UNIVERSIDAD DE SALAMANCA

FACULTAD DE DERECHO

DEPARTAMENTO DE DERECHO ADMINISTRATIVO, FINANCIERO Y PROCESAL

PROGRAMA DE DOCTORADO

«ADMINISTRACIÓN, HACIENDA Y JUSTICIA EN EL ESTADO SOCIAL»

VNiVERSiDAD D SALAMANCA

TESIS DOCTORAL

CAMBIO DE PARADIGMA EN LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL Y SU INTERRELACIÓN CON LA SOCIEDAD DIGITAL

DOCTORANDO

D. JOSÉ LUIS DOMÍNGUEZ ÁLVAREZ

INVESTIGADOR BENEFICIARIO DEL PROGRAMA DE FORMACIÓN DEL PROFESORADO UNIVERSITARIO FPU DEL MINISTERIO DE EDUCACIÓN CULTURA Y DEPORTE

FPU2017-01088

DIRECTOR

PROF. DR. D. MARCOS M. FERNANDO PABLO

TUTOR

PROF. DR. D. DANIEL TERRÓN SANTOS

SALAMANCA, OTOÑO 2022

RESUMEN

La investigación tiene por objeto profundizar en el análisis de las abruptas transformaciones que ha experimentado el derecho fundamental a la protección de datos de carácter personal en el seno de las Administraciones públicas en los últimos tiempos, ante la paulatina incorporación y aplicación del recurso tecnológico en las diferentes actuaciones administrativas. La dificultosa tarea plantea un detallado viaje por los distintos hitos jurídicos que han contribuido al alumbramiento de un derecho fundamental fuertemente administrativizado, con el propósito de dar cuenta de las dispares y profundas transformaciones que este instituto jurídico ha sufrido fruto del transcurso del tiempo y de las sucesivas oleadas digitalizadoras, las cuales han forzado su reinvención en numerosas ocasiones, a medida que se incrementaba el catálogo de amenazas y nuevos desafíos.

No obstante, como habrán comprobado el presente estudio no está concebido para realizar una simple revisión del estado del arte de la cuestión. Fruto de este anhelo, la tesis doctoral huye expresamente de los cómodos esquemas empleados con carácter general para acometer el análisis de este derecho fundamental, con el firme propósito de servir a un loable objetivo, que no es otro que el de contribuir modestamente, como diría RUBÍ NAVARRETE, Adjunto a la Dirección de la Agencia Española de Protección de Datos, a «favorecer el conocimiento de las trincheras de la protección de datos de carácter personal». Por esta razón, no nos limitamos únicamente a examinar el más de un siglo que separa la formulación teórica primigenia de la protección de la vida privada elaborada por WARREN y BRANDEIS, del poderoso Reglamento General de Protección de Datos o del esperado Paquete Digital Europeo.

Así pues, la investigación que hoy defendemos, imbuida quizá por ese espíritu humanista que imprime el estrecho contacto con las aulas del Estudio salmantino, pretende traspasar los muros universitarios y ofrecer una relectura, desde el prisma de los procesos de digitalización y modernización de las Administraciones públicas, eminentemente práctica y actualizada de un derecho fundamental que está llamado a ser el instituto básico para la plena eficacia y garantía del conjunto de derechos y libertades fundamentales reconocidos constitucionalmente, erigiéndose además como la piedra angular del Estado social y democrático de Derecho ante la (r)evolución digital.

Defender abiertamente esta premisa exige huir conscientemente de la visión buenista que envuelve el análisis del fenómeno de la transformación tecnológica

de nuestras sociedades entre una gran parte de la doctrina iuspublicista, ya que si bien es cierto que la apresurada transición digital de las estructuras sociales y económicas está dibujando innumerables ventanas de oportunidad para el conjunto de la población, no es menos cierto que esta rápida incursión de las tecnologías disruptivas ha evidenciado la urgente necesidad de contar con un sólido marco ético y jurídico que permita regular las ventajas, potencialidades y riesgos que entraña la (r)evolución digital, situando la dignidad de la persona en el centro de cuantos esfuerzos metodológicos se destinen a la búsqueda de soluciones normativas innovadoras que permitan caminar hacia la consecución del ansiado humanismo tecnológico.

Esta apremiante cuestión exige una minuciosa labor jurídica orientada no solamente a la articulación de garantías que permitan salvaguardar la plena vigencia y efectividad del elenco de derechos fundamentales ya reconocidos, sino también la identificación de reformas legales necesarias, así como de aquellas lagunas jurídicas que requieran una regulación adicional para otorgar seguridad jurídica, elemento indispensable que debe vehicular cualquier intento de fomento de la innovación digital.

A tal fin, nuestra investigación se encuentra dividida en cuatro grandes capítulos, los cuales están engarzados de tal manera que permiten atesorar no solamente un profundo conocimiento del derecho fundamental de la protección de datos de carácter personal, sino también identificar las nociones esenciales del sustrato tecnológico que subyace bajo la etiqueta de IA, así como de los procesos de digitalización y datificación experimentados por las Administraciones públicas, al objeto de poder deslindar con claridad los numerosos impactos que la tecnificación de la acción administrativa, en primer término, y la automatización y el recurso a la inteligencia artificial en el momento actual están ocasionando sobre la esfera privada de los particulares. Se pretende, por tanto, abordar tres grandes cuestiones examinadas por la doctrina hasta la fecha de forma desagregada, dispersión solamente alterada por algunos estudios puntuales sobre la materia realizados por extraordinarios académicos de la talla de PIÑAR MAÑAS.

Así, en el Capítulo primero analizamos el tránsito de los primeros instrumentos internacionales en materia de protección de datos de carácter personal a la configuración de un verdadero ordenamiento europeo de la privacidad. Para ello, en primer término, se realiza un sucinto análisis de aquellos textos normativos internacionales que contribuyeron a sentar las bases y principios esenciales del actual sistema europeo de tutela jurídica de la protección de la privacidad para acto seguido, detenernos en el estudio pormenorizado de todos y cada uno de los

instrumentos normativos que han contribuido al avance, perfeccionamiento y posterior consolidación del derecho a la protección de datos de carácter personal en el continente europeo, escenificando la transfiguración de esta garantía, la cual pasa de ser una simple exigencia más para el correcto funcionamiento del mercado común europeo a convertirse en un derecho fundamental autónomo, tal y como se desprende del art. 8 de la Carta de Derechos Fundamentales de la Unión Europea.

Especial mención requiere el análisis del actual marco normativo europeo de privacidad, presidido por el todopoderoso Reglamento General de Protección de Datos, entre cuyas numerosas innovaciones sobresalen la irrupción de la responsabilidad proactiva, la sustancial ampliación de los derechos subjetivos de los interesados, la preponderancia de la privacidad desde el diseño y por defecto, la instauración del registro de actividades de tratamiento o la introducción de la figura del delegado de protección de datos, las cuales han traído consigo un verdadero giro copernicano en la regulación de la materia que ha terminado removiendo los cimientos del tradicional esquema de cumplimiento normativo al que plácidamente estaban acostumbradas las Administraciones públicas.

También aparecen reflejados en este trabajo algunos hitos normativos posteriores, cuya vinculación con la esfera de la protección de datos está más que justificada. Nos estamos refiriendo a la Directiva (UE) 2019/1024, relativa a los datos abiertos y la reutilización de la información del Sector público y al Reglamento (UE) 2022/868, relativo a la gobernanza europea de datos, los cuales generan un buen número de interrogantes desde el prisma de la privacidad, toda vez que representan una serie de concesiones en favor del mercado único digital que pueden desdibujar los contornos propios del modelo europeo de protección de datos personales.

Más relevantes e innovadoras resultan las reflexiones esbozadas acerca del carácter poliédrico del sistema europeo de protección de datos, donde se incide en dos elementos vehiculares que representan, a nuestro buen saber y entender, el núcleo irreductible de la actual regulación contenida en el RGPD. Nos estamos refiriendo, como no podía ser de otra manera, al principio de responsabilidad proactiva y al enfoque de riesgo, premisas que permiten diseñar un marco normativo flexible, capaz de adaptarse y resistir al fenómeno de la obsolescencia normativa que imprime la vertiginosa transformación tecnológica. También se reflejan en este epígrafe una serie de importantes reflexiones acerca del futuro del sistema europeo de protección de datos de carácter personal, a la luz de la aprobación de diversos instrumentos que darán cobertura al esperado Paquete Digital Europeo. Finalmente, se examina en este primer capítulo la fuerza

expansiva del RGPD, el cual está ejerciendo una fuerte influencia en el contexto internacional como motor de modernización de diversas legislaciones. Con la finalidad de evidenciar la relevancia de este «efecto Bruselas», se acomete el análisis del espacio iberoamericano de protección de datos, la creación de la mayor área mundial de flujos de datos seguros tras la adopción de la Decisión de adecuación de Japón y el estudio de la Ley de Protección de la Información Personal de la República Popular China, la cual, sorpresivamente, guarda una extraordinaria similitud con el RGPD.

Revisada la configuración del poderoso ordenamiento europeo de privacidad, dedicamos el Capítulo segundo de nuestra investigación a hacer lo propio con el esquema normativo nacional de protección de datos de carácter personal, destacando sus numerosas fortalezas, sus deficiencias y márgenes de mejora, mediante la propuesta de una serie de ideas-fuerza que deberían tenerse en cuenta en la futura revisión de los instrumentos jurídicos encargados de ordenar la cuestión, de la mano de la experiencia acumulada por la Agencia Española de Protección de Datos, la cual se esconde tras buena parte de las innovaciones jurídico-administrativas que han situado a nuestro modelo de protección de datos personales a la cabeza de la Unión Europea.

Para ello, en primer término, se realizan una serie de consideraciones acerca de la importante y vanguardista referencia a la informática introducida en la Constitución española de 1978 para, acto seguido, profundizar en el carácter jurisprudencial del nacimiento de la protección de datos personales como derecho autónomo. Seguidamente, centramos nuestra atención en el estudio del entramado de normas impulsado por nuestro legislador con el propósito de dar desarrollo al derecho fundamental a la protección de datos de carácter personal, examinando al detalle los avances que presenta cada norma con respecto a su predecesora, y deteniendo nuestra mirada en la novísima Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Asimismo, encuentran cobijo en este segundo capítulo dos importantes y novedosas propuestas para el futuro de la protección de datos de carácter personal. En primer lugar, destaca la fervorosa defensa de la inclusión de la dimensión de protección de datos personales en la iniciativa legislativa, mediante la modificación de la ordenación que da cobertura jurídica a la memoria de análisis de impacto normativo, con el propósito de incluir un estudio sistematizado del impacto que en el derecho fundamental a la protección de datos personales de los interesados ejercerán los distintos tratamientos de datos previstos en los

diferentes instrumentos legislativos impulsados. No obstante, conviene precisar que nuestra pretensión no se limita única y exclusivamente a incorporar la dimensión de la protección de datos de carácter personal en la estructura y contenido de la MAIN sino también a publicitar las garantías específicas que resulten de dicho análisis, mediante la inclusión en el propio texto articulado de un precepto concreto relativo a la protección de datos de carácter personal.

En segundo lugar, destaca la urgencia de articular garantías jurídicas efectivas que permitan dotar de efectividad al elenco de nuevos derechos digitales reconocidos a propósito de la promulgación del Título X LOPDGDD y la adopción de la afamada Carta de Derechos Digitales, los cuales si bien es cierto que constituyen un ejemplo extraordinario de la conveniencia de avanzar en el establecimiento de un conglomerado de derechos que permitan garantizar la subordinación de la tecnología al individuo y preservar la dignidad de la persona frente al imperio de la digitalización, no cuentan con fórmulas de intervención administrativa tangibles que permitan impulsar verdaderamente una digitalización humanista efectiva.

En el Capítulo tercero, dedicado al análisis de los nuevos confines de la protección de datos de carácter personal se realiza un importante esfuerzo por desenmarañar los requerimientos técnicos que sustentan el avance de la inteligencia artificial y las decisiones automatizadas. Para ello, se examinan, en primer término, las diferentes oleadas digitalizadoras de la sociedad, prestando especial atención a fenómenos tales como el machine learning, el deep learning o el procesamiento del lenguaje natural y sus múltiples manifestaciones. También se acomete el estudio del ciclo de vida de las herramientas de inteligencia artificial y se esbozan una serie de premisas esenciales para garantizar la adecuación al RGPD de aquellos tratamientos de datos personales que empleen estas novedosas invenciones.

De igual forma, se aborda el creciente protagonismo de la ética digital, incidiendo en la necesaria «reserva de humanidad», la conveniencia de combatir los sesgos algorítmicos y las dificultades y potencialidades propias de la explicabilidad de la inteligencia artificial. También se incluyen un buen número de reflexiones acerca de la gestión del riesgo para los derechos y libertades fundamentales de la ciudadanía, prestando especial atención a la afectación que los sistemas algorítmicos ocasionan en el concreto ámbito de la privacidad, la quiebra del principio de no discriminación, la erosión de la tutela judicial efectiva o en la alteración del binomio libertad-seguridad.

La gobernanza algorítmica es otro de los temas de estudio que se incardinan en este capítulo tercero, cuyo reflejo trasciende el establecimiento de límites y controles a la inteligencia artificial, contemplando además el protagonismo que posee la

Agencia Española de Protección de Datos ante la algoritmización de la sociedad y el diseño de nuevas garantías institucionales frente al avance de la transformación digital.

De igual forma, se acomete el estudio de los nuevos instrumentos normativos en materia de inteligencia artificial, para lo cual se realiza un estudio comparado de la Propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de Inteligencia Artificial y otras iniciativas internacionales destinadas a embridar el despliegue de esta poderosa tecnología, como son las Opiniones orientativas sobre el fortalecimiento de la gobernanza integral de los algoritmos del servicio de información de Internet adoptadas por la República Popular China y la Ley de Responsabilidad Algorítmica de Estados Unidos.

Como cierre de nuestra tesis doctoral, se dedica el Capítulo cuarto a dilucidar la situación que atraviesa la protección de datos de carácter personal en el seno de las distintas Administraciones públicas, haciendo especial énfasis en el cambio de paradigma que supone, así como en las ventajas, potencialidades y desafíos que entraña la creciente proliferación de procesos de automatización y el exponencial recurso a la inteligencia artificial dentro del Sector público, extremo que justifica los esfuerzos destinados a conocer el funcionamiento de esta poderosa solución tecnológica en el capítulo inmediatamente anterior.

A tal fin, se examina el marco normativo que ha guiado la transformación digital de las Administraciones públicas durante los últimos decenios, con el propósito de identificar, en primer término, las deficiencias e incongruencias propias del proceso de despliegue de la administración electrónica y, acto seguido, las carencias que laten en el corazón de la vacua e insuficiente regulación que en nuestros días está dando pie al impulso de la administración automatizada sin las debidas garantías para los ciudadanos o administrados.

Asimismo, se intenta clarificar la repercusión que la transformación digital de las Administraciones públicas ocasiona en la esfera privada de la ciudadanía, lo que nos lleva a destacar la importancia capital que ostentan la información y los datos personales como principal activo del poder público, al tiempo que se profundiza en los usos que las Administraciones públicas hacen tanto de las decisiones automatizadas como de otro conjunto de importantes y variadas tecnologías (cookies y tecnologías de seguimiento, redes sociales, cloud computing, big data, Blockchain y tecnologías de riesgo distribuido, metaverso, etc.).

Pero sin lugar a dudas, el pasaje más relevante de este capítulo es el relativo al estudio de lo que hemos denominado como «régimen de (ir)responsabilidad de las

Administraciones públicas en materia de protección de datos», donde mediante el análisis exhaustivo de las más de quinientas resoluciones sancionadoras impuestas durante la última década por la Agencia Española de Protección de Datos a las instituciones públicas se analizan los perniciosos efectos que la excepción al régimen general de responsabilidad y la problemática del apercibimiento de las autoridades públicas están propiciando en nuestros días, se dibujan los contornos del necesario reconocimiento de la responsabilidad patrimonial de las Administraciones públicas frente a la vulneración de los derechos de la privacidad de los particulares y se identifican los principales desafíos pendientes de abordar para garantizar la correcta tutela de la protección de datos personales en el seno de las Administraciones públicas.

Para finalizar, se incorporan una serie de valiosas reflexiones acerca de los riesgos que comporta la transformación digital del Sector público desde el prisma de la ciberseguridad y su estrecha relación con la privacidad. Bajo la premisa de que sin protección de datos personales no existe ciberseguridad se acomete la revisión de la génesis y evolución de la ciberseguridad en la Unión Europea, la conveniencia de fortalecer la Estrategia de Ciberseguridad española y la actuación de los elementos institucionales que velan actualmente por la seguridad e integridad de los sistemas de información del poder público, en un contexto marcado por el creciente impacto de las amenazas híbridas y la transformación del modelo tradicional de seguridad.

Con todo ello, aún a riesgo de la rápida obsolescencia a la que está expuesta la presente investigación, fruto de la celeridad con la que se suceden los acontecimientos en el ámbito tecnológico y la hipertrofia normativa que caracteriza este concreto ámbito del ordenamiento jurídico, creemos estar en disposición de afirmar que la presente tesis doctoral ofrece una visión completa no solo del estadio regulatorio en el que se encuentra actualmente la tutela jurídica de la protección de datos de carácter personal y su implantación en el ecosistema de Administraciones públicas, sino también de identificar y ofrecer respuestas innovadoras que permitan revertir sus principales deficiencias, al tiempo que contribuye a vislumbrar los principales desafíos y la senda por la que transitará este importante instituto jurídico en los años venideros, cuestiones todas ellas que justifican la extensión de la obra y que dan buena cuenta del desafío normativo al que nos enfrentamos como sociedad, pues como recuerda CARISSA VÉLIZ, «[e]s demasiado tarde para impedir que se desarrolle la economía de los datos, pero no es demasiado tarde para recuperar nuestra privacidad. Nuestros derechos civiles están en juego. Las decisiones que tomemos sobre la privacidad hoy y en los próximos años moldearán durante décadas el futuro de la humanidad».

CONCLUSIONES

Del capítulo primero de esta investigación, dedicado a analizar la evolución de los instrumentos internacionales en materia de protección de datos de carácter personal y la configuración del sistema europeo de tutela jurídica de la privacidad, se han extraído las siguientes conclusiones:

I. El derecho a la protección de datos de carácter personal ha experimentado un largo e intenso recorrido durante la segunda mitad del siglo XX y las dos primeras décadas del siglo XXI, hasta llegar a asentarse en nuestro ordenamiento jurídico con una rapidez inusitada. En su alumbramiento y posterior reconocimiento como derecho autónomo puede percibirse la impronta de una serie de precedentes internacionales orientados a garantizar la tutela de este bien jurídico. De esta forma, documentos emblemáticos de profundo calado, tales como la Declaración Universal de los Derechos Humanos, el Convenio Europeo o el Pacto Internacional de los Derechos Civiles y Políticos para la Protección de los Derechos Humanos y Libertades Fundamentales, entre otros, contribuyeron a sentar las bases sobre las que, tiempo después, la Unión Europea acometerá la construcción del más ambicioso sistema de tutela jurídica de los derechos de la privacidad existente hasta la fecha.

II. El continente europeo se ha caracterizado, desde mediados de los años sesenta del pasado siglo, por abanderar la protección de los derechos fundamentales y las libertades públicas de la ciudadanía mediante el establecimiento de un marco legislativo preciso, orientado a embridar los claroscuros del fenómeno tecnológico, unificar las pretensiones de los distintos actores implicados en la primigenia tecnificación de las sociedades europeas de la época y, especialmente, capaz de ofrecer un conjunto de medios efectivos de protección de los derechos y libertades fundamentales del conjunto de la ciudadanía europea. De esta forma, la Unión Europea ha llevado a cabo una labor extraordinariamente diligente caracterizada con frecuencia, hasta la llegada del Reglamento General de Protección de Datos, por el establecimiento de lo que podemos llamar «legislación genérica de mínimos», lo que ha supuesto en la práctica el incremento progresivo de los estándares de protección de los datos personales en los Estados miembros, produciendo una auténtica ola homogeneizadora, tanto de los medios de protección, como de los mecanismos adoptados para garantizar la plena eficacia de los derechos de la ciudadanía en relación con el tratamiento de sus datos personales.

III. El desarrollo del derecho a la protección de datos de carácter personal es el relato de un éxito mayúsculo del proyecto de integración europea. Esta dificultosa empresa no ha estado exenta de controversia y ha exigido numerosos esfuerzos por parte de todos los actores implicados, sin los cuales no habría sido posible transitar el pedregoso camino que ha recorrido la tutela jurídica de la privacidad en el continente europeo. Esta garantía ha pasado de ser, en un primer momento, una exigencia instrumental más al servicio de la edificación del mercado único común (art. 100A TCE), a convertirse en un derecho fundamental autónomo (art. 8 CE) que, en nuestros días, se erige como la piedra angular para la defensa de la dignidad de la persona ante los envites de la transformación digital.

IV. La llegada del Reglamento General de Protección de Datos ha supuesto un giro copernicano en materia de protección de datos personales con respecto a la situación anterior. Dicho hito normativo introduce, a veces directamente, a veces de forma soterrada, un nuevo modelo de protección de datos personales sustentado sobre un novedoso enfoque de riesgo y una premisa sumamente innovadora, como es la necesidad de avanzar hacia el uso responsable de la información de carácter personal. Este cambio de paradigma puede percibirse con meridiana claridad en cuestiones tan relevantes como la irrupción del principio de *accountability* o responsabilidad proactiva, la inclusión de los principios de privacidad desde el diseño y por defecto, la aproximación a la protección de datos basada en el análisis de riesgos, la incorporación de la figura del delegado de protección de datos, el fortalecimiento de los códigos de conducta, la exigencia de llevar a cabo un registro de las actividades de tratamiento, la regulación de medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado y un largo etcétera de cuestiones que producen una auténtica catarsis en el modelo europeo de protección de datos de carácter personal.

V. La batalla entre la privacidad y el avance tecnológico es una confrontación desigual. Conscientes de la celeridad con la que la innovación tecnológica evoluciona y del importante riesgo de obsolescencia al que están expuestos los instrumentos normativos que aspiran a ordenar esta escurridiza realidad, las Instituciones europeas destinaron innumerables esfuerzos a diseñar un sistema de tutela jurídica del derecho fundamental a la protección de datos de carácter personal dúctil y maleable, capaz de adaptarse a los innumerables desafíos que plantea la transformación digital de las estructuras sociales y económicas. Esta ardua y laboriosa tarea se acometió mediante la instauración,

en el seno del Reglamento General de Protección de Datos, del principio de responsabilidad proactiva o accountability (art. 5.2 RGPD) como sustento del nuevo marco normativo, haciendo propia una aspiración que las autoridades de protección de datos llevaban persiguiendo y defendiendo con ahínco desde finales de la primera década del siglo XXI. De esta forma, el RGPD se erige como una norma-código con vocación de permanencia en el tiempo, capaz de poner coto y hacer frente a las (i)lógicas invenciones de quienes abogan por el impulso desbocado del fenómeno tecnológico.

VI. El Reglamento General de Protección de Datos ha establecido los estándares de protección de datos personales más ambiciosos de las legislaciones en materia de privacidad existentes hasta la fecha. Más allá de la efectividad de sus reglas de aplicación extraterritorial por las que organizaciones ubicadas fuera de la Unión Europea pueden quedar sujetas a su aplicación (art. 3.2 RGPD), incluido su régimen sancionador, lo cierto es que el Reglamento ha provocado una oleada de reformas normativas que traspasan las fronteras europeas. Este fenómeno, conocido como efecto Bruselas, ha permitido en último término que el RGPD se haya convertido en el motor de modernización de la legislación en materia de privacidad de una pluralidad de terceros Estados, incluso en algunos casos, hasta llegar a alcanzar latitudes que distan extraordinariamente de los principios, derechos y valores que dan forma al proyecto europeísta, como ocurre en el supuesto de la República Popular China.

VII. La paulatina aprobación del Paquete Digital de la Unión Europea plantea multitud de interrogantes y desafíos para la pervivencia del sistema europeo de protección de datos de carácter personal, tal y como lo conocemos en nuestros días. Las sucesivas propuestas normativas están plagadas de multitud de lagunas que, de forma sistemática, desoyen las normas y principios básicos de protección de datos de carácter personal. Esta problemática no es nueva, pero no por ello menos alarmante. En los últimos años estamos asistiendo, de forma velada, a la alteración de las prioridades del proyecto de integración europea. Los derechos y libertades fundamentales del conjunto de la ciudadanía europea están pasando a un discreto segundo plano, con lo que ello supone para la pervivencia del viejo Estado de Derecho, fruto de la virulenta incursión que las grandes corporaciones tecnológicas están ejerciendo en las Instituciones europeas so pretexto de avanzar con celeridad hacia la necesaria consolidación del mercado único digital.

Por su parte, del capítulo segundo de este estudio, el cual se ha destinado al examen del asentamiento, consolidación y perfeccionamiento de la protección de datos personales en el ordenamiento jurídico interno, rescatamos las siguientes conclusiones:

VIII. Frente a la creencia mayoritaria, la Constitución española de 1978, aun haciendo una difusa referencia a la informática, no contempla en modo alguno la protección de datos de carácter personal como derecho fundamental. No será, hasta la STC 254/1993 cuando se mencione por vez primera la celebérrima libertad informática, entendida esta como derecho fundamental autónomo, cuyo origen se encuentra en la dignidad de la persona (art. 10.1 CE) y con clara interacción con el derecho a la intimidad (art. 18.1 CE), artículos que ofrecen el soporte constitucional necesario para la elaboración de una nueva estructura, un nuevo derecho fundamental, autónomo, distinto, con finalidades específicas, el derecho a la protección de datos de carácter personal, tarea que no se materializará hasta recién estrenado el siglo XXI, con la llegada de la STC 292/2000.

IX. Pese a la falta de premura del legislador español a la hora de adoptar los instrumentos pertinentes para salvaguardar, de forma efectiva, la intimidad y la privacidad del conjunto de la ciudadanía frente al avance de la *informática*, en desarrollo de la previsión constitucional consagrada en el art. 18.4 de nuestra Carta Magna, lo cierto es que la protección de datos de carácter personal ha experimentado un avance extraordinario en las últimas cuatro décadas, gracias al despliegue del ordenamiento comunitario en la materia, la labor desarrollada por instituciones fundamentales como la Agencia Española de Protección de Datos y la dedicación constante de extraordinarios académicos. Todo ello ha permitido situar a nuestro país como un auténtico referente a la hora de velar por la garantía efectiva de la tutela jurídica de la protección de datos de carácter personal, lo que nos ha permitido incluso liderar algunas de las grandes conquistas recientes en la materia, entre las que destacan por su especial repercusión y trascendencia, el reconocimiento del derecho al olvido, la articulación de un poderoso régimen sancionador o el impulso del pionero Canal Prioritario.

X. La promulgación de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales tenía como propósito no solamente fortalecer la tutela jurídica de la protección de datos de carácter personal, sino también ampliar de manera considerable la esfera personal de la ciudadanía mediante el reconocimiento de un nuevo marco de protección de la dignidad de la persona ante el avance digital. Este jalón normativo, cuyo

contenido pretende ir más allá de las fronteras propias de la protección de datos personales, al apostar de forma decidida por la introducción de aspectos reguladores en determinados elementos que se vinculan a los derechos digitales de la ciudadanía, ha estado rodeado de polémica y sucesivas contradicciones de sus inicios. Entre sus pasajes más sombríos destaca la introducción, por medio de su disposición final tercera, de un cambio sustancial y sumamente peligroso de la Ley Orgánica 5/1985, de 19 de junio, del Régimen Electoral General, en forma de un nuevo art. 58.bis, el cual permite sin previo aviso que los partidos políticos puedan recopilar datos personales relativos a las opiniones políticas de las personas, vaciando de contenido, en la práctica, buena parte de las previsiones contenidas en la nueva regulación de protección de datos de carácter personal, en lo que respecta a las categorías especiales datos. Este precepto que fue duramente criticado por los expertos en privacidad, matizado por la Agencia Española de Protección de Datos mediante la elaboración de la primera circular adoptada por la Institución con la finalidad de minimizar los posibles daños derivados de su aplicación ante la proximidad de comicios electorales, terminó siendo declarado inconstitucional poco más tarde por el Alto Tribunal fruto de un recurso planteado por el Defensor del Pueblo.

XI. Si bien es cierto que la actual regulación en materia de protección de datos de carácter personal constituye la referencia indiscutible en la que mirarse, cuando han transcurrido más de cuatro años desde la plena aplicación del RGPD y la LOPDGDD comienzan a entreverse una serie de lagunas o fallas normativas que están erosionando el poderoso esquema regulador orquestado en el continente europeo con el propósito de garantizar la tutela jurídica de la privacidad. Entre estas debilidades pueden destacarse cuestiones tales como que el modelo europeo de protección de datos personales se caracteriza por estar pensado por y para los grandes prestadores de servicios digitales, que existe una clara ausencia de previsiones orientadas a facilitar el cumplimiento normativo de las pequeñas y medianas empresas que no realizan tratamientos de riesgo, que se requiere acometer una mayor precisión terminológica y un mayor espíritu armonizador, que habría sido conveniente establecer un catálogo mínimo de medidas de privacidad en lugar de fiar por completo el sistema europeo de protección de datos personales al enfoque de riesgo, que reviste carácter urgente repensar el sistema de gobernanza europeo de privacidad y la modificación del mecanismo de ventanilla única que late en el corazón del Reglamento europeo o que habría sido conveniente atemperar el entusiasta protagonismo del delegado de protección de datos, entre otras muchas cuestiones.

XII. Examinada la prodigiosa maraña normativa que envuelve en la actualidad el derecho fundamental a la protección de datos de carácter personal, a la que hay que añadir la prolífica producción legislativa sectorial que ejerce un impacto directo en la esfera privada de las personas físicas, se constata la necesidad de repensar la técnica legislativa y reformar el Real Decreto 931/2017, de 27 de octubre, por el que se regula la Memoria del Análisis de Impacto Normativo, con la finalidad de incorporar la dimensión de la protección de datos de carácter personal en la iniciativa normativa del Estado. En este sentido, se defiende abiertamente la necesidad de que, parte del legislador, al introducir regulaciones en nuestro ordenamiento jurídico que tengan especial trascendencia en los tratamientos de datos de carácter personal, se proceda previamente a un análisis de los riesgos que puedan derivarse de los mismos, incluyendo en la citada Memoria del Análisis de Impacto Normativo un estudio sistematizado del impacto que en el derecho fundamental a la protección de datos personales de los interesados han de tener los distintos tratamientos de datos que prevé la ley. Adicionalmente, conviene precisar que nuestra pretensión no se limita única y exclusivamente a incorporar la dimensión de la protección de datos de carácter personal en la estructura y contenido de la referida Memoria, sino también a publicitar las garantías específicas que resulten de dicho análisis, mediante la inclusión de un precepto concreto relativo a la protección de datos de carácter personal en el propio texto articulado de los futuros instrumentos jurídicos.

XIII. La promulgación de la LOPDGDD y la adopción de la Carta de Derechos Digitales constituyen un ejemplo extraordinario de la conveniencia de avanzar en el establecimiento de un conglomerado de derechos que permitan garantizar la subordinación de la tecnología al individuo y preservar la dignidad de la persona frente al imperio de la digitalización. Sin embargo, aún persiste numerosas zonas sombrías tales como la necesidad de articular nuevas formas de intervención administrativa que permitan impulsar una digitalización humanista efectiva, la urgencia de clarificar la naturaleza jurídica de estos nuevos derechos digitales e incluso la conveniencia de afrontar la constitucionalización de estas nuevas garantías de la ciudadanía para blindar la seguridad jurídica y maximizar la confianza de la población en el mundo digital. A este respecto, conviene precisar que los derechos digitales contemplados en el Título X de la LOPDGDD no contemplan garantía alguna y el legislador no encomienda su tutela a ningún elemento institucional concreto, dotado de los poderes públicos pertinentes para garantizar su efectividad. Solamente el art. 5.2 del Real Decreto 389/2021, de 1 de junio, por el que se aprueba el Estatuto de la Agencia Española de Protección de Datos atribuye a

dicha Agencia la función de supervisar la aplicación de la normativa vigente en materia de garantía de los derechos digitales contemplados en los artículos 89 a 94 LOPDGDD.

XIV. El advenimiento del nuevo marco jurídico europeo de protección de datos de carácter personal ha venido acompañado de la renovación del añejo Estatuto de la Agencia Española de Protección de Datos, instrumento normativo que tiene por objeto modernizar la organización y adaptar la acción administrativa del elemento institucional encargado de salvaguardar la tutela jurídica de los derechos de la privacidad. Este movimiento lejos de desdibujar el protagonismo de la autoridad de protección de datos, ha traído consigo un fortalecimiento y un sustancial incremento de las competencias de esta última, lo que se ha traducido en la práctica en algunas modificaciones significativas orientadas a fortalecer la seguridad jurídica, fomentar la transparencia, garantizar su independencia, modernizar su estructura o clarificar e incrementar el cuadro de funciones de esta institución capital. Las repercusiones del nuevo texto no se han hecho esperar y el nuevo Estatuto está realizando las funciones de dique de contención durante el actual procedimiento de renovación de los órganos directivos de la Agencia, frente a quienes aviesamente pretenden socavar la independencia de una institución que encarna las notas características del mejor servicio público.

En lo que respecta al capítulo tercero, donde nos adentramos en el estudio de los nuevos confines de la protección de datos personales ante el avance de la inteligencia artificial y las decisiones automatizadas, podemos destacar las siguientes ideas:

XV. Los avances en la potencia informática, la disponibilidad de enormes cantidades de datos y el diseño de nuevos sistemas algorítmicos han permitido un extraordinario despegue de la inteligencia artificial, convirtiéndose en una de las principales prioridades de la Unión Europea, en la medida en que permite impulsar productos y servicios personalizados, baratos y duraderos en sectores esenciales, tales como la economía verde y circular, la maquinaria, la agricultura, la salud, la moda, el turismo, etc. También facilita el acceso a la información, educación y formación, y está llamada a disponer de un papel protagonista en la consecución de los objetivos del Pacto Verde Europeo y la transformación digital de las Administraciones públicas. Sin embargo, la IA genera numerosas dudas entre los usuarios, investigadores, especialistas, autoridades y la propia industria encargada de su desarrollo. En singular, estas preocupaciones se centran en lo que concierne a los aspectos relativos al

cumplimiento normativo, el respeto de los derechos y libertades fundamentales de los interesados (privacidad, igualdad y no discriminación, dignidad, etc.) o la seguridad jurídica de todos los intervinientes en aquellos procesos en los que la innovación digital se erige como componente primordial; cuestiones esenciales que, ante la inacción de los poderes públicos, terminan por constituir un importante freno para el correcto desarrollo tecnológico.

XVI. Con la finalidad de disipar los interrogantes que envuelven el prodigioso avance de las nuevas tecnologías, en especial la IA, es urgente que el poder público ofrezca una respuesta decidida, tendente al establecimiento de un sólido marco ético y normativo que refuerce la protección de los derechos individuales y colectivos, con el propósito de garantizar la inclusión y el bienestar social del conjunto de la ciudadanía. Esta apremiante cuestión exige una minuciosa labor jurídica orientada no solamente a la articulación de garantías que permitan salvaguardar la plena vigencia y efectividad del elenco de derechos fundamentales ya reconocidos, sino también la identificación de reformas legales necesarias, así como de las lagunas normativas que requieran una regulación adicional para otorgar seguridad jurídica, elemento indispensable para el fomento de la innovación digital.

XVII. Maximizar el aprovechamiento de las externalidades positivas que dibuja el avance digital y la inteligencia artificial en el horizonte más próximo exige, necesariamente, garantizar el pleno respeto de los derechos fundamentales y libertades públicas reconocidos, como son la libertad de expresión, la libertad de establecimiento y ejercicio de una actividad empresarial en línea, la protección de datos personales, la intimidad y el derecho al olvido, y la protección de la creación intelectual individual, entre otras. Asimismo, conviene proceder al establecimiento de un conjunto completo de principios digitales que permita informar a los usuarios y orientar a los responsables políticos y a los operadores digitales. Entre estos principios, como mínimo, deberían figurar el acceso universal a los servicios de internet, el entorno en línea seguro y fiable, la educación y las competencias digitales universales, la reserva de humanidad, así como la protección y capacitación de los menores en el espacio en línea.

XVIII. Urge avanzar en el establecimiento de soluciones normativas que permitan delimitar el potencial alcance negativo del desarrollo tecnológico, desde una órbita humanista, supeditando el avance digital al servicio de la sociedad en su conjunto. Todo ello hace que los poderes públicos no puedan asistir impasibles, como meros observadores, a este cambio de paradigma en el que están en juego los derechos y libertades fundamentales de la ciudadanía, especialmente

en lo que se refiere a la dignidad y a la privacidad del individuo, institutos jurídicos que el paso del tiempo y la transformación digital amenazan con desdibujar casi por completo. En este sentido, reviste especial importancia ahondar en el papel protagonista que el Derecho administrativo posee a la hora de contener los perniciosos efectos que los crecientes procesos de digitalización y datificación de la sociedad entrañan para el conjunto de la población.

XIX. Resulta necesaria la toma de decisiones de ética digital anticipando aquellos escenarios que puedan generar riesgos para la privacidad y los derechos y libertades fundamentales restantes, prestando especial atención al potencial que poseen estas tecnologías emergentes, al combinarlas con actuaciones de tratamiento masivo de datos personales y técnicas de *big data*, para permitir la reidentificación de los individuos e invadir la esfera personal de la ciudadanía. Ciertamente, la ética digital persigue proteger valores tales como la dignidad, la libertad, la democracia, la igualdad, la autonomía del individuo y la justicia frente al gobierno de un razonamiento mecánico, lo que la convierte en otro de los elementos capitales a la hora de avanzar en el establecimiento de un desarrollo tecnológico antropocéntrico, ético, sostenible, igualitario y respetuoso con los derechos y valores fundamentales que integran la concepción de ciudadanía europea. En otras palabras, sin las debidas cauciones en materia de ética y privacidad difícilmente se podrá lograr el ansiado humanismo tecnológico y el despegue de la economía digital se verá seriamente mermado. Ante esta tesitura, no parece extraño que la normativa de protección de datos de carácter personal esté llamada a jugar un papel esencial ante los desconocidos horizontes que plantea la innovación tecnológica, convirtiéndose en última instancia en el *dique de contención* encargado de preservar la dignidad de la persona ante un caudal incesante de nuevas amenazas y riesgos envueltos en forma de novedosas aplicaciones o sistemas algorítmicos.

XX. La mayor parte de los sistemas de IA emplean datos personales, lo que significa que la protección de datos se ve afectada de muy diversas maneras y exige la plena aplicación de la regulación vigente en la materia, la cual constituye en la actualidad, como hemos defendido durante la presente investigación, el único instrumento jurídico capaz de embridar eficazmente los desafíos y zonas de riesgo que envuelven el exponencial avance digital, dotar de certidumbre el despliegue de la economía digital y preservar la dignidad de la persona ante los innumerables avatares que dibuja el horizonte tecnológico en el corto y medio plazo. Pese a todo ello, aún existe mucha incertidumbre respecto al verdadero

significado de la toma de decisiones automatizadas y el derecho a una revisión humana ligada al uso de la IA y a la toma de decisiones automatizadas. Por lo tanto, consideramos necesario que el Comité Europeo de Protección de Datos y el Supervisor Europeo de Protección de Datos valoren la posibilidad de aclarar dichos conceptos cuando se haga referencia a ellos en el Derecho de la Unión. Asimismo, los organismos de protección de datos nacionales deben ofrecer una orientación práctica sobre cómo deben adecuarse los usos y fórmulas de inteligencia artificial para cumplir taxativamente las disposiciones normativas en materia de protección de datos de carácter personal.

XXI. Resulta fundamental determinar qué modelo de gobernanza de la IA queremos instaurar en el viejo continente europeo, ya que de esta decisión dependerá no solamente sentar las bases para el desarrollo de esta poderosa tecnología y sus aplicaciones, velando por su integridad, su equidad y su alineación con valores compartidos, y minimizando sus riesgos y efectos indeseados a nivel económico y social, sino también buena parte del futuro marco normativo encargado de regular la IA. Dentro de este sistema de gobernanza algorítmica cobra singular protagonismo el necesario establecimiento de límites y controles a las soluciones de inteligencia artificial, como pueden ser aquellas previsiones destinadas a facilitar la liberalización del código algorítmico, el establecimiento de sistemas de auditorías, el impulso de procesos de evaluación pública, la apuesta por la composición de equipos de desarrollo tecnológico interdisciplinares o la adopción de normas técnicas y estándares en materia de inteligencia artificial.

XXII. El Plan de Recuperación, Transformación y Resiliencia «España puede» contempla entre sus objetivos prioritarios garantizar un proceso de transformación digital plenamente coherente con los valores constitucionales y la protección de los derechos individuales y colectivos. Para ello, la Agenda España Digital 2026 y la Estrategia Nacional de Inteligencia Artificial prevén el establecimiento de una serie de nuevas garantías de carácter instrumental con las que se pretende avanzar en el desarrollo efectivo de esa digitalización humanista que vertebra infinidad de documentos programáticos del conjunto de las Administraciones públicas españolas. Entre estas garantías instrumentales se encuentra el diseño de la Agencia Estatal de Administración Digital y de la Agencia Española de Supervisión de Inteligencia Artificial, medidas que constituye un paso más hacia adelante en la travesía hacia el establecimiento de un verdadero modelo de gobernanza de la IA. Sin embargo, en nuestra opinión, esta decisión es errónea y no comprendemos las razones que abocan al legislador español a optar por el establecimiento de entidades y organismos de nuevo cuño para el desempeño de funciones encaminadas a la

supervisión de los efectos que el desarrollo de los sistemas algorítmicos ejercen sobre los derechos fundamentales de la ciudadanía, en lugar de apostar por el fortalecimiento de la Agencia Española de Protección de Datos, entidad que dispone de una contrastada y extraordinaria experiencia en la materia y que, pese a sus limitados medios, personales especialmente, hasta la fecha había asumido con tesón y diligencia esta dificultosa tarea.

XXIII. La Unión Europea lleva trabajando casi un lustro en el diseño de una suerte de RGPD en materia de inteligencia artificial, con el propósito de adoptar la primera norma jurídica *stricto sensu* propuesta en el campo de la inteligencia artificial y superar las limitaciones propias del enfoque ético que se había impuesto hasta la fecha. No obstante, en el contexto internacional comienzan a vislumbrarse otra serie de intentos normativos, de distinta magnitud y alcance, que conviene igualmente examinar, con el objetivo de dominar la amalgama de iniciativas reguladoras que aspirar a ordenar el vertiginoso despliegue de los sistemas algorítmicos en las diferentes economías y sociedades. Del análisis comparado de todos ellos se constata que la propuesta de regulación europea por la que se establecen normas armonizadas en materia de inteligencia artificial no solamente resulta la iniciativa regulatoria internacional más ambiciosa puesta en marcha hasta la fecha, sino también la más precisa y completa, en vista tanto de la férrea ordenación de requerimientos que deben cumplir los Sistemas de Alto Riesgo de Inteligencia Artificial, como del modelo de gobernanza que aspira a instaurar con el propósito de salvaguardar los derechos y libertades fundamentales de la ciudadanía europea.

Por último, del análisis de los procesos de digitalización y automatización de las Administraciones públicas, pueden extraerse las siguientes conclusiones críticas:

XXIV. El imparable impacto que la (r)evolución digital ejerce sobre buena parte de las instituciones clásicas del Derecho Administrativo y sobre la propia acción administrativa en sí misma nos aboca inexorablemente hacia la necesidad de repensar los esquemas normativos de tal forma que permitan incorporar los innumerables avances propiciados al calor de la cuarta revolución industrial en la actuación cotidiana de las diferentes Administraciones públicas, especialmente en lo que atañe a la mejora y simplificación de las relaciones entre administrados y Administraciones públicas o la modernización de los servicios públicos prestados por estas últimas.

XXV. Actualmente nos encontramos en un momento temporal en el que, sobre la base de la vacua e insuficiente regulación del art. 41 LRJSP, las distintas Administraciones públicas comienzan a acentuar su recurso a poderosos sistemas algorítmicos, algunos de muy dudoso y oscurantista funcionamiento, que entrañan innumerables riesgos para el conjunto de la sociedad y la pervivencia del viejo Estado de Derecho. Transitar hacia la Administración automatizada e inteligente exige no solamente conocer las lagunas y deficiencias normativas que vehicularon la inconclusa instauración de la administración electrónica, con el propósito de no incurrir nuevamente en tales errores, sino también precisar la base legal y las condiciones en las que este despliegue de sistemas algorítmicos puede realizarse con las suficientes garantías para no erosionar los derechos fundamentales y las libertades públicas de la ciudadanía, circunstancia esta última que, por desgracia, parece pasar desapercibida ante la mirada de quienes, lejos de la proporcionalidad, envueltos en la bandera de la eficacia y bajo la cómoda ensoñación de la eficiencia administrativa, promueven la instauración forzosa de una administración automatizada o inteligente sin ni tan siquiera calcular los innumerables riesgos que estas soluciones tecnológicas pueden comportar para el conjunto de la sociedad.

XXVI. El despliegue de la tecnología y la innovación digital está transformando profundamente la forma de actuación de las Administraciones públicas y su relación con los ciudadanos buscando mejorar los tiempos de respuesta, facilitando la accesibilidad, simplificando trámites y ahorrando costes. En efecto, el avance de la Administración Digital, permite ofrecer mecanismos más avanzados para implementar tanto los servicios que prestan a los administrados como aquellos requeridos para su propio funcionamiento interno. Estos servicios son, en muchos casos, tratamientos de datos personales que se implementan haciendo uso de una o varias tecnologías aportando eficacia, eficiencia, disponibilidad, interoperabilidad y la racionalización de los recursos, entre otros beneficios. Como contrapartida, existe un riesgo específico asociado al tratamiento de datos personales por parte de las Administraciones públicas, cuando estas hacen uso de las tecnologías emergentes. Ante esta tesitura, urge delimitar, el alcance que el RGPD y la LOPDGDD poseen en el conjunto de las Administraciones públicas, con la finalidad de identificar las principales transformaciones que el poder público debe acometer para garantizar la plena efectividad de la regulación en materia de protección de datos de carácter personal y abanderar el avance de una digitalización humanista, finalidad esta última que debe guiar la proyección del ordenamiento jurídico vigente sobre la realidad tecnológica.

XXVII. La práctica cotidiana de las Administraciones públicas permite entrever, en términos generales, un acusado retraso en el proceso de adaptación a las exigencias contenidas en la actual regulación encargada de garantizar la tutela jurídica de la protección de datos de carácter personal. Esta perniciosa tendencia se traduce en un incumplimiento normativo flagrante que puede producir una afectación nuclear de los derechos de la privacidad de la ciudadanía, comprometiendo la seguridad de la información que obra en poder de la Administración pública y erosionando el modelo europeo de protección de datos de carácter personal.

XXVIII. La LOPDGDD limita toda sanción a las Administraciones públicas por vulneración de la regulación en materia de protección de datos a un apercibimiento y a dictar «las medidas que proceda adoptar para que cese la conducta o se corrijan los efectos de la infracción que se hubiese cometido», lo que en última instancia se ha convertido en una vía de escape del régimen general de responsabilidad en materia de protección de datos de carácter personal, colisionando con el espíritu del RGPD, el cual se caracteriza por el fortalecimiento del régimen de infracciones y sanciones como presupuesto para garantizar que la vulneración de este derecho fundamental no quede impune en ninguno de los Estados miembros, y por otro, a alcanzar una armonización que impida la existencia de regulaciones dispares. De igual forma, esta vacua concepción de la responsabilidad de la Administración pública ante el incumplimiento de la regulación en materia de protección de datos amenaza con tensionar aún más la labor de inspección y control desempeñada con maestría por la Agencia Española de Protección de Datos, erosionando el principio de responsabilidad proactiva que vehicula el actual modelo europeo de protección de datos de carácter personal y regresando a antiquísimas formas de intervención administrativa, las cuales transitaban sobre un cómodo esquema de cumplimiento normativo (regulación, ejecución, control y sanción) incapaz de hacer frente al conjunto de nuevos desafíos e interrogantes que propicia el avance digital.

XXIX. El contexto normativo vigente exige repensar el régimen de (ir)responsabilidad de las Administraciones públicas ante la vulneración de la actual normativa de protección de datos de carácter personal y transitar hacia el reconocimiento de la responsabilidad patrimonial del poder público derivada de la inobservancia sistemática de las obligaciones comprendidas en el actual sistema europeo de tutela jurídica de la privacidad, de manera similar a lo contemplado en la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y

enjuiciamiento de infracciones penales y de ejecución de sanciones penales, cuyo capítulo VII prevé que los procedimientos de reclamación que se planteen ante las autoridades de protección de datos se rijan por lo establecido en la Ley Orgánica 3/2018, de 5 de diciembre, o, en su caso, por la normativa reguladora de la autoridad de protección de datos correspondiente. En nuestra opinión, esta regulación nos parece sustancialmente más adecuada que el régimen de irresponsabilidad contemplado en el art. 77 LOPDGDD , en el que no se realiza una sola mención a la institución de la responsabilidad patrimonial de las Administraciones públicas para quienes vean vulnerados sus derechos fundamentales, libertades públicas o intereses legítimos, fruto de la inacción y la inobservancia generalizada de las obligaciones en materia de protección de datos.

XXX. La academia debería ser el reducto y la caja de resonancia encargada de la defensa de la dignidad de la persona ante los avatares del fenómeno tecnológico. Ello exige no solamente repensar las tradicionales metodologías docentes e investigadoras asentadas por el transcurso del impertérrito paso del tiempo en estas instituciones de enseñanza superior, sino también redoblar los esfuerzos a la hora de potenciar la educación para la digitalización, todo ello con el propósito de asegurar la adquisición de competencias digitales, presupuesto indispensable para garantizar no solamente el uso responsable y seguro de los medios digitales y la promoción de una auténtica cultura de la privacidad, sino también, y lo que es más importante, como elemento decisivo para alcanzar el ansiado humanismo tecnológico.