ARTÍCULO - Tesis Premiadas Convocatoria de Premios RADE 2024

El carácter poliédrico del actual sistema europeo de protección de datos de carácter personal ante la transformación digital

The Polyhedral Nature of the current European Personal Data Protection System in the Face of Digital Transformation

José Luis Domínguez Álvarez*
Profesor del Área de Derecho Administrativo. Universidad de Salamanca
jldoal@usal.es

RESUMEN

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, estableciendo con ello los estándares de protección de datos más ambiciosos de las legislaciones en materia de privacidad existentes hasta la fecha. Sin embargo, el avance digital plantea novísimos desafíos capaces de tensionar el sistema europeo de privacidad, a cuyo análisis se detiene la presente contribución científica.

PALABRAS CLAVE: Reglamento General de Protección de Datos; transformación digital; innovación; efecto Bruselas; responsabilidad proactiva; enfoque de riesgo.

ABSTRACT

The battle between privacy and technological advancement is an unequal confrontation. Aware of the speed with which technological innovation evolves and of the significant risk of obsolescence to which the normative instruments that aspire to manage this elusive reality are exposed, the European institutions devoted countless efforts to designing a system of legal protection of the fundamental right to the protection of data of a ductile and malleable personal nature, able to adapt to the myriad challenges posed by the digital transformation of social and economic structures, thereby establishing the most ambitious data protection standards of privacy legislation to date. However, the digital advance poses new challenges, capable of stressing the European privacy system, whose analysis is stopped by the present scientific contribution.

KEYWORDS: General Data Protection Regulation; digital transformation; innovation; Brussels effect; proactive responsibility; risk approach.

* El autor fue galardonado con el Premio RADE Ciencias Jurídicas en la Convocatoria de Premios RADE 2023 a la mejor tesis doctoral por su tesis *Cambio de paradigma de la protección de datos de carácter personal y su interrelación con la sociedad digital.*

1. INTRODUCCIÓN

La Real Academia Española define la palabra «poliédrico» como aquella realidad «que posee o manifiesta varias facetas». Cuando nos aproximamos al examen del actual sistema europeo de protección de datos de carácter personal observamos con perplejidad como los innumerables esfuerzos realizados por el legislador europeo y los diferentes Estados miembros acabaron colmatando y reflejándose en la edificación de un marco normativo extraordinariamente innovador, a veces no exento de complejidad, capaz de producir un auténtico cambio de paradigma en la regulación del fenómeno digital y la tutela jurídica de los derechos y libertades fundamentales de la ciudadanía europea en lo que respecta al tratamiento de sus datos personales.

En efecto, la adopción del 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 (RGPD), trajo consigo un auténtico *tsunami normativo*, cuyas oleadas siguen siendo aún hoy en día visibles, dentro y fuera de las fronteras del continente europeo.

Ciertamente, el Reglamento General de Protección de Datos trajo consigo una nueva forma de concebir la protección de datos de carácter personal, mediante la audaz apuesta por la incorporación de nuevas *fórmulas* de cumplimiento normativo, desconocidas hasta el momento en el ordenamiento comunitario de la privacidad.

Surge así un novedoso sistema en el que la flexibilidad y la responsabilidad proactiva, unidas al diseño de un vigoroso régimen sancionador y un entramado institucional compuesto por robustas autoridades independientes de control, son las notas características indispensables, y que, pese a la creencia apriorística mayoritaria en contrario, no han impedido el establecimiento de un poderoso modelo de protección de los derechos de la privacidad, ni tan siquiera en aquellos momentos de tribulación tan complejos como los instantes más aciagos vividos durante la crisis sociosanitaria de la COVID-19. Quizá sea esta incorporación dual de instrumentos de ordenación procedentes de las diferentes tradiciones normativas europeas, la *perfecta* simbiosis entre el Derecho continental europeo y el Derecho anglosajón[1], la que se esconde detrás de su aparente éxito y la que ha

[1] El nacimiento del RGPD representa una respuesta decidida del continente europeo en materia de protección de datos frente a los crecientes desafíos éticos y jurídicos propiciados por el avance de los entornos digitales universalmente implantados. En consonancia con este ecosistema digital representa un nuevo paradigma, o por lo menos, un cambio radical en la manera de concebir la regulación en materia de protección de datos hasta la fecha. La pretensión, espíritu o filosofía que se esconde tras el RGPD no es tanto el de norma de obligado cumplimiento, sino más bien la apuesta por la creación de una cultura de cumplimiento normativo, cuestión de origen netamente anglosajón, que ha obligado a remover los cimientos de la mentalidad romanista imperante hasta el momento, lo

propiciado en última instancia su enorme fuerza expansiva, hasta llegar a convertir el sistema europeo de protección de datos en la referencia indiscutible en la materia en otras latitudes del Planeta.

2. EL ESTABLECIMIENTO DE UNA NORMATIVA DE DATOS DE CARÁCTER PERSONAL FLEXIBLE COMO PREMISA PARA GARANTIZAR LA REGULACIÓN DEL FENÓMENO TECNOLÓGICO

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[2], 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[3]. Esta ardua y laboriosa tarea se acometió mediante la instauración del principio de «responsabilidad proactiva» o «*accountability*» como piedra angular del nuevo marco normativo, haciendo propia una aspiración que las autoridades independientes de protección de datos llevaban persiguiendo y defendiendo con ahínco desde finales de la primera década del siglo XXI[4].

que no está exento de complejidad para algunos actores, como ocurre en el supuesto concreto de las Administraciones públicas españolas.

