudios Políticos y Constitucionales, Madrid, 2022, p. 104.

[185] Así, Barrio Andrés, M.: «Inteligencia artificial: origen, concepto, mito y realidad», en: *El Cronista del Estado Social y Democrático de Derecho*, núm. 100, septiembre-octubre 2022, p. 20.

[186] En este sentido, Boix Palop, A., *op. cit.*, nota 94, pp. 100-101.

[187] El artículo 23 de la Ley 15/2022 continúa así: «3. Las administraciones públicas y las empresas promoverán el uso de una Inteligencia Artificial ética, confiable y respetuosa con los derechos fundamentales, siguiendo especialmente las recomendaciones de la Unión Europea en este sentido. 4. Se promoverá un sello de calidad de los algoritmos.»

Sin negar que estas previsiones entrañan un paso adelante en la senda de la juridificación de la transparencia en el ámbito de las decisiones públicas apoyadas en algoritmos, salta a la vista también lo modesto de este avance. El artículo 23 de la Ley 15/2022, aun superando obviamente la condición de *mera* suma de recomendaciones propia de la Carta de Derechos Digitales dada su naturaleza de *soft law*, aún no ha abandonado con rotundidad y plenamente el terreno de la fijación de fines orientadores que también caracteriza en parte a la Carta. El artículo 23 de la Ley 15/2022 es norma, sí, pero se encarga más de establecer objetivos tendenciales encauzadores de la acción de la Administración que imponerle concretas obligaciones inmediatamente exigibles («las administraciones públicas favorecerán…» o «priorizarán…»; «se promoverá…»; etc). En cualquier caso, parece llamada a cumplir la nada desdeñable función de servir a su vez como estímulo para que los diferentes niveles de gobierno profundicen en la transparencia algorítmica en sus correspondientes ámbitos competenciales.

Así parece ponerlo de manifiesto el Decreto-ley 2/2023, de 8 de marzo, de medidas urgentes de impulso a la inteligencia artificial en Extremadura. Este Decreto-ley se presenta como el instrumento que pone en marcha los mandatos contenidos en el artículo 23 de la Ley 15/2022 (Exposición de Motivos, I), y en consonancia con ello recoge expresamente en su articulado algunas de sus disposiciones[188]. Pero contiene asimismo otros preceptos que tienen un mayor alcance y de los que se derivan, al menos sobre el papel, una más intensa virtualidad jurídica. Tal es el caso de su artículo 11 («Sistemas de inteligencia artificial en la toma de decisiones»), cuyo apartado primero dice así:

> «La Administración pública autonómica podrá adoptar actos administrativos mediante sistemas de inteligencia artificial en el marco de un procedimiento administrativo, de acuerdo con los Derechos digitales de la ciudadanía en sus relaciones con las Administraciones Públicas, descritos en la Carta de Derechos Digitales

[188] Según establece el artículo 3 del Decreto-ley («Principios generales»): «1. La Administración pública autonómica fomentará el uso de una inteligencia artificial ética, confiable y respetuosa con los derechos fundamentales, siguiendo especialmente las recomendaciones de la Unión Europea, de acuerdo con lo previsto en el artículo 23.4 de la Ley 15/2022, de 12 de julio, integral para la igualdad de trato y la no discriminación. 2. La Administración pública autonómica promoverá la calidad en el uso de inteligencia artificial, favoreciendo, entre otras medidas, el empleo de sistemas de IA que incorporen sellos o certificados de calidad y acrediten su conformidad a las exigencias de seguridad exigidas por la Unión Europea. Además, velará por el cumplimiento de estos estándares de calidad certificada cuando sean obligatorios en sistemas de alto riesgo.» Y, más adelante, el apartado tercero de su artículo 10 dispone lo siguiente: «En todo caso, conforme al apartado 1 del artículo 23 de la Ley 15/2022, de 12 de julio, favorecerán la puesta en marcha de mecanismos para que los algoritmos involucrados en la toma de decisiones que utilice tengan en cuenta criterios de minimización de sesgos, transparencia y rendición de cuentas siempre que sea factible técnicamente. En estos mecanismos se incluirán su diseño y datos de entrenamiento, y abordarán su potencial impacto discriminatorio. Para lograr este fin, se promoverá la realización de evaluaciones de impacto que determinen el posible sesgo discriminatorio.»

> del Gobierno de España y la Declaración Europea sobre los Derechos y Principios Digitales para la Década Digital (2023/C 23/01)».

El primer asunto que quizá haya reclamado la atención del lector es que, tal y como se desprende de su tenor literal, la reconocida capacidad de la Administración pública autonómica de «adoptar actos administrativos mediante sistemas de inteligencia artificial» se condiciona al cumplimiento de los derechos mencionados en el artículo XVIII de la Carta de Derechos Digitales[189]. Por lo tanto, consciente o inadvertidamente, el Gobierno autonómico ha hecho suyos y, por tanto, juridificado y elevado a la condición de verdaderos derechos jurídicamente exigibles lo que en la Carta no eran sino «principios (derechos) programáticos». Transustanciación que no es sino consecuencia del funcionamiento de la técnica de la remisión: el objeto de la remisión (los derechos consagrados en el artículo XVIII de la Carta) pasa a ser parte integrante de la norma de remisión, incorporándose a la misma como cualquier otro asunto regulado directa y explícitamente en ella.

Por otro lado, los amplios términos con que el artículo 11.1 del Decreto-ley habilita a la Administración autonómica para adoptar actos administrativos empleando sistemas de IA permiten interpretar que, a su amparo, podrían llegar a tomarse decisiones totalmente automatizadas. Una lectura del precepto sostenible a la luz de su tenor literal que, sin embargo, plantea de inmediato el interrogante de determinar en qué medida habilitaciones genéricas de esta naturaleza son compatibles con las exigencias establecidas al respecto en el artículo 22.1.b) RGPD. Pero no es este el lugar ni la ocasión para detenerse en el examen de esta cuestión.

Ahora, lo que interesa es destacar que el Decreto-ley 2/2023 tampoco descuida incorporar alguna explícita mención a la imprescindible transparencia. En efecto, el apartado segundo del artículo 11 prosigue a continuación: «Para ello, además de los requisitos previstos en el artículo 41 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, se dará la debida publicidad del mecanismo de decisión, de las prioridades asignadas en el procedimiento de evaluación y de la toma de decisiones, así como de todos los datos que puedan impactar en su contenido». En qué se concreta esa «debida publicidad» a la que alude el precepto es, sin embargo, un asunto que el Decreto-ley prefiere orillar. Comoquiera que sea, una vez convalidado por el Pleno de la Cámara en sesión celebrada el 23 de marzo de 2023, proporciona por las razones referidas un elevado grado de tutela de los derechos digitales que entran en juego cuando se toman decisiones públicas basadas en algoritmos.

Es de prever que medidas favorecedoras de la transparencia algorítmica de esta índole vayan paulatinamente incorporándose a la normativa reguladora de las diver-

[189] Este artículo XVIII aparece precisamente bajo la rúbrica «Derechos digitales de la ciudadanía en sus relaciones con las Administraciones Públicas».

sas Administraciones y/o de los diferentes sectores materiales, e incluso se extienda a la actividad jurisdiccional en cuanto se atribuya también expresamente a jueces y tribunales la capacidad de adoptar decisiones automatizadas, tal y como está ya proyectado[190].

Ahora bien, con independencia de cuál sea la voluntad política del legislador de profundizar en la transparencia, no cabe soslayar que la principal dificultad que debe orillarse a este respecto reside en la circunstancia de que muy frecuentemente las Administraciones recurren al sector privado para la elaboración de los programas informáticos empleados en la toma de decisiones; supuestos en los que, como tuvimos ocasión de comprobar páginas atrás, operan de forma particularmente intensa los límites a la transparencia derivados de la propiedad intelectual [art. 14.1.j) LTAIBG] y del secreto empresarial [art. 14.1.h) LTAIBG].

Nada impide, sin embargo, desde la perspectiva de estos límites, que el legislador decida imponer obligatoriamente a las empresas que deseen contratar con la Administración la accesibilidad al correspondiente programa, que podría llegar incluso a exigir la revelación del entero algoritmo o de su contenido esencial, el código fuente. Pues, por más que en esos límites se proyecten derechos e intereses constitucionalmente protegidos (más concretamente, los derechos fundamentales a la propiedad privada y a la libertad de empresa), parece evidente que el consentimiento excluye de raíz todo atisbo de menoscabo de los mismos. No es, pues, de naturaleza jurídica la principal dificultad que ha de sortearse para avanzar en la transparencia algorítmica en estos supuestos, sino de carácter puramente material: es más que probable que las empresas tecnológicas especializadas se resistan a contratar con la Administración, bajo la ineludible condición de revelar conocimientos técnicos muy sensibles, si no reciben una adecuada contraprestación que compense esa pérdida.

La certidumbre de que el disfrute de los derechos entraña necesariamente un coste para las arcas públicas[191] adquiere, por tanto, un matiz singular cuando está en juego el derecho de acceso a la información algorítmica.

---

[190] Cuando estas líneas se ultiman, el Proyecto de Ley de Medidas de Eficiencia Digital del Servicio Público de Justicia se encuentra aún en tramitación en el Congreso de los Diputados; proyecto que contempla tanto «actuaciones automatizadas» (que no necesitan intervención humana en cada caso singular) como «actuaciones asistidas» (*Boletín Oficial de las Cortes Generales. Congreso de los Diputados*, XIV Legislatura, Serie A: Proyectos de Ley, de 12 de septiembre de 2022, núm. 116-1). Para más detalles sobre estas decisiones judiciales basadas en algoritmos, véase Medina Guerrero, M., «Cláusulas de apertura y ejercicio de la función jurisdiccional en el Reglamento General de Protección de Datos», en: Paulner Chulvi, C.; García Mahamut, R.; Tomás Mallén, b. s. (eds), *La implementación del Reglamento General de Protección de Datos en España y el impacto de sus cláusulas abiertas*, Tirant lo Blanch, Valencia, 2023, pp. 201-226 (en prensa).

[191] Holmes, S.; Sunstein, C. R., *The Cost of Rights. Why Liberty Depends on Taxes*, W. W. Norton & Company, New York-London, 1999.

V. BIBLIOGRAFÍA

Aparicio Vaquero, J.P., «Comentario al Título VII del Libro I ("Programas de ordenador")», en Bercovitz Rodríguez-Cano, R. (Coord.), *Comentarios a la Ley de Propiedad Intelectual*, 4ª edición, Tecnos, Madrid, 2017, pp. 1355-1529.

Balaguer Callejón, F., *La constitución del algoritmo*, Fundación Manuel Giménez Abad de Estudios Parlamentarios y del Estado Autonómico, Zaragoza, 2022.

Barrio Andrés, M., «Inteligencia artificial: origen, concepto, mito y realidad», en: *El Cronista del Estado Social y Democrático de Derecho*, núm. 100, septiembre-octubre 2022, pp.

Bercovitz Rodríguez-Cano, R., «Comentario al artículo 13», en Bercovitz Rodríguez-Cano, R. (Coord.), *Comentarios a la Ley de Propiedad Intelectual*, 4ª edición, Tecnos, Madrid, 2017, pp. 223-226.

Bloch-Wehba, H., «Access to Algorithms», en: *Fordham Law Review* Vol. 88, 2020, pp. 1265-1314.

Boix Palop, A., «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* Vol.1, 2020, p. 224-269.

——«Transparencia en la utilización de inteligencia artificial por parte de la Administración», en: *El Cronista del Estado Social y Democrático de Derecho*, núm. 100, septiembre-octubre 2022, pp. 90-105

Brauneis, R.; Goodman, E. P., «Algorithmic Transparency for the Smart City», en: *The Yale Journal of Law & Technology*, Vol. 20, 103, 2018, pp. 103-176.

Brkan, M., «Do Algorithms Rule the World? Algorithmic Decision-Making in the Framework of the GDPR and Beyond», en: *International Journal of Law and Information Technology*, 11 January 2019, pp. 1-29 (he utilizado la versión disponible en https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3124901)

Brkan, M.; Bonnet, G., «Legal and Technical Feasibility of the GDPR's Quest for Explanation of Algorithmic Decisions: of Black Boxes, White Boxes and Fata Morganas», en: *European Journal of Risk Regulation*, 11 (2019), pp. 18—50 (doi:10.1017/err.2020.10)

Buchner, B., «Comentario al artículo 22», en: Kühling, J.; Buchner, B. (Hersg.), *Datenschutz-Grundverordnung Bundesdatenschutzgesetz. Kommentar*, 2. Auflage, C. H. Beck, München, 2018, pp. 508-520.

Busuioc, M., «Accountable Artificial Intelligence: Holding Algorithms to Account», en: *Public Administration Review*, Vol. 00, Iss. 00, pp. 1-12 (DOI: 10.1111/puar.13293).

Capilla Roncero, F. *et al.* (dirs.), *Derecho digital: Retos y cuestiones actuales*, Thomson Reuters Aranzadi, 2018.

Celeste, E., *Digital Constitutionalism. The Role of Internet Bill of Rights*, Routledge, Abingdon, 2023.

Cerrillo i Martínez, A., «Doce propuestas para la mejora de la regulación de la transparencia en España», en: Bermúdez Sánchez, J. (coord.), *La reforma de la regulación de transparencia y buen gobierno en España*, Centro de Estudios Políticos y Constitucionales, Madrid, 2022, pp. 91-125.

——«Actividad administrativa automatizada y utilización de algoritmos», en Castillo Blanco, F. A. *et al.* (dirs.), *Las políticas de buen gobierno en Andalucía (I): Digitalización y transparencia*, Instituto Andaluz de Administración Pública, Sevilla, 2022, pp. 259-287.

——«La transparencia de los algoritmos que utilizan las administraciones públicas», en: Camp Batalla, R. (ed.), *Anuario de Transparencia Local 3/2020*, Fundación Democracia y Gobierno Local, Madrid, 2021, pp. 41-78.

——«El impacto de la inteligencia artificial en el Derecho Administrativo. ¿Nuevos conceptos para nuevas realidades técnicas?», en: *Revista General de Derecho Administrativo* 50 (2019).

Chiacchio, M. G., «L'utilizzo dell'algoritmo nelle procedure valutative della PA (Commento a Consiglio di Stato, Sez. VI, Sent. 8 aprile 2019, N. 2270)», en: *European Journal of Privacy Law & Technologies* 2019/2, pp. 137-143

Citron, D. K., «Technological Due Process», en: *Washington University Law Review,* Vol. 85 Issue 6, 2008, pp. 1249-1313.

Cotino Hueso, L., «SyRI, ¿a quién sanciono?» Garantías frente al uso de inteligencia artificial y decisiones automatizadas en el sector público y la sentencia holandesa de febrero de 2020», en: *La Ley Privacidad, Wolters Kluwer nº 4,* mayo 2020.

——«Qué concreta transparencia e información de algoritmos e inteligencia artificial es la debida», en: *Revista Española de la Transparencia*, núm. 16, primer semestre de 2023, pp. 17-63.

Cotino, L.; Boix, P. (coordinadores), *Los límites al derecho de acceso a la información pública*, Tirant lo Blanch, Valencia, 2021.

De Gregorio, G., *Digital Constitutionalism in Europe*, Cambridge University Press, Cambridge, 2022.

De la Cueva, J., «Código fuente, algoritmos y fuentes del Derecho», en: *El notario del siglo XXI: revista del Colegio Notarial de Madrid,* núm. 77, 2018 [http://www.elnotario.es/index.php/hemeroteca/revista-77/opinion/opinion/8382-codigo-fuente-algoritmos-y-fuentes-del-derecho; fecha de la última consulta: 16 de diciembre de 2022].

Diakopoulos, N., «Algorithmic Accountability Reporting: On the Investigation of Black Boxes», Columbia Journalism School, Tow Center for Digital Journalism, 2014 (https://doi.org/10.7916/D8ZK5TW2).

——«Algorithmic Accountability. Journalistic investigation of computational power structures», en: *Digital Journalism*, 2014 (htpps://dx.doi.org/10.1080/21670811.2014.976411).

——«Accountability in Algorithmic Decision Making», *Communications of the ACM*, Vol. 59 Nº 2, febrero 2016, pp. 56-62.

Edwards, L.; Veale, M., «Slave to the Algorithm? Why a `Right to Explanation´ is probably not the Remedy you are looking for», en: *Duke Law & Technology Review*, Vol. 16 Nº 1, 2017, pp. 18-84.

——«Enslaving the Algorithm: From a «Right to an Explanation» to a «Right to Better Decisions»?», en: *IEEE Security & Privacy* (2018) 16(3), pp. 46-54 (doi:10.1109/MSP.2018.2701152).

Fernández Masía, E., *La protección de los programas de ordenador en España*, Tirant lo Blanch, Valencia, 1996.

——«Comentario al artículo 96», en: Palau Ramírez, F.; Palao Moreno, G. (dir.), *Comentarios a la Ley de Propiedad Intelectual*, Tirant lo Blanch, Valencia, 2017, pp. 1199-1209.

Fernández Ramos, S., «Derecho de acceso: Dos novedades autonómicas en 2022 y una tercera que no pudo ser», en: *Revista Española de la Transparencia*, núm. 15, julio-diciembre 2022, pp. 35-62.

Fernández Ramos, S.; Pérez Monguió, J. M., *El derecho al acceso a la información pública en España*, Thomson Reuters Aranzadi. Cizur Menor, 2017.

Franck, L., «Comentario al artículo 15», en: Gola, P.; Heckmann, D. (Hrsg.), *Datenschutz-Grundverordnung VO (EU) 2016/679. Bundesdatenschutzgesetz. Kommentar*, 3ª edición, C. H. Beck, München, 2022, pp. 475-503.

Giurdanella, C.; Guarnaccia, E., *Elementi di diritto amministrativo elettronico*, Halley, Matelica, 2005.

Gola, P.; Heckmann, D. (Hrsg.), *Datenschutz-Grundverordnung VO (EU) 2016/679. Bundesdatenschutzgesetz. Kommentar*, 3ª edición, C. H. Beck, München, 2022.

Guichot, E.; Barrero Rodríguez, C., *El derecho de acceso a la información pública*, Tirant lo Blanch, Valencia, 2020 .

Gutiérrez David, M. E., «Administraciones inteligentes y acceso al código fuente y los algoritmos públicos. Conjurando riesgos de cajas negras decisionales», en: *Derecom*, 30, 2021, pp. 143-228 (https://www.derecom.com/derecom/).

——«El derecho de acceso a la información pública contractual y sus límites», en: Cotino, L.; Boix, P. (coordinadores), *Los límites al derecho de acceso a la información pública*, Tirant lo Blanch, Valencia, 2021, pp. 243-293.

Holmes, S.; Sunstein, C. R., *The Cost of Rights. Why Liberty Depends on Taxes*, W. W. Norton & Company, New York-London, 1999.

Huergo Lora, A., «Una aproximación a los algoritmos desde el Derecho Administrativo», en: Huergo Lora, A. (dir.), *La regulación de los algoritmos*, Thomson Reuters Arazandi, Cizur Menor, 2020, pp. 23-87.

——«Administraciones Públicas e inteligencia artificial: ¿más o menos discrecionalidad?», en: *El Cronista del Estado Social y Democrático de Derecho*, octubre- noviem-

bre 2021 [he utilizado la versión de *La Administración al día*, Estudios y Comentarios, INAP, 25/01/2022].

——«El derecho de transparencia en el acceso a los códigos fuente», en: *Anuario de Transparencia Local 5/2022*, Fundación Democracia y Gobierno Local, Madrid, 2023, pp. 35-66.

Iaselle, M., «Diritti di accesso all'algoritmo, TAR Lazio apre nuovi scenari», *Altalex* 17 de mayo de 2017 (https://www.altalex.com/documents/news/2017/05/17/diritto-di-accesso-algoritmo).

Ingold, A., «Comentario al artículo 14», en SYDOW, G. (Hrsg), *Europäische Datenschutzgrundverordnung. Handkommentar*, 2. Auflage, Nomos, 2018, pp. 536-545.

Jiménez-Castellanos Ballesteros, I., «Decisiones automatizadas y transparencia administrativa: nuevos retos para los derechos fundamentales», en: *Revista Española de la Transparencia*, núm. 16, enero-junio 2023, pp. 191-215.

Kaminski, M. E., «The Right to Explanation, Explained», en: *University of Colorado Law Legal Studies Research Paper* No. 18-24, *Berkeley Technology Law Journal* Vol. 34, No.1, 2019, pp. 1-25 (disponible en https://ssrn.com/abstract=3196985, así como en http://dx.doi.org/10.2139/ssrn.319695)

Kloepfer, M., *Informationsfreiheitsgesetz und Schutz von Betriebs- und Geschäftsgeheimnissen - Betriebs- und Geschäftsgeheimnisse in verschiedenen Rechtsgebieten und verschiedenen Kontexten,* Rechtsgutachten im Auftrag des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, Junio 2011.

Kroll, J. A. *et al.*, «Accountable Algorithms», en: *University of Pennsylvania Law Review*, Vol. 165, 2017 pp. 633-705.

Kühling, J.; Martini; M. *et al.*, *Die Datenschutz-Grundverordnung und das nationale Recht. Erste Überlegungen zum innerstaatlichen Regelungsbedarf*, Verlagshaus Monsenstein und Vannerdat, Münster, 2016.

Laat, P. B. de, «Algorithmic Decision-Making Based on Machine Learning from Big Data: Can Transparency Restore Accountability?», en: *Philos. Technol* 2017, pp. 1-18 [https://doi.org/10.1007/s13347-017-0293-z].

Lessig, L., *Code and other laws of cyberspace*, Basic Books, New York, 1999.

Maggiolino, M., «EU Trade Secrets Law and Algorithmic Transparency» (March 31, 2019), en: *Bocconi Legal Studies Research Paper* No. 3363178. [Disponible en SSRN: https://ssrn.com/abstract=3363178; o bien en htpps://dx.doi.org/10.2139/ssrn.3363178; última consulta: 16/02/2023].

Malgieri, G., «*Trade Secrets v Personal Data*: a possible solution for balancing rights», en: *International Data Privacy Law*, Volume 6, Issue 2, 2016, pp. 102-116.

Mancosu, G., «Les algorithmes publics déterministes au prisme du cas italien de la mobilité des enseignants», en: *Rivista italiana di informática e diritto*, Fascicolo 1-2019, pp. 75-85 (DOI: 10.32091/RIID0005).

Martínez Espín, P., «Comentario al artículo 14», en Bercovitz Rodríguez-Cano, R. (Coord.), *Comentarios a la Ley de Propiedad Intelectual*, 4ª edición, Tecnos, Madrid, 2017, pp. 227-256.

Martini, M.; Nink, D., «Wenn Maschinen entscheiden … — vollautomatisierte verwaltungsverfahren und der Persönlichkeitsschutz», en: *Neue Zeitschrift für Verwaltungsrecht-Extra*, 10, 2017, pp. 1-14.

Mazur, J., «Right to Access Information as a Collective-Based Approach to the GDPR's Right to Explanation in European Law», en: *Erasmus Law Review* december 2018 | No. 3, pp. 178-189 - doi: 10.5553/ELR.000116 [disponible en: https://ssrn.com/abstract=3356770].

Mecklenburg, W.; Pöppelmann, B. H., *Informationsfreiheitsgesetz*, Deutscher Journalisten-Verband *et al.*, Berlin, 2007.

Medina Guerrero, M., «El derecho a conocer los algoritmos utilizados en la toma de decisiones. Aproximación desde la perspectiva del derecho fundamental a la protección de datos personales», en: *Teoría y Realidad Constitucional*, núm. 49, 2022, pp. 141-171.

——*La vinculación negativa del legislador a los derechos fundamentales*, McGraw Hill, Madrid, 1996.

Menell, P. S., «Tailoring a Public Policy Exception to Trade Secret Protection», en: *California Law Review,* Vol. 105, Nº 1 (February 2018), pp. 1-63.

Messia de la Cerda Caballero, J. A., «Comentario al artículo 14 i) y j)», en: Troncoso Reigada, A. (dir.), *Comentario a la Ley de transparencia, acceso a la información pública y buen gobierno*, Civitas/Thomson Reuters, Madrid, 2017, pp. 935-958.

Noto la Diega, G., «Against the Dehumanisation of Decision-Making — Algorithmic Decisions at the Crossroads of Intellectual Property, Data Protection, and Freedom of Information», en: *Journal of Intellectual Property, Information Technology and E-Commerce Law (JIPITEC)*, 9, 2018, pp. 3-34.

Olivares Olivares, B., «Transparencia y aplicaciones informáticas en la Administración tributaria», en: *Crónica Tributaria*, núm. 174, 2000, pp. 89-111.

Oswald, M. *et al.*, *The UK Algorithmic Transparency Standard: A Qualitative Analysis of Police Perspectives*, 7 julio 2022 (https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4155549)

Palau Ramírez, F.; Palao Moreno, G. (dir.), *Comentarios a la Ley de Propiedad Intelectual*, Tirant lo Blanch, Valencia, 2017.

Palma Ortigosa, A., «Decisiones automatizadas en el RGPD. El uso de algoritmos en el contexto de protección de datos», en: *Revista General de Derecho Administrativo*, 50, 2019.

Plaza Penadés, J., «Comentario al artículo 14», en: Rodríguez Tapia, J. M. (Dir.), *Comentarios a la Ley de Propiedad Intelectual*, 2ª edición, Civitas/Thomson Reuters, Cizur Menor, 2009, pp. 150-169.

Ponce Solé, J. «Inteligencia artificial, Derecho administrativo y reserva de humanidad: algoritmos y procedimiento debido tecnológico», en: *Revista General de Derecho Administrativo,* 50, 2019.

Pooley, J., «Trade secrets: The other IP right», en: *WIPO Magazine*, 3/2013.

Presno Linera, M. A., *Derechos fundamentales e inteligencia artificial*, Marcial Pons, Madrid, 2022.

Rallo Lombarte, A., «Una nueva generación de derechos digitales», en: *Revista de Estudios Políticos*, núm. 187, 2020, pp. 101-135.

Rivero Ortega, R., «Algoritmos, inteligencia artificial y policía predictiva del Estado vigilante», en: *Revista General de Derecho Administrativo*, núm. 62, 2023.

Rodríguez Álvarez, J. L., «Transparencia y protección de datos personales: criterios legales de conciliación», en: Canals Ametller (ed.), *Datos. Protección, Transparencia y Buena Regulación*, Documenta Universitaria, Girona, pp. 53-85.

Rodríguez Tapia, J. M., «Comentario al artículo 97», en: Rodríguez Tapia, J. M. (Dir.), *Comentarios a la Ley de Propiedad Intelectual*, 2ª edición, Civitas/Thomson Reuters, Cizur Menor, 2009, pp. 591-593.

Rum, A. L., «Il provvedimento amministrativo adottato mediante algoritmo: il ruolo dell'intelligenza artificiale nel proceso decisionale della P.A.», en: *Il Diritto Amministrativo. Rivista Giuridica*, Año XV, n. 02, Febbraio 2023.

Scheja, K., «Schutz von Algorithmen in Big Data Anwendungen», en: *Computer und Recht*, 8/2018, pp. 485-492.

Schneider, J., «Urheberrechtsschutz für Software», en: Schneider, J. (ed.), *Handbuch EDV-Recht: IT-Recht mit IT-Vertragsrecht, Datenschutz, Rechtsschutz und E-Business*, Otto Schmidt KG, 2017, pp. 1023-1130.

Schulte, U.; Timm, M., «Entscheidungsanmerkung zu dem Urteil des Bundesgerichtshofes vom 28.1.2014 — VI ZR 156/13. Umfang des Auskunftsanspruches gegen die Schufa-Scorewerte», en: *Neue Juristische Wochenschrift*, Heft 17/2014, pp. 1235-1239.

Selbst, A. D.; Powles, J., «Meaningful information and the right to explanation», en: *International Data Privacy Law*, 2017, Vol. 7, No. 4, pp. 233-242. [doi:10.1093/idpl/ipx022].

Soares Fariño, D., «The Portuguese Charter of Human Rights in the Digital Age: a legal appraisal», en: *Revista Española de la Transparencia*, núm. 13, 2021, pp. 85-101.

Soriano Arnanz, A. «Decisiones automatizadas: problemas y soluciones jurídicas. Más allá de la protección de datos», *Revista de Derecho Público: Teoría y Método*, Vol. 3, 2021, pp. 85-127.

Soto Bernabeu, L., «La importancia de la transparencia algorítmica en el uso de la inteligencia artificial or la Administración tributaria», en: *Crónica Tributaria*, núm. 179, 2021, pp. 93-129.

Spielkamp, M., «AlgorithmWatch: What Role Can a Watchdog Organization Play in Ensuring Algorithmic Accountability?», en: Cerquitelli, T.; Quercia, D.; Pasquale, F. (Eds.), *Transparent Data Mining for Big and Small Data*, Springer, 2017, pp. 207-215.

Valero Torrijos, J., «Las garantías jurídicas de la inteligencia artificial en la actividad administrativa desde la perspectiva de la buena administración», en: *Revista Catalana de Dret Públic*, núm. 58, 2019.

Vendrell Cervantes, C., «Comentario al artículo 14», en: Palau Ramírez, F./Palao Moreno, G. (dir.), *Comentarios a la Ley de Propiedad Intelectual*, Tirant lo Blanch, Valencia, 2017, pp. 264-295.

Vestri, G., «La inteligencia artificial ante el desafío de la transparencia algorítmica. Una aproximación desde la perspectiva jurídico-administrativa», en: *Revista Aragonesa de Administración Pública*, núm. 56, 2021, pp. 368-398.

Vilasau Solana, M., «El consentimiento general y de menores», en: Rallo Lombarte, A. (dir.), *Tratado de protección de datos*, Tirant lo Blanch, Valencia, 2019, pp. 197-250.

Villalba Cano, L., «La representación de los interesados (Comentario al artículo 80 RGPD)», en: Troncoso Reigada, A. (dir.), *Comentario al Reglamento General de Protección de Datos y a la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales*, Tomo II, Civitas/Thomson Reuters, Cizur Menor, 2021, pp. 3019-3040.

Viola, L., «L'intelligenza artificiale nel procedimento e nel processo amministrativo: lo stato dell'arte», *federalismi.it*. *Rivista di Diritto Pubblico italiano, comparato, europeo*, núm. 21, 2018, pp. 2-44.

Wachter, S.; Mittelstadt, B.; Floridi, L.,«Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation», en: *International Data Privacy Law,* 2017, Vol. 7, No. 2, pp. 76-99 [doi:10.1093/idpl/ipx005].

Wegener, B. W., *Zum Verhältnis des Rechts auf freien Zugang zu Umweltinformationen zum Urheberrecht -Gutachten-*, Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit, mayo 2010.

Weichert, T., «Die verfassungsrechtliche Dimension der Algorithmenkontrolle», *Datenschutz Nachrichten* 3/2018, pp. 132-138.

Zarsky, T. Z., «Transparent Predictions», en: *University of Illinois Law Review*, Vol. 2013, No 4, 2013, pp. 1503-1570.

CAPÍTULO 6

SOBRE EL DERECHO A CONOCER QUIÉN HA ACCEDIDO A MIS DATOS

Iñaki González-Pol González

Letrado del Defensor del Pueblo Andaluz
Delegado de Protección de Datos del Parlamento de Andalucía, del Defensor del Pueblo Andaluz y de la Junta Electoral de Andalucía

SUMARIO

I. INTRODUCCIÓN

A pesar de la extraordinaria diligencia con la que actúan las Administraciones Públicas en la gestión de sus distintas bases de datos, en ocasiones algunos empleados de las mismas hacen uso ilegítimo de los permisos que tienen atribuidos por razón de su cargo para realizar consultas que van orientadas a satisfacer su propia curiosidad o a atender finalidades particulares espurias.

Ejemplo de ello son los casos que han trascendido a los medios de comunicación, protagonizados por profesionales sanitarios que han accedido a la historia clínica de compañeros, familiares o pacientes con quienes no tenían relación asistencial; por agentes de las Fuerzas y Cuerpos de Seguridad del Estado que han consultado bases de datos policiales para fines estrictamente personales e ilícitos; o por autoridades y funcionarios que, valiéndose de su condición, han logrado obtener información personal de políticos, representantes de trabajadores, de compañeros o incluso de vecinos llegando incluso a hacerla pública a través de distintos canales de difusión.

Se trata de conductas que, sin duda, pueden constituir una clara infracción del ordenamiento jurídico hasta el punto de llegar a tener relevancia penal. En este senti-

do, el artículo 197.2 del Código Penal sanciona a quien, sin estar autorizado, acceda por cualquier medio a datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado, y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero.

Por su parte, el artículo 198 del citado Código dispone que «La autoridad o funcionario público que, fuera de los casos permitidos por la Ley, sin mediar causa legal por delito, y prevaliéndose de su cargo, realizare cualquiera de las conductas descritas en el artículo anterior, será castigado con las penas respectivamente previstas en el mismo, en su mitad superior y, además, con la de inhabilitación absoluta por tiempo de seis a doce años».

Pero más allá del análisis relativo a la antijuridicidad de la conducta o a la naturaleza de la infracción, el objeto del presente estudio se centra en dirimir si la persona titular de los datos, esto es, la persona interesada, tiene derecho a conocer quién ha accedido a los mismos.

Se pretende pues analizar los mecanismos con los que cuenten las personas cuyos datos obren en poder de las Administraciones Públicas para conocer quién ha accedido a los mismos y con qué propósito; ello, como garantía para controlar el adecuado tratamiento de la información por parte del responsable del tratamiento.

De este modo, la primera cuestión que debe ser objeto de estudio concierne a la obligatoriedad o no de tenencia, por parte de las Administraciones, de un registro en el que consten los distintos accesos realizados a las bases de datos.

Resuelta esta cuestión, se procederá a continuación a analizar si el ordenamiento vigente reconoce a las personas interesadas un derecho de acceso a dicho registro, en particular, a los datos identificativos de las personas que, en su caso, hayan consultado sus datos.

Tal cuestión se abordará, en un primer término, atendiendo a la normativa reguladora del derecho fundamental a la protección de datos, prosiguiendo el estudio con el análisis de la normativa reguladora del derecho de acceso a la información pública.

Finalmente, se dispondrá un apartado con las principales conclusiones extraídas a través del presente trabajo.

II. SOBRE LA OBLIGACIÓN DE DISPONER DE LA INFORMACIÓN RELATIVA A LOS ACCESOS REALIZADOS A LOS SISTEMAS DE INFORMACIÓN

El apartado primero del artículo 4 del Reglamento General de Protección de Datos[1] (en adelante, RGPD) define como «datos personales» toda información sobre una

[1] 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.

persona física identificada o identificable («el interesado»), señalando que se considerará persona física identificable «toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona».

De este modo, y salvo que haya mediado un proceso de anonimización, los datos de ciudadanos y ciudadanas contenidos en las distintas bases de datos de las Administraciones Públicas merecen la consideración de datos personales y su tratamiento por parte de aquellas se encuentra sometido a lo preceptuado en el RGPD y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD), en atención al ámbito de aplicación previsto para sendas normas en sus respectivos artículos 2.

Subrayada esta premisa, resulta procedente acudir a la normativa reguladora del derecho fundamental a la protección de datos para analizar si ésta requiere la tenencia, por parte de las Administraciones Públicas, de un registro de los accesos que se produzcan a sus bases de datos.

A este respecto, ya por el año 1999, el Real Decreto 994/1999, de 11 de junio, por el que se aprobaba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal exigía la tenencia, por parte de los «responsables de ficheros», de un registro de accesos.

Esta medida de seguridad se incluía entre las de nivel alto que resultaban exigibles para ficheros automatizados que contuviesen datos de ideología, religión, creencias, origen racial, salud o vida sexual así como datos obtenidos para fines policiales sin consentimiento de las personas afectadas. En concreto, el artículo 24 de la norma reglamentaria establecía lo siguiente:

> «Artículo 24. Registro de accesos.
>
> 1. De cada acceso se guardarán, como mínimo, la identificación del usuario, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado.
>
> 2. En el caso de que el acceso haya sido autorizado, será preciso guardar la información que permita identificar el registro accedido.
>
> 3. Los mecanismos que permiten el registro de los datos detallados en los párrafos anteriores estarán bajo el control directo del responsable de seguridad competente sin que se deba permitir, en ningún caso, la desactivación de los mismos.
>
> 4. El período mínimo de conservación de los datos registrados será de dos años.
>
> 5. El responsable de seguridad competente se encargará de revisar periódicamente la información de control registrada y elaborará un informe de las revisiones realizadas y los problemas detectados al menos una vez al mes».

Inmediatamente después, el legislador orgánico aprobó la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD), que presentaba entre sus principales novedades la extensión del alcance regulatorio a los tratamientos no automatizados de datos.

Dicha Ley Orgánica fue objeto de desarrollo a través del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, cuyo Título VIII estaba dedicado a la regulación de las medidas de seguridad.

Con respecto a éstas, se establecían igualmente tres niveles de seguridad: básico, medio y alto, con medidas de seguridad que se iban sumando al transitar de un nivel a otro.

En este sentido, para ficheros o tratamientos de nivel medio se requería la implantación de las medidas de seguridad previstas para el nivel básico y, además, de aquellas otras concebidas específicamente para el nivel medio.

Asimismo, en el caso de ficheros o tratamientos de nivel alto, éstos debían disponer de las medidas de seguridad previstas para el nivel básico, para las del medio y, junto a ellas, las específicas del nivel alto.

En cuanto a la concreción de las medidas de seguridad, la norma reglamentaria daba respuesta a la ampliación previamente aludida del alcance regulatorio de la Ley Orgánica, distinguiendo así entre aquellas medidas que debían disponerse en supuestos de tratamientos automatizados y aquellas otras que se concebían en particular para tratamientos no automatizados.

Pues bien, por lo que respecta al registro de accesos, esta medida de seguridad se insertaba entre las de nivel alto en supuestos de tratamientos automatizados de datos. En concreto, el art. 103 del RD 1720/2007 establecía lo siguiente:

> «Artículo 103. Registro de accesos.
>
> 1. De cada intento de acceso se guardarán, como mínimo, la identificación del usuario, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado.
>
> 2. En el caso de que el acceso haya sido autorizado, será preciso guardar la información que permita identificar el registro accedido.
>
> 3. Los mecanismos que permiten el registro de accesos estarán bajo el control directo del responsable de seguridad competente sin que deban permitir la desactivación ni la manipulación de los mismos.
>
> 4. El período mínimo de conservación de los datos registrados será de dos años.
>
> 5. El responsable de seguridad se encargará de revisar al menos una vez al mes la información de control registrada y elaborará un informe de las revisiones realizadas y los problemas detectados.
>
> 6. No será necesario el registro de accesos definido en este artículo en caso de que concurran las siguientes circunstancias:

a) Que el responsable del fichero o del tratamiento sea una persona física.
b) Que el responsable del fichero o del tratamiento garantice que únicamente él tiene acceso y trata los datos personales.

La concurrencia de las dos circunstancias a las que se refiere el apartado anterior deberá hacerse constar expresamente en el documento de seguridad».

De este modo, esta medida de seguridad resultaba obligatoria en ficheros o tratamientos de datos de nivel alto, a saber:

a) Los referidos a datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual.
b) Los que contengan o se refieran a datos recabados para fines policiales sin consentimiento de las personas afectadas.
c) Aquéllos que contengan datos derivados de actos de violencia de género.

Para el caso de los tratamientos no automatizados de datos, entre las medidas de seguridad de nivel alto se insertaban las contenidas en los apartados segundo y tercero del artículo 113 de la norma reglamentaria.

En este sentido, se requería el establecimiento de mecanismos que permitiesen identificar los accesos realizados en el caso de documentos que pudieran ser utilizados por múltiples usuarios, señalando el apartado tercero del precepto que el acceso de personas no incluidas en el supuesto anterior debía quedar adecuadamente registrado de acuerdo con el procedimiento establecido al efecto en el documento de seguridad.

Este esquema regulatorio de las medidas de seguridad planteado por el legislador orgánico del año 1999, desarrollado a través del mencionado Real Decreto 1720/2007, se ha visto sustancialmente modificado con ocasión de la entrada en vigor y aplicación efectiva del RGPD.

En este sentido, el legislador europeo establece, en el artículo 32 del RGPD, la obligación, para el responsable del tratamiento, de concretar e implementar medidas de seguridad técnicas y organizativas apropiadas para garantizar el nivel de seguridad adecuado al riesgo en función del estado de la técnica, los costes de aplicación y la naturaleza, alcance, contexto y fines del tratamiento, así como en función de la probabilidad en la que pueda materializarse el riesgo y la gravedad de la afección a los derechos y libertades de las personas afectadas.

Es decir, a diferencia de lo que ocurría antes, donde las medidas de seguridad que habían de ser implementadas eran detalladas en la norma, ahora tales medidas de seguridad deben ser concretadas por los responsables de tratamiento en atención a las variables antedichas.

Se les exige pues llevar a cabo un proceso previo de evaluación de los riesgos que sobre los derechos y libertades de las personas afectadas son inherentes al tratamiento.

A partir de ahí, debe procederse a la concreción e implementación de las medidas técnicas y organizativas necesarias para mitigar tales riesgos, previamente identificados.

Siendo esto así, debe tenerse presente no obstante lo dispuesto en la Disposición adicional primera de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

En este sentido, dicha Disposición adicional prevé lo siguiente:

> «Disposición adicional primera. Medidas de seguridad en el ámbito del sector público.
>
> 1. El Esquema Nacional de Seguridad incluirá las medidas que deban implantarse en caso de tratamiento de datos personales para evitar su pérdida, alteración o acceso no autorizado, adaptando los criterios de determinación del riesgo en el tratamiento de los datos a lo establecido en el artículo 32 del Reglamento (UE) 2016/679.
>
> 2. Los responsables enumerados en el artículo 77.1 de esta ley orgánica deberán aplicar a los tratamientos de datos personales las medidas de seguridad que correspondan de las previstas en el Esquema Nacional de Seguridad, así como impulsar un grado de implementación de medidas equivalentes en las empresas o fundaciones vinculadas a los mismos sujetas al Derecho privado.
>
> En los casos en los que un tercero preste un servicio en régimen de concesión, encomienda de gestión o contrato, las medidas de seguridad se corresponderán con las de la Administración pública de origen y se ajustarán al Esquema Nacional de Seguridad».

Por consiguiente, y conforme a esta previsión, las Administraciones Públicas deberán acudir al Esquema Nacional de Seguridad (en adelante, también ENS) para determinar las medidas que deban implantarse en caso de tratamiento de datos personales con el propósito de evitar su pérdida, alteración o acceso no autorizado, adaptando los criterios de determinación del riesgo en el tratamiento de los datos a lo establecido en el RGPD.

Siendo esto así, procede en este punto analizar si dicho Esquema Nacional de Seguridad prevé la necesidad de tenencia, por parte de las Administraciones Públicas, de un registro de los accesos que se produzcan a sus respectivas bases de datos.

A este respecto procede partir de que el artículo 12 del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, integrado en el Capítulo III dedicado a «Política de seguridad y requisitos mínimos de seguridad», previene en sus apartados primero y segundo la obligatoriedad, para las Administraciones Públicas, de contar con una política de seguridad formalmente aprobada por el órgano competente, añadiendo el apartado sexto del mencionado artículo que dicha política de seguridad se habrá de establecer de acuerdo con los principios básicos señalados en el capítulo II y que se desarrollará aplicando, entre otros, los siguientes requisitos mínimos:

«e) Autorización y control de los accesos.
h) Mínimo privilegio.
l) Registro de la actividad y detección de código dañino».

Por su parte, el apartado 7 de dicho artículo 12 señala que estos requisitos mínimos se exigirán «en proporción a los riesgos identificados en cada sistema, de conformidad con lo dispuesto en el artículo 28, alguno de los cuales podrá obviarse en sistemas sin riesgos significativos».

Acudiendo a continuación al mencionado artículo 28, nos encontramos con que su apartado primero prevé que

> «Para dar cumplimiento a los requisitos mínimos establecidos en el presente real decreto, las entidades comprendidas en su ámbito de aplicación adoptarán las medidas y refuerzos de seguridad correspondientes indicados en el anexo II, teniendo en cuenta:
> a) Los activos que constituyen los sistemas de información concernidos.
> b) La categoría del sistema, según lo previsto en el artículo 40 y en el anexo I.
> c) Las decisiones que se adopten para gestionar los riesgos identificados».

Por lo que hace al citado Anexo II, éste contempla en el marco operacional de explotación, para la dimensión relativa a la trazabilidad, la medida de seguridad consistente en la disposición de un Registro de actividad, previéndose su aplicación en sistemas de categoría básica, media y alta.

De este modo, se exige:

— La generación de un registro de auditoría, que incluirá, al menos, el identificador del usuario o entidad asociado al evento, fecha y hora, sobre qué información se realiza el evento, tipo de evento y el resultado del evento (fallo o éxito), según la política de seguridad y los procedimientos asociados a la misma.
— La activación de los registros de actividad en los servidores.

Todo ello, conforme a lo dispuesto en artículo 24 del ENS, que establece (la cursiva es nuestra):

> «Artículo 24. Registro de actividad y detección de código dañino.
> 1. Con el propósito de satisfacer el objeto de este real decreto, con plenas garantías del derecho al honor, a la intimidad personal y familiar y a la propia imagen de los afectados, y de acuerdo con la normativa sobre protección de datos personales, de función pública o laboral, y demás disposiciones que resulten de aplicación, *se registrarán las actividades de los usuarios, reteniendo la información*

estrictamente necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa.

2. Al objeto de preservar la seguridad de los sistemas de información, garantizando la rigurosa observancia de los principios de actuación de las Administraciones públicas, y de conformidad con lo dispuesto en el Reglamento General de Protección de Datos y el respeto a los principios de limitación de la finalidad, minimización de los datos y limitación del plazo de conservación allí enunciados, los sujetos comprendidos en el artículo 2 podrán, en la medida estrictamente necesaria y proporcionada, analizar las comunicaciones entrantes o salientes, y únicamente para los fines de seguridad de la información, de forma que sea posible impedir el acceso no autorizado a las redes y sistemas de información, detener los ataques de denegación de servicio, evitar la distribución malintencionada de código dañino así como otros daños a las antedichas redes y sistemas de información.

3. *Para corregir o, en su caso, exigir responsabilidades, cada usuario que acceda al sistema de información deberá estar identificado de forma única, de modo que se sepa, en todo momento, quién recibe derechos de acceso, de qué tipo son éstos, y quién ha realizado una determinada actividad*».

A resultas de cuanto antecede, procede colegir la obligatoriedad para las Administraciones Públicas de disponer, entre las medidas de seguridad que han de implementar, de un registro de actividad de tal modo que se garantice la identificación de cada uno de los usuarios del sistema de información y la actividad desarrollada por éstos.

III. SOBRE LA POSIBILIDAD DE ACCEDER AL REGISTRO DE ACCESOS POR PARTE DE LA PERSONA CUYOS DATOS ESTÁN SIENDO OBJETO DE TRATAMIENTO

Conforme al análisis realizado en el apartado anterior, la normativa reguladora del derecho fundamental a la protección de datos requiere que por parte de las Administraciones Públicas se dispongan una serie de medidas de seguridad entre las que se incluye la tenencia de un registro de la actividad de los usuarios, de tal modo que, a través de una serie de identificadores únicos se sepa, en todo momento, quién recibe derechos de acceso, de qué tipo son éstos y quién ha realizado una determinada actividad en el sistema de información.

Por consiguiente, la implementación de esta medida de seguridad, requerida por el Esquema Nacional de Seguridad, permite, por ejemplo, disponer de información acerca de quién ha consultado el historial clínico de un paciente, quién ha modificado un determinado campo en un expediente administrativo o quién ha impreso determinada documentación obrante en el sistema.

Siendo esto así, procede analizar en este punto si la persona cuyos datos estén siendo objeto de tratamiento puede conocer quién ha tenido acceso a los mismos.

III.1. Derecho de acceso en materia de protección de datos

III.1.1. *Contenido y alcance del derecho*

Conforme a la doctrina del Tribunal Constitucional, contenida entre otras en la STC 292/2000, de 30 de noviembre (RTC 2000\292) (la cursiva es nuestra),

> «*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.
>
> En fin, son elementos característicos de la definición constitucional del derecho fundamental a la protección de datos personales los derechos del afectado a consentir sobre la recogida y uso de sus datos personales y a saber de los mismos. Y *resultan indispensables para hacer efectivo ese contenido el reconocimiento del derecho a ser informado de quién posee sus datos personales y con qué fin, y el derecho a poder oponerse a esa posesión y uso requiriendo a quien corresponda que ponga fin a la posesión y empleo de los datos. Es decir, exigiendo del titular del fichero que le informe de qué datos posee sobre su persona, accediendo a sus oportunos registros y asientos, y qué destino han tenido, lo que alcanza también a posibles cesionarios*; y, en su caso, requerirle para que los rectifique o los cancele».

De acuerdo con lo anterior, el derecho a conocer quiénes son los posibles destinatarios de los datos personales forma parte indisoluble del contenido esencial del derecho fundamental, entendido éste como el poder de disposición y de control sobre los propios datos personales.

En consonancia con esta premisa, el RGPD consagra, entre los derechos de las personas interesadas, el derecho de acceso, y lo hace a través del artículo 15.

Así, en virtud de dicho precepto, el interesado puede obtener del responsable del tratamiento (i) la confirmación de si sus datos están siendo objeto de tratamiento y (ii), en el supuesto en que así sea, el acceso a sus datos y determinada información adicional, entre la que se incluye la relativa a los fines del tratamiento, las categorías de datos objeto de tratamiento y los destinatarios o categorías de destinatarios a los que se hayan comunicado o se vayan a comunicar los datos.

El Considerando 63 de la norma europea ahonda en el sentido y la razón de ser de este derecho de acceso, señalando lo siguiente (la cursiva y la negrita son nuestras):

> «*Los interesados deben tener derecho a acceder a los datos personales recogidos que le conciernan* y a ejercer dicho derecho con facilidad y a intervalos razonables, ***con el fin de conocer y verificar la licitud del tratamiento***. Ello incluye el derecho de los interesados a acceder a datos relativos a la salud, por ejemplo los datos de sus historias clínicas que contengan información como diagnósticos, resultados de exámenes, evaluaciones de facultativos y cualesquiera tratamientos o intervenciones practicadas. *Todo interesado debe, por tanto, tener el derecho a conocer y a que se le comuniquen*, en particular, los fines para los que se tratan los datos personales, su plazo de tratamiento, *sus destinatarios*, […]»

De este modo, se evidencia que el cometido del derecho de acceso es doble. Por un lado, hace posible que las personas interesadas conozcan el tratamiento que, en su caso, se esté realizado de sus datos personales y, por otro, les permite verificar la licitud de dicho tratamiento.

Para ello, el responsable del tratamiento debe facilitar a los interesados que ejerciten el derecho de acceso la información concerniente a los fines del tratamiento, los destinatarios o las categorías de destinatarios a los que se hayan comunicado o se vayan a comunicar los datos personales y cuantos otros aspectos relaciona el artículo 15 del RGPD.

III.1.2. *Consideración o no como tercero destinatario de los datos de la persona que realice la consulta*

Aclarado que el derecho fundamental a la protección de datos consiste en el poder de disposición y de control sobre los datos personales y que, por ende, el derecho de acceso, como mecanismo de verificación de la existencia de tratamiento y de la licitud del mismo, forma parte de su contenido esencial, procede analizar a continuación si mediante el ejercicio de este derecho de acceso la persona interesada puede conocer qué personas han consultado sus datos.

En este punto, procede insertar dos variables muy sustanciales para la adecuada resolución de la cuestión objeto de análisis: la primera, la relativa a la pertenencia o no

a la Administración Pública responsable del tratamiento o a un encargado designado por ésta de las personas que hayan realizado la consulta de los datos; y la segunda, la concerniente a la finalidad del tratamiento llevado a cabo por las personas que accedan a los datos, en particular, si la misma difiere de la fijada por la Administración responsable del tratamiento.

Con respecto a la primera de las variables, las Directrices 70/2020, del Comité Europeo de Protección de Datos, sobre los conceptos de «responsable del tratamiento» y «encargado del tratamiento» en el RGPD[2], señalan que «En principio, todo tratamiento de datos personales realizado por empleados en el ámbito de las actividades de una organización se presumirá realizado bajo el control de dicha organización».

En este sentido, a juicio de dicho Comité, «Los empleados que disponen de acceso a datos personales dentro de una organización no se consideran en general «responsables del tratamiento» ni «encargados del tratamiento», sino «personas que actúan bajo la autoridad del responsable o del encargado» en el sentido del artículo 29 del RGPD».

Por consiguiente, cuando la consulta de los datos se lleve a cabo por parte de un empleado que preste servicios para la Administración Pública responsable del tratamiento o para un encargado de tratamiento designado por ésta, en tales casos no se estará, a priori, ante una comunicación de datos.

No obstante, decimos que ello es así «a priori» porque resulta necesario atender a la segunda de las variables apuntadas, relativa a la finalidad del tratamiento realizado por dicho empleado.

De este modo, si el empleado en cuestión no estuviese autorizado por la Administración para llevar a cabo el tratamiento de los datos o si, estándolo, los destinase a fines distintos a los fijados por dicha Administración, en tal caso dicho empleado adquirirá la condición de tercero destinatario de los datos, se considerará responsable de tratamiento y asumirá todas las consecuencias y responsabilidades[3].

III.1.3. *Posibilidad de acceso a la información relativa a los destinatarios de los datos*

Tal y como se ha señalado previamente, mediante el ejercicio del derecho de acceso previsto en el artículo 15 del RGPD el interesado puede conocer la identidad de las personas destinatarias de sus datos.

De este modo, ante eventuales consultas de sus datos realizadas por empleados no autorizados por la Administración o en supuestos de utilización de dichos datos para fines distintos a los fijados por el responsable del tratamiento, procederá informar de

[2] https://edpb.europa.eu/system/files/2022-02/eppb_guidelines_202007_controllerprocessor_final_es.pdf

[3] En este sentido se pronuncia el Comité Europeo de Protección de Datos en las Directrices 70/2020, sobre los conceptos de responsable del tratamiento y encargado del tratamiento en el RGPD.

la identidad de tales empleados al amparo de lo dispuesto en el artículo 15.1.c) del RGPD, toda vez que los mismos habrían adquirido la consideración de terceros destinatarios de los datos y responsables del tratamiento en atención a las previamente aludidas Directrices 70/2020, del Comité Europeo de Protección de Datos, sobre los conceptos de responsable del tratamiento y encargado de tratamiento en el RGPD.

Esta misma conclusión es alcanzada por la Agencia Vasca de Protección de Datos en el Dictamen número D19-005, emitido en relación a una consulta sobre el contenido y alcance del derecho de acceso a los datos personales que obran en poder de la Administración en la que la persona consultante presta sus servicios[4], cuando indica:

> «Y si tal y como plantea la consulta, existiese la posibilidad de que personal de la propia Administración responsable del tratamiento hubiese accedido a los datos personales para fines distintos para los que se recabaron u obtuvieron, parece a todas luces innegable que dicha información tiene que proporcionarse al titular de dichos datos que ejercita el derecho de acceso, delimitándose con la mayor precisión posible el tratamiento así realizado. Sólo de esa forma, la persona titular de los datos personales podrá, en su caso, emprender las acciones legales que estime convenientes en defensa de su derecho fundamental a la protección de sus datos personales».

La misma consecuencia se deriva en supuestos de consultas a la base de datos realizadas por empleados ajenos a la Administración responsable del tratamiento o de algún encargado designado por ésta.

Así, conforme señala la Autoridad Catalana de Protección de Datos en el Informe Jurídico IAI 30/2022 emitido a petición de la Comisión de Garantía del Derecho de Acceso a la Información Pública en relación a la reclamación contra la denegación de un colegio profesional de la solicitud de acceso a información relacionada con los accesos a dos expedientes que afectan a la persona reclamante[5], «por la vía del ejercicio del derecho de acceso a los datos personales previsto en la normativa de protección de datos (art. 15 RGPD), la persona reclamante puede acceder a la identidad de los destinatarios de la información que no sea personal del colegio o de algún encargado del tratamiento».

Cuestión distinta sería que la persona que realizara la consulta ostentase la condición de personal al servicio de la Administración o de un encargado de tratamiento de ésta, que dispusiera de autorización suficiente y que no destinase los datos a una finalidad distinta a la prevista por el responsable del tratamiento.

En tal caso, la identificación de dicho empleado no se vería amparada por el derecho de acceso toda vez que estaría actuando bajo la autoridad del responsable o del

[4] https://www.euskadi.eus/contenidos/dictamen_avpd/d19_005/es_def/adjuntos/CN18-021_DIC_D19-005.pdf

[5] https://apdcat.gencat.cat/web/.content/Resolucio/Resolucions_Cercador/Dictamens/2022/Documents/es_iai_2022_030.pdf

encargado en el sentido del artículo 29 del RGPD y, por consiguiente, no tendría la condición de destinatario de los datos.

III.2. Derecho de acceso a la información pública

Conforme a lo concluido en el apartado anterior del presente análisis, el derecho de acceso regulado en el artículo 15 del RGPD no ampara el conocimiento, por parte de la persona interesada, de los datos identificativos de aquellas personas que hayan consultado sus datos personales ostentando la condición de personal al servicio de la Administración Pública o de un encargado de tratamiento de ésta, haciendo uso de la autorización concedida para ello, y no destinándolos a una finalidad distinta.

Esta circunstancia exige analizar si el acceso a dichos datos estaría justificado por la normativa reguladora del derecho de acceso a la información pública, representada a nivel estatal por la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.

A este respecto, procede partir del propio concepto de información pública, que es definido por el artículo 13 de la citada ley como «los contenidos o documentos, cualquiera que sea su formato o soporte, que obren en poder de alguno de los sujetos incluidos en el ámbito de aplicación de este título y que hayan sido elaborados o adquiridos en el ejercicio de sus funciones».

De este modo, la información contenida en el registro de actividad exigido para las Administraciones Públicas por el artículo 24 del ENS, donde se incluye la identificación de cada uno de los usuarios el sistema y la actividad desarrollada por éstos, resulta subsumible dentro del concepto de información pública.

Siendo esto así, y asumiendo el pleno sometimiento de las Administraciones Públicas a la normativa de transparencia y acceso a la información pública en los términos recogidos por el artículo 2 de la citada Ley estatal, resulta necesario dirimir en qué medida el derecho a la protección de datos del empleado que haya consultado los datos personales del interesado opera como límite al derecho de acceso a la información pública.

A este respecto, no debe perderse de vista que la persona interesada estaría solicitando a la Administración el acceso a la información relativa a la identidad de las personas que, en su condición de empleadas de la propia Administración o de un encargado de tratamiento de ésta, hayan consultado sus datos haciendo uso de los permisos concedidos al efecto.

Se trataría pues de información meramente identificativa, relacionada con la organización, funcionamiento o actividad pública del órgano, y con respecto a la misma el artículo 15.2 de la Ley 19/2013 prevé que con carácter general se concederá acceso, salvo que en el caso concreto prevalezca la protección de datos personales u otros derechos constitucionalmente protegidos sobre el interés público en la divulgación que lo impida.

Esta circunstancia obliga a que, con carácter general, la Administración dé traslado para alegaciones de la solicitud de acceso a la información pública planteada por el interesado para, con ello, poder garantizar el pleno respeto de todos los derechos e intereses objeto de protección.

En todo caso, para la adecuada resolución del asunto, la Administración responsable del tratamiento debe tener presente que la mera oposición del empleado no bastaría para justificar la denegación del acceso a la información pública, debiendo en consecuencia ponderar las circunstancias concurrentes en cada caso particular.

A tal efecto, no debe obviar que el conocimiento, por parte del interesado, de la identidad de las personas que hayan accedido a sus datos es, en los términos que indica la Autoridad Catalana de Protección de Datos en el Informe Jurídico previamente aludido, «una medida que permite el control por parte de la persona interesada, de qué personas han accedido a su información personal, por lo que, desde el punto de vista del derecho a la protección de datos, este acceso obedece a un interés legítimo y constituye una garantía para controlar el adecuado tratamiento de la información por parte del responsable del tratamiento».

Finalmente, procede recordar que para el supuesto en que la Administración actuante denegara el acceso a la información pública, la persona interesada podría interponer la oportuna reclamación ante la autoridad de control en materia de transparencia, con carácter potestativo y previo a la eventual impugnación en vía contencioso-administrativa[6].

III.3. Conclusiones

A resultas de cuanto se ha expuesto en los apartados anteriores procede concluir lo siguiente:

— Que conforme a lo dispuesto en el artículo 24 del Esquema Nacional de Seguridad, las Administraciones Públicas están obligadas a disponer de un registro de actividad que garantice la identificación de cada uno de los usuarios del sistema de información y la actividad desarrollada por éstos.
— Que la información contenida en dicho registro de actividad merece la consideración de información pública, conforme a lo dispuesto por la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.
— Que el derecho de acceso en materia de protección de datos prevenido en el artículo 15 del RGPD, permite al interesado conocer la identidad de las personas destinatarias de sus datos.

[6] Con respecto al régimen regulatorio de estas impugnaciones, véanse los artículos 23 y 24 de la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.

— Que ante eventuales consultas a las bases de datos realizadas por empleados de las Administraciones Públicas que no hubiesen sido oportunamente autorizados para ello; o incluso en supuestos de utilización de dichos datos para fines distintos a los fijados por el responsable del tratamiento, dichos empleados merecerían la consideración de terceros destinatarios de los datos y responsables del tratamiento.
— Que al tener la consideración de destinatarios de los datos, el conocimiento de su identidad por parte de la persona interesada estaría amparado por el derecho de acceso en materia de protección de datos.
— Que por el contrario, derecho de acceso regulado en el artículo 15 del RGPD no ampara el conocimiento, por parte de la persona interesada, de los datos identificativos de aquellas personas que hayan consultado sus datos personales ostentando la condición de personal al servicio de la Administración Pública o de un encargado de tratamiento de ésta, haciendo uso de la autorización concedida para ello, y no destinándolos a una finalidad distinta, ya que en tales supuestos no tendrían la consideración de terceros destinatarios de los datos.
— Que en este último caso, el acceso a la información relativa a la identidad de las personas que hayan realizado la consulta procedería encauzarlo a través de la normativa de transparencia y acceso a la información pública.
— Que en tal caso, la información solicitada por el interesado al amparo de la Ley 19/2013 sería información meramente identificativa, relacionada con la organización, funcionamiento o actividad pública del órgano, y con respecto a la misma el artículo 15.2 de la citada Ley prevé que con carácter general se concederá acceso a la misma, salvo que en el caso concreto prevalezca la protección de datos personales u otros derechos constitucionalmente protegidos sobre el interés público en la divulgación que lo impida.
— Que la concurrencia de esta circunstancia obliga a que, con carácter general, la Administración dé traslado para alegaciones de la solicitud de acceso a la información pública planteada por el interesado para, con ello, poder garantizar el pleno respeto de todos los derechos e intereses objeto de protección.
— Que la mera oposición del empleado no bastaría para justificar la denegación del acceso a la información pública, debiendo la Administración ponderar las circunstancias concurrentes en cada caso particular.
— Que en todo caso, para la adecuada resolución del asunto, la Administración responsable del tratamiento debe tener presente que el conocimiento, por parte del interesado, de la identidad de las personas que hayan accedido a sus datos es una medida que permite el control de qué personas han accedido a su información personal, por lo que, desde el punto de vista del derecho a la protección de datos, este acceso obedece a un interés legítimo y constituye una garantía para controlar el adecuado tratamiento de la información por parte del responsable del tratamiento.

— Que en el supuesto en que la Administración denegase el acceso a la información pública, el interesado podría interponer la oportuna reclamación ante la autoridad de control en materia de transparencia, con carácter potestativo y previo a la eventual impugnación en vía contencioso-administrativa.

Finalmente, procede significar que durante la fase de inserción de correcciones de la presente publicación, el Tribunal de Justicia de la Unión Europea ha dictado Sentencia, de fecha 22 de junio de 2023 (asunto C-579/21), que tiene especial relevancia en el asunto objeto de análisis.

Analizada la doctrina del Tribunal, se concluye la vigencia de las conclusiones extraídas y la oportunidad de adicionar las siguientes:

— Que el derecho de acceso prevenido en el artículo 15 del RGPD debe interpretarse en el sentido de que la información relativa a las operaciones de consulta de datos personales de una persona, la fecha en la que éstas se hayan realizado y los fines de estas operaciones constituyen información que la persona interesada tiene derecho a obtener del responsable del tratamiento.
— Que el derecho de acceso previsto en el artículo 15 del RGPD no alcanzaría a la información relativa a la identidad de las personas que realizaron las operaciones de consulta cuando éstas hubiesen actuado bajo la autoridad y conforme a las instrucciones de la Administración responsable del tratamiento, a menos que esa información resultase indispensable para permitir al interesado ejercer efectivamente los derechos que le confiere el RGPD y siempre bajo la condición de que se tengan en cuenta los derechos y libertades de aquellas personas.
— Que en base a ello, resultaría preciso proporcionar a la persona interesada toda la información necesaria para garantizar el contenido del derecho de acceso para así evitar vaciarlo de contenido. Para ello, sería oportuno implementar mecanismos que impidan la revelación de la identidad de la persona que haya consultado los datos pero que, al mismo tiempo, hagan factible individualización y la comprobación, por parte del interesado, de la licitud de cada una de las operaciones realizadas de consulta de sus datos. Así, por ejemplo, sería oportuno informar acerca de consultas realizadas de la historia clínica del interesado detallando fechas y horas de las mismas, los centros sanitarios y los servicios o departamentos desde los que se hubieran realizado, la categoría profesional y demás información que permita vincular los accesos realizados por una misma persona, utilizando para ello mecanismos de anonimización y explicitando, en todo caso, las finalidades de cada una de dichas consultas.

CAPÍTULO 7

LA REGULACIÓN DEL DERECHO DE ACCESO A LA INFORMACIÓN PÚBLICA Y LA PROTECCIÓN DE DATOS PERSONALES: PUNTOS DE CONFLICTO Y OPORTUNIDADES DE MEJORA LEGISLATIVA

Elisabet Samarra Gallego

Presidenta de la Comisión de Garantía del Derecho de Acceso
a la Información Pública de Cataluña

SUMARIO

I. EL CONFLICTO ENTRE EL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES Y EL DERECHO A LA INFORMACIÓN

La protección de datos personales es, con mucho, el límite más invocado para restringir o denegar el derecho de acceso a la información pública, pero también el peor aplicado. Muchas administraciones y ciudadanos perciben ambos derechos como incompatibles y entienden que el conflicto entre ambos debe resolverse sacrificando necesariamente el derecho de acceso a la información en beneficio de la protección de datos personales.

Esta errónea apreciación suele fundamenta en alguno de estos presupuestos:

- Implantación del derecho a la protección de datos frente a la novedad del derecho de acceso a la información pública:

El derecho a la protección de datos personales cuenta con una larga tradición legal, es protegido y casi sacralizado por las administraciones, y ampliamente conocido y exigido por la ciudadanía. En cambio, el derecho de acceso a la información pública es

un derecho de nueva cuña legal, relegado por las administraciones a un papel secundario y residual al que destinan los escasos recursos sobrantes, si los hay, y que aún no se ha incorporado conscientemente a la cartera de derechos individuales y cívicos por parte de la mayor parte de la ciudadanía, que difícilmente conocen que pueden pedir información y menos aún que pueden reclamarla gratuitamente ante un órgano de garantía. Todo ello se traduce en una percepción, más o menos consciente, de que perjudicar al derecho de protección de datos personales tiene un mayor coste que vulnerar el derecho a la información, de forma que muchas administraciones optan, ante el conflicto de ambos, por el primero.

- Supeditación del acceso a información pública que contenga datos personales al consentimiento del afectado.

En realidad, en el procedimiento de acceso a la información pública, el consentimiento del afectado solo es exigible para el acceso a categorías de datos personales sensibles, de otro modo excluidas del acceso por la ley de transparencia. Respecto de cualquier otro dato personal, el consentimiento no es requisito para la legitimidad de la cesión del dato y no tiene otro efecto que la eventual suspensión de la ejecución de la resolución estimatoria durante el plazo para interponer recurso contencioso administrativo.

Efectivamente el artículo 6.1 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril, 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, RGPD) establece distintas bases alternativas para la licitud del tratamiento («El tratamiento sólo será lícito si se cumple al menos una de estas condiciones»); una es, efectivamente, el consentimiento del afectado (apartado a) y otra distinta (apartado c) es que derive del cumplimiento de una obligación legal aplicable al responsable tratamiento de datos personales. Este último es el fundamento de la licitud del tratamiento de datos personales en el marco del derecho de acceso a la información, visto que se establece como una obligación de las administraciones por una norma con rango de ley. Y puesto que las bases de licitud del tratamiento se plantean por el Reglamento europeo como alternativas i no acumulativas, no tiene ningún fundamento exigir que, en el derecho de acceso, deban darse acumuladamente las condiciones del apartado a y c.

El artículo 6.3 RGPD establece que la base del tratamiento indicado en el apartado 1.c deberá ser establecida por el derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento, en este caso la ley de transparencia, y que la finalidad del tratamiento deberá quedar determinada en dicha base jurídica, que podrá contener disposiciones específicas para adaptar la aplicación de normas del presente Reglamento, entre otras, las condiciones generales del tratamiento y los fines de la

comunicación, y que dicha base jurídica deberá cumplir un objetivo de interés público y será proporcional al fin legítimo perseguido.

De todo lo anterior debe concluirse que, conforme al artículo 6.1 RGPD, la licitud del tratamiento de datos personales para la satisfacción del derecho de acceso a la información pública no requiere que se del consentimiento del afectado previsto en el apartado a) puesto que ya cumple con la condición alternativa y no acumulativa establecida en el apartado c), y por lo tanto, será lícito el tratamiento de datos personales si, conforme al artículo 6.3 RGPD, se hace conforme a las condiciones y requisitos de la ley de transparencia, ponderando su relevancia para cumplir el objetivo de interés público perseguido por ese marco legal, y si es proporcional al fin legítimo perseguido. Este último requisito de proporcionalidad está vinculado estrechamente al principio de minimización de datos personales del artículo 5.1.c RGPD, y requiere que, además de los criterios ponderativos específicos de la ley de transparencia, deba aplicarse también a la ponderación el principio de minimización de los datos personales cedidos, comprobando que sean adecuados, pertinentes y limitados en relación con el fin de la transparencia y el control de las administraciones públicas, y descartando sacrificios desproporcionados de datos personales que no resulten necesarios ni relevantes para esa finalidad.

En la misma línea, el articulo 86 RGPD dispone que los datos personales de documentos oficiales en posesión de alguna autoridad u organismo público podrán ser comunicados de conformidad con la legislación de los estados miembros, a fin de conciliar el acceso del público a documentos oficiales con el derecho a la protección de los datos personales. De nuevo, el RGPD legitima el tratamiento de los datos personales en documentos oficiales si es conforme a la ley que determina el régimen de acceso a la información pública, sin ninguna referencia ni condicionante al consentimiento del afectado.

Conforme a esta regulación europea, el artículo 8 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD) establece que el tratamiento de datos personales se considerará fundado en el cumplimiento de una obligación legal exigible al responsable, en los términos previstos en el artículo 6.1.c) del Reglamento (UE) 2016/679, cuando así lo prevea una norma con rango de ley, que podrá determinar las condiciones generales del tratamiento y los tipos de datos objeto del mismo, así como las cesiones que procedan como consecuencia del cumplimiento de la obligación legal. Y la Disposición adicional segunda de dicha ley establece que, cuando el tratamiento de los datos personales derive de las obligaciones de publicidad activa y del acceso a la información pública regulados por las leyes de transparencia estatal o autonómica, se someterá a dichas normas.

Así pues, la cesión de datos personales en el marco del derecho de acceso a la información pública es lícita si es conforme al régimen jurídico de acceso a la información establecido en la ley de transparencia, y el acceso no puede condicionarse al

consentimiento de la persona afectada, excepto que sea la propia ley de transparencia la que determine que debe concurrir, tal y como dispone para el acceso a categorías especiales de datos personales sensibles.

Por tanto, el trámite de traslado de las solicitudes de información o sus reclamaciones no debe tener la finalidad de recabar el consentimiento del afectado, sino asegurar que tiene la oportunidad de aportar a la ponderación elementos casuísticos particulares, si los hay, que puedan tener incidencia en la resolución. Y lo cierto es que en la inmensa mayoría de los casos, el afectado no aprecia correctamente lo que se le pide (posiblemente inducido en su error por el oficio de traslado de las administraciones) y se limita a expresar su falta de consentimiento, sin mayor argumentación ni consideración de su particular afectación, lo que, como hemos visto, no es vinculante para la administración ni determinante para justificar la desestimación de la solicitud, ni tendrá otro efecto automático más que la determinación de la suspensión temporal de la ejecución de la resolución estimatoria del derecho de acceso durante el plazo para que el afectado pueda interponer recurso contencioso administrativo.

- Considerar que debe ser prevalente siempre el derecho a la protección de datos personales por su carácter de derecho fundamental.

Algunos creen que el hecho de que la protección de datos personales tenga el reconocimiento de derecho fundamental, mientras que el derecho de acceso a la información pública no lo tenga como tal, es razón suficiente para que, siempre que entren en conflicto, deba hacerse prevalecer el primero sobre el segundo. Esta atribución de mejor protección por su carácter fundamental, sin embargo, no se compadece con la regulación expresa de las leyes implicadas: la ley de protección de datos personales, que remite a la legislación de transparencia (Disposición Adicional Segunda LOPDGDD), y la ley de transparencia, que lo regula como un límite al acceso estableciendo las condiciones de su aplicación: régimen de exclusión del acceso de los datos personales de categoría especial excepto si se aporta el consentimiento; régimen general de acceso a los datos meramente identificativos del personal público, y una obligación de ponderación casuística y motivada en el acceso al resto de datos personales. Ni una ni otra ley establece una preponderancia predeterminada del derecho a la protección de datos personales sobre el derecho de acceso a la información, ni siquiera establecen que deba tenerse en cuenta el carácter de derecho fundamental del derecho a la protección de datos personales como un elemento de ponderación en favor del mismo. No existe, pues, justificación legal para prejuzgar la prevalencia del derecho a la protección de datos personales y la supeditación del derecho de acceso a la información en caso de conflicto.

Tampoco puede sostenerse que exista una necesaria e incondicional supeditación del derecho de acceso a la información al derecho de protección de datos personales por el mayor rango normativo de su regulación, puesto que es la propia ley orgánica

de protección de datos la que remite a la regulación de la ley ordinaria de transparencia para determinar las condiciones de acceso a los datos personales contenidos en la información pública.

Todas las razones anteriores, y seguro que algunas más, predisponen a las administraciones y entes públicos al rechazo de las solicitudes de acceso a información si en ellas hay datos personales, y más allá incluso, las condiciona irremisiblemente al rechazo si los afectados no consienten, lo que conduce a que cerca del 70% de las reclamaciones contra resoluciones expresas de desestimación del acceso estén fundamentadas en la protección de datos personales.

II. POSIBILIDAD DE MEJORA LEGISLATIVA: EL INFORME DE LA AGENCIA O AUTORIDAD DE PROTECCIÓN DE DATOS PERSONALES EN EL PROCEDIMIENTO DE RECLAMACIÓN DE ACCESO A INFORMACIÓN PÚBLICA

La legislación de transparencia catalana tiene, en líneas generales, idéntica regulación de la protección de datos personales como límite al acceso a la información pública, si bien contiene una particularidad en el procedimiento de reclamación que se propone como mejora de la legislación básica estatal.

El artículo 42.8 de la ley de transparencia catalana (Ley 19/2014, del 29 de diciembre, sobre la transparencia, el derecho de acceso a la información pública y buen gobierno) prevé que en el procedimiento de reclamación de información pública y cuando la desestimación del acceso se haya fundamentado en la protección de datos personales, el órgano de garantía (en Cataluña, la Comisión de Garantía del Derecho de Acceso a la Información Pública) pueda requerir el informe de la Autoridad de protección de datos personales como elemento de juicio para su resolución: «Si la denegación se ha fundamentado en la protección de datos personales, la Comisión debe solicitar informe a la Autoridad Catalana de Protección de Datos, el cual debe ser emitido en el plazo de quince días».

Se trata de un informe preceptivo, pero no vinculante para la Comisión, en el cual la autoridad catalana de protección de datos analiza el encaje de la petición de acceso a la información con el derecho a la protección de datos personales, a la vista del informe de la administración y de las alegaciones que hayan podido realizar los afectados en fase de traslado, y dictamina su parecer exclusivamente en relación con este límite al acceso. Este dictamen lo hace la Autoridad aplicando la ley de transparencia, desde la premisa de que la ley de transparencia constituye la base jurídica legitimante de la cesión de datos personales y determinante de la finalidad y las condiciones de acceso. Y el hecho de que su pronunciamiento no sea vinculante para el órgano de garantía del acceso a la información, que válidamente puede ponderar de distinta forma la aplicación del límite a la protección de datos personales y resolver en sentido contrario o

parcialmente diverso, es una muestra más de que el legislador en ningún momento admitió ni dispuso esa primacía del derecho a la protección de datos personales sobre el derecho de acceso.

Este informe sobre la adecuación del acceso reclamado al derecho a la protección de datos se remite a las partes y se reproduce ampliamente en la resolución de la reclamación, y en caso de que el sentido de la resolución de la reclamación se aparte de la conclusión del informe de la autoridad de protección de datos, se motiva en un fundamento jurídico.

Esta vía permite que el órgano de garantía del derecho a la protección de datos personales participe en el procedimiento de reclamación del derecho de acceso a la información pública cuando la satisfacción del segundo comporte la vulneración del primero, y aporte su análisis ponderativo del acceso desde la exclusiva y única ponderación de este límite. Ello aporta mayor garantía a los afectados, que en la resolución de la reclamación conocen no solo el criterio del órgano de garantía del derecho de acceso a la información pública, sino también el criterio del órgano de garantía de la protección de datos personales, y cuando es coincidente (lo que sucede en el 90% de los casos) aporta una solidez jurídica adicional al pronunciamiento estimatorio o desestimatorio del acceso fuera de sospechas y recelos, lo que posiblemente sea el factor más relevante del ínfimo nivel de litigiosidad de los afectados contra nuestro órgano de garantía por vulneración de la protección de datos personales.

Este trámite sirve, también, al necesario balance de los bienes jurídicos a proteger por cada órgano de garantía, y contribuye a que se equilibren y se analicen con una visión conjunta y global, como derechos a proteger ambos, y no solo uno, ni uno por encima del otro.

III. EL ACCESO A DATOS PERSONALES PROPIOS Y LA CONFLUENCIA DE PROCEDIMIENTOS DE GARANTÍA DEL ACCESO A LA INFORMACÍON

La Ley de transparencia catalana dispone lo siguiente respecto a los datos propios del solicitante de información pública:

> «Art. 24.3: Las solicitudes de acceso a la información pública que se refieran solamente a datos personales del solicitante deben resolverse de acuerdo con la regulación del derecho de acceso establecido por la legislación de protección de datos de carácter personal.»

Conforme a ello, el acceso a los datos propios del solicitante que se contengan en la información pública se valora conforme al régimen de acceso del artículo 15 del Reglamento europeo de Protección de Datos Personales (RGPD): acceso reconocido a

la información propia en poder de la administración, incluída la fuente u origen de estos datos, y a las comunicaciones de dichos propios a terceros, identificados nominalmente y por la organización a la que pertenecen.

Por otra parte, existe un procedimiento ante la APDCAT para las reclamaciones por denegación de uno de los derechos ARQUEO establecido en la Ley 32/2010, del 1 de octubre, de la Autoridad Catalana de Protección de Datos:

> «Artículo 16. Tutela de los derechos de acceso, rectificación, oposición y cancelación
>
> 1. Las personas interesadas a las que se deniegue, en parte o totalmente, el ejercicio de los derechos de acceso, de rectificación, de cancelación o de oposición, o que puedan entender desestimada su solicitud por el hecho de no haber sido resuelta y no enviada dentro del plazo establecido, pueden presentar una reclamación ante la Autoridad Catalana de Protección de Datos.
>
> 2. La Autoridad Catalana de Protección de Datos tiene que resolver expresamente sobre la procedencia o improcedencia de la reclamación a que hace referencia el apartado 1 en el plazo de seis meses, con la audiencia previa de la persona responsable del fichero y también de las personas interesadas si el resultado del primer trámite de audiencia lo hace necesario. Una vez transcurrido este plazo, si la Autoridad no ha notificado la resolución de la reclamación, se entiende que ha sido desestimada.
>
> 3. La resolución de estimación total o parcial de la tutela de un derecho tiene que establecer el plazo en que este se tiene que hacer efectivo.
>
> 4. Si la solicitud de ejercicio del derecho ante la persona responsable del fichero es amada, en parte o totalmente, pero el derecho no se ha hecho efectivo en la forma y los plazos exigibles de acuerdo con la normativa aplicable, las personas interesadas lo pueden poner en conocimiento de la Autoridad Catalana de Protección de Datos para que se lleven a cabo las actuaciones sancionadoras correspondientes.»

Debe entenderse, pues, que cuando una persona física pretenda acceder a la información propia en poder de las administraciones o a las comunicaciones que hayan hecho éstas a terceros, deberá seguir el procedimiento previsto en la legislación de datos personales, y reclamar, en su caso, ante la autoridad o agencia de protección de datos personales. En estos casos, si la reclamación se presenta ante la GAIP, se procede a su derivación a la Autoridad de Protección de Datos de Cataluña (APDCAT) para que resuelva conforme esa normativa. Por su parte, cuando la APDCAT recibe una reclamación por acceso a información en la que, además de datos propios, constan datos de terceras personas, procede a derivarla a la Comisión de Garantía del Derecho de Acceso a la Información Pública (GAIP) para que resuelva la reclamación conforme a la normativa de transparencia.

Estas son las reglas de reparto establecidas, pero lo cierto es que existen zonas de confluencia que generan duplicidades y confusiones a los ciudadanos, y otras, más preocupantes, en las que se genera un vacío de protección, que sería necesario regular.

En este sentido, hemos atendido diversas reclamaciones en las que el reclamante solicita al Instituto Catalán de Salud la identidad de los facultativos que habían accedido a su historia clínica, la fecha y el motivo, derivadas de la APDCAT, que se inhibió entendiendo que no existía comunicación a terceros por lo que quedaba fuera de su ámbito de protección. El posicionamiento del APDCAT sobre lo que comprende el concepto de derecho de acceso a la trazabilidad de la historia clínica del paciente quedaría comprendido en esta fundamentación:

> «4.1. Sobre el derecho de acceso a la trazabilidad de la historia clínica
>
> La persona reclamante pedía la trazabilidad referida al periodo comprendido de 25 a 27 de mayo de 2020, de 2 a 6 de febrero de 2021 y 11 de junio a 30 de julio de 2021. Al respecto, en respuesta a la petición, el [centro hospitalario] desestimó la solicitud argumentando que no procedía facilitar «los nombres y otros datos personales de profesionales que han accedido a su historia clínica por razón de sus funciones».

Establecido lo anterior, hay que tener en cuenta los términos concretos de la petición, que se referían a la «trazabilidad» de la historia clínica. Al respecto, el Anexo IV del Real Decreto 3/2010, de 8 de enero, por el cual se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, vigente en el momento que se formuló la solicitud, define la trazabilidad como la «propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente en dicha entidad». En términos similares, el Real Decreto 311/2022, de 3 de mayo, por el cual se regula el Esquema Nacional de Seguridad, y se deroga el Real Decreto 3/2010 mencionado, define la trazabilidad como la «propiedad o característica consistente en que las actuaciones de una entidad (persona o proceso) puedan ser trazadas e forma indiscutible hasta dicha entidad».

Por su parte, la «Guía de Seguridad de las TIC CCN-STIC 803. ENTE [Esquema Nacional de Seguridad]. Valoración de los sistemas» elaborada por el Centro Criptológico Nacional, se refiere a la trazabilidad como «poder comprobar a posteriori quién ha accedido a, o modificado, una cierta información».

De acuerdo con lo anterior, procede afirmar que la trazabilidad de los accesos a la historia clínica de un paciente comprende la información sobre la identidad, cargo y/o categoría del personal del responsable del tratamiento que accede, la fecha y hora de los accesos, centro y módulo o unidad desde la cual se accede, y también conocer los destinatarios o categorías de destinatarios a las cuales se facilitó la información clínica (es decir, a qué entidades o personas de fuera la organización se van comunicar los datos clínicos).

Ahora bien, de entre todo aquello que se ha dicho que abarca el concepto de «trazabilidad» aplicado a los accesos a la historia clínica, sólo las comunicaciones efectuadas a entidades o personas de fuera del ámbito del responsable del tratamiento forman parte del derecho de acceso previsto al artículo 15 del RGPD.

Pues bien, en relación con la respuesta del (centro hospitalario), procede señalar que esta Autoridad ha puesto de manifiesto en varias resoluciones y dictámenes (PT 60/2020, PT 21/2019, CNS 8/2019 y CNS 53/2019, entre otros), que no forma parte del derecho de acceso previsto en el artículo 15 el RGPD, conocer la identificación del personal que trabaja por cuenta del responsable del tratamiento (en este caso, el centro sanitario) que ha accedido a la historia clínica.

Y ello porque, en esencia, este tipo de acceso no se puede considerar una comunicación de datos a terceras personas destinatarias; y consiguientemente, no se puede incluir dentro del apartado c) del referido artículo, como información que la persona afectada tiene derecho a conocer en ejercicio de este derecho («los destinatarios o laso categorías de destinatarios a los que se comunicaron o serán comunicados los datos personales, en particular destinatarios en terceros uno organizaciones internacionales»).

Es cierto que el Grupo del artículo 29 — integrado por las Autoridades de Protección de Datos de los estados miembros de la Unión Europea, el Supervisor Europeo de Protección de Datos, y la Comisión Europea: hoy sustituido por el Comité Europeo de Protección de Datos — recomendó a los estados miembros de la Unión Europea que reconocieran el derecho del paciente a conocer la información sobre quién y cuándo ha accedido a su historia clínica, con el fin de generar confianza sobre los tratamientos efectuados con sus datos sanitarios; y en términos similares se ha pronunciado esta Autoridad.

Pero lo cierto es que la regulación del derecho de acceso prevista al artículo 15 RGPD no lo contempla. Otra cosa es que el centro sanitario, a pesar de no tener la obligación legal de hacerlo, facilite esta información siguiendo la mencionada recomendación.

De acuerdo con lo expuesto, el centro sanitario debería haber informado al ahora reclamante de aquellas eventuales comunicaciones que la entidad hubiera efectuado a terceras personas destinatarias de los datos, o en caso de no haberse producido ninguna comunicación, informado de este extremo, ya que esta información sí forma parte del derecho de acceso garantizado y regulado por el artículo 15 del RGPD.

A la vista de las anteriores consideraciones, hay que estimar el derecho de acceso de la persona reclamante a obtener la trazabilidad de su historia clínica, pero únicamente y exclusivamente con respecto a conocer la información relativa a las eventuales comunicaciones a terceras personas destinatarias de los datos, o bien a obtener información sobre la inexistencia de estas. (…) «

De conformidad con este posicionamiento expuesto, la APDCAT remite al procedimiento de acceso a la información previsto por la ley de transparencia para solicitar

la información sobre los accesos a la historia clínica del reclamante producidos dentro del ámbito organizativo del responsable del tratamiento, y a la GAIP para su reclamación:

> «Con respecto a la trazabilidad de los accesos a la historia clínica de un paciente desde la perspectiva del contenido del derecho de acceso regulado en el artículo 15 del RGPD —la desatención del cual constituye el objeto del presente procedimiento de tutela—, hay que puntualizar que la información que hay que proporcionar es la relativa a los destinatarios o categorías de destinatarios a quien se habría facilitado la información clínica, es decir, la identificación de las entidades o personas de fuera de la organización a quién se comunicaron los datos clínicos. Por lo tanto, no incluiría la identidad del personal adscrito al responsable del tratamiento (en este caso, el ICS) que ha accedido a la historia clínica.

Por otra parte, la normativa sanitaria que se ha transcrito en el fundamento de derecho 2.º tampoco reconoce el derecho del paciente a conocer la identidad de los profesionales que han accedido a la suya historia clínica. Otra cosa es que la persona reclamante pueda acceder a esta información ejerciendo el derecho de acceso a la información pública regulado en el artículo 18 y ss. de la Ley 19/2014, del 29 de diciembre, de transparencia, acceso a la información pública y buen gobierno.

Por lo tanto, con respecto a la solicitud de acceso referida a la trazabilidad de la historia clínica, procede reconocer el derecho de la persona reclamante a acceder a la información en lo referente al periodo solicitado (del 07/10/2018 al 06/10/2020) sobre los destinatarios o categorías de destinatarios a quienes se hayan comunicado sus datos, y desestimar la reclamación con respecto a la solicitud de acceso al resto de información sobre trazabilidad, por exceder del alcance material del derecho de acceso previsto al arte. 15 del RGPD».

Derivadas las reclamaciones a la GAIP por parte de la APDCAT, esta Comisión las ha resuelto estimando el derecho de acceso a los accesos producidos en el marco de la organización del responsable del tratamiento a la historia clínica del reclamante conforme a la ley catalana de transparencia. Entre ellas, la Resolución de la GAIP 785/2022, de 22 de septiembre, de la que se reproduce parcialmente su fundamento jurídico 2:

> «Por lo que se ha dicho en los párrafos anteriores, si las personas que han accedido al historial clínico de la persona reclamante son externas al ICS [Instituto Catalán de la Salud], el artículo 15.1 RPDP garantiza el derecho de la persona reclamante a conocer estos accesos, derecho que incluye la identidad las personas que han accedido a su historial y las circunstancias de los accesos producidos. Sin embargo, hay que valorar a la luz de la LTAIPBG el derecho de personas al servicio del ICS a acceder a los datos personales de la persona reclamante, porque en este

caso no se aplica preferentemente el artículo 15 RPDP, sino la legislación de transparencia y del derecho de acceso a la información pública.

Como ya se ha dicho al inicio de este fundamento jurídico, al ser el historial clínico laboral del ICS de la persona reclamante información pública, cualquier persona tiene derecho a acceder a él, a menos que concurran causas legales que justifiquen la denegación. La causa legal que concurre al caso es la protección de los datos personales de las personas que han accedido al historial de la persona reclamante, ya que, entre otras cosas, se solicita su identidad. El acceso a la información solicitada (nombre y apellidos y categoría profesional del personal al servicio del ICS que ha entrado en el historial clínico laboral de la persona reclamante y las otras varias circunstancias indicadas en la solicitud [fecha y motivo] debe regirse por el artículo 24.2 LTAIPBG, ya que los datos personales que forman parte de la información solicitada ni son meramente identificativos relacionadas con la organización y el funcionamiento de la Administración (en este caso, sería de aplicación el artículo 24.1 LTAIPBG), ni especialmente protegidas por el artículo 23 LTAIPBG. Según el artículo 24.2 LTAIPBG, «si se trata de otra información que contiene datos personales no incluidos en el artículo 23, se puede dar acceso a la información, con la previa ponderación razonada del interés público en la divulgación y los derechos de las personas afectadas. Para llevar a cabo esta ponderación se debe tener en cuenta, entre otras, las circunstancias siguientes: a) El tiempo transcurrido. b) La finalidad del acceso, especialmente si tiene una finalidad histórica, estadística o científica, y las garantías que se ofrezcan. c) El hecho de que se trate de datos relativos a menores de edad. d) El hecho de que pueda afectar a la seguridad de las personas».

Además del interés general inherente al acceso a la información pública, según la legislación de transparencia y acceso a la información pública, el derecho de la persona reclamante a la información sobre la identidad de las personas que han accedido a su historial clínico resulta reforzado significativamente si se tiene en cuenta que pide información sobre las personas que han accedido a una información suya que está especialmente protegida, muy relevante tanto desde el punto de vista de su intimidad como de sus condiciones de trabajo. En cambio, para las personas que han accedido al historial, la divulgación de su identidad a la persona reclamante no les comporta ningún sacrificio significativo, porque si han accedido legítimamente, en ejercicio de sus funciones profesionales, la información divulgada afecta únicamente datos de su dimensión profesional, sin afectación de su privacidad; y si no han accedido legítimamente, difícilmente pueden invocar la protección de su identidad para tapar su actuación ilegítima.

Los antecedentes 18 y 19 indican que la Reclamación ha sido notificada a las terceras personas afectadas, es decir, a los y las profesionales del ICS que han entrado en la historia clínica laboral de la persona reclamante, a las cuales se ha dado la oportunidad presentar alegaciones. Únicamente una de las terceras personas afectadas ha con-

testado esta notificación y no se opone en absoluto a las pretensiones de la persona reclamante, ni pone de manifiesto que el acceso solicitado en este procedimiento comporte para ella ningún perjuicio.

En atención a las anteriores consideraciones, es procedente estimar la Reclamación 44/2022, declarar el derecho de la persona reclamante a la información solicitada sobre los accesos a su historia clínica laboral en el programa PREVEN utilizado por el servicio de prevención de riesgos laborales del ICS, en el periodo comprendido entre el 20 de agosto del 2020 y el 20 de agosto del 2021, y con indicación de los siguientes datos para cada acceso: fecha, nombre y categoría de los profesionales que han accedido, motivo y unidad, centro y población desde la que se ha producido cada acceso».

Esta Resolución está recurrida por el ICS ante el Tribunal Superior de Justicia de Cataluña argumentando la incompetencia dela GAIP para atender esta reclamación y considerando competente a la APDCAT, a pesar de que fue precisamente esta autoridad la que derivó a la GAIP la reclamación. No existe aún sentencia, aunque sí desestimación de la medida cautelar de suspensión de la Resolución de la GAIP solicitada por el recurrente.

Así, la protección a los ciudadanos respecto de la información sobre los accesos producidos en su historial clínico se protegen, si son dentro de la organización del responsable del tratamiento, por la GAIP aplicando la ley de transparencia, y si son de personas ajenas al responsable del tratamiento, por la APDCAT aplicando el procedimiento de garantía de acceso a datos personales.

Desde el punto de vista del reclamante, es difícil justificar que la su petición deba ser fraccionada y reclamada por dos vías y ante dos órganos distintos, pero sobretodo, esto plantea a mi juicio un vacío de protección que sin amparo la trazabilidad de los accesos a historias clínicas por parte de personal propio del titular de los datos cuando éste sea una entidad privada no sometida a la ley de transparencia. En estos casos, y según esta aplicación estricta del término «comunicación» del artículo 15.1.c RGPD, la persona afectada por el acceso a datos propios tan sensibles como los de su salud no podría obtener el amparo de la autoridad de protección de datos personales, ni tampoco podría reclamarla por el procedimiento de la ley de transparencia, puesto que no serían sujetos obligados por ella.

Nos encontramos, pues, ante una zona de desprotección en un ámbito de la máxima importancia y sensibilidad, como los accesos a datos clínicos, que debemos abordar, recordando que el Grupo del artículo 29 recomendó a los estados miembros de la Unión Europea que reconocieran el derecho del paciente a conocer la información sobre quién y cuándo ha accedido a su historia clínica, para generar confianza sobre los tratamientos efectuados con sus datos sanitarios.

En el seminario sobre Administración digital que, organizado por el CEPC, tuvo lugar el 4 de octubre de 2022, buena parte de las intervenciones abordaron el modo en que la creciente utilización de las nuevas tecnologías por parte de las administraciones públicas repercute en los derechos de la ciudadanía. A lo largo de esa jornada se puso de manifiesto que no se trata solamente de determinar cómo puede —o, incluso, debe— redefinirse el contenido de los tradicionales derechos fundamentales para garantizar su vigencia en el entorno digital sino también de reconocer e implantar nuevos y específicos derechos conectados directamente con la actuación de los poderes públicos en el *ciberespacio*. Por otro lado, en la medida en que las diferentes administraciones, cada vez más, desempeñan sus funciones y prestan los servicios públicos a través de decisiones basadas, total o parcialmente, en algoritmos, el desarrollo de la Administración digital supone una verdadera prueba de resistencia para la virtualidad del derecho de acceso a la información consagrado en la legislación reguladora de la transparencia: al fin y al cabo, el «contenido esencial» de esta legislación reside en asegurar que la ciudadanía esté en condiciones de conocer cómo se toman las decisiones atinentes a la cosa pública. De estas y otras cuestiones conexas debatidas en aquel seminario se hacen eco las diversas colaboraciones que integran este libro.

Manuel Medina es catedrático de Derecho Constitucional de la Universidad de Sevilla. Ha sido letrado del Tribunal Constitucional (1994-1998), director de la Fundación Democracia y Gobierno Local (2004-2010) y director del Consejo de Transparencia y Protección de Datos de Andalucía (2016-2020). Entre otros, ha recibido el Premio Jesús María de Leizaola 1990 (Gobierno vasco) y el Premio Nicolás Pérez Serrano 1991 del Centro de Estudios Constitucionales. Los derechos fundamentales constituyen una de sus principales líneas de investigación. Con independencia de recientes publicaciones relativas al derecho a la protección de datos personales y a la libertad de información, cabe destacar entre sus trabajos, como aproximaciones a la teoría general de los derechos, *La vinculación negativa del legislador a los derechos fundamentales,* McGraw-Hill, 1996 y «Grundrechte in Spanien», *Handbuch der Grundrechte in Deutschland und Europa,* Band X (Merten/Papier, Hrsg.), C. F. Müller, 2017.

GOBIERNO ABIERTO
GOBIERNO DE ESPAÑA
MINISTERIO DE LA PRESIDENCIA, RELACIONES CON LAS CORTES Y MEMORIA DEMOCRÁTICA
U23
CENTRO DE ESTUDIOS POLÍTICOS Y CONSTITUCIONALES