De esta forma, el RGPD hace una llamada a la responsabilidad, a la auto-responsabilidad de los distintos actores implicados en el tratamiento de datos personales, estableciendo nuevas garantías para los interesados y, lo que es más importante, imponiendo una responsabilidad proactiva a los actores de los tratamientos de datos. Desaparece así un listado exhaustivo y pormenorizado de obligaciones y exigencias legales, en favor de la articulación de un marco de actuación que exige la diligencia de responsables y encargados de tratamiento para su correcto funcionamiento. Esta idea-fuerza se refleja de igual forma en la transfiguración del papel de las autoridades de control, al pretender que pasen de la mera ejecución de actividades de policía a la realización de las funciones propias de un órgano o ente de carácter regulador y colaborador con los implicados en el cumplimiento de la protección de datos personales, sin perder de vista eso si su capacidad sancionadora, la cual se ve fuertemente reforzada.

[2] Hablar de la regulación del fenómeno tecnológico hasta la fecha era hacer alusión obligatoria a la noción de «legislación motorizada». Dicho término fue acuñado por Carl Schmitt para hacer referencia a la rápida evolución del ordenamiento jurídico, en el que se produce una vertiginosa sucesión de normas que, poco tiempo después de entrar en vigor, son derogadas por otras posteriores.

[3] No en vano, la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Derechos Digitales (en adelante, LOPDDG), afirma en su Preámbulo que el RGPD supone la revisión de las bases legales del modelo europeo de protección de datos, más allá de una mera actualización de la normativa vigente.

[4] En efecto, ya en el año 2010 el GT29 propugnaba la necesidad de proceder a la incorporación del aludido principio de «responsabilidad proactiva» a la normativa sobre protección de datos; de manera que se garantizara que fueran los responsables del tratamiento de datos personales los que acreditaran ante las respectivas autoridades de control que habían tomado las decisiones apropiadas y eficaces para garantizar los derechos a la protección de sus

La virtualidad de esta innovación jurídica, consagrada en el art. 5.2 RGPD, reside en la exigencia de que el responsable del tratamiento aplique medidas técnicas y organizativas apropiadas a fin de garantizar y demostrar que el tratamiento que realiza es conforme con el Reglamento[5]. Se trata, por tanto, de instaurar un mecanismo que permita dar un paso más en el compromiso del responsable de datos con sus obligaciones de protección de datos[6]. De esta forma, se exige no solamente cumplir la normativa vigente sino encontrarse, en todo momento, en disposición de demostrar que se ha actuado de modo diligente ante cualquier requerimiento de las autoridades de control o los propios interesados, teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento[7].

Esta actitud proactiva podría resumirse en la manida frase que ha popularizado la Agencia Española de Protección de Datos, según la cual, «no incumplir ya no será suficiente»[8]. Es decir, se trata de asegurar un compromiso elevado de cumplimiento que permita garantizar el necesario respeto a los derechos de los particulares a la vez que facilita el incremento incesante del flujo de datos que circula entre los entes públicos, las corporaciones y los particulares[9].

datos personales. *Vid.* GRUPO DE TRABAJO DEL ARTÍCULO 29, *Dictamen 3/2010, sobre el principio de responsabilidad,* adoptado el 13 de julio de 2010, in totum [WP 173].

[5] En relación con la circunstancia de la adopción o no por el responsable o el encargado del tratamiento de medidas técnicas y organizativas adecuadas, pueden citarse los siguientes pronunciamientos jurisprudenciales: STS 1477/2020, de 10 de noviembre, STS 1620/2020, de 26 de noviembre; así como la Sentencia de la Audiencia Nacional de 30 de abril y 14 de mayo de 2021, que resuelven, en la mayoría de los supuestos, problemas de posible aplicación retroactiva del RGPD.

[6] *Vid.* PIÑAR MAÑAS, J.L. «Hacia un nuevo modelo europeo de protección de datos», en PIÑAR MAÑAS, J.L. (Dir.), Reglamento general de protección de datos: hacia un nuevo modelo europeo de privacidad, Reus, Madrid, 2016, p. 16.

[7] Por tanto, es necesario determinar el nivel de riesgo para los derechos y libertades de los afectados, a fin de aplicar las medidas adecuadas atendiendo a dichos riesgos. En relación a este punto, el Considerando 76 RGPD indica que «[l]a probabilidad y la gravedad del riesgo para los derechos y libertades del interesado debe determinarse con referencia a la naturaleza, el alcance, el contexto y los fines del tratamiento de datos. El riesgo debe ponderarse sobre la base de una evaluación objetiva mediante la cual se determine si las operaciones de tratamiento de datos suponen un riesgo o si el riesgo es alto». Es decir, el Reglamento considera insuficiente el no incumplimiento, incluyendo obligaciones dirigidas a la prevención de los mismos. La no aplicación de estas medidas es sancionable. Se exige que las medidas técnicas y organizativas que se adopten en la organización se revisen y se actualicen cuando sea necesario. Por otro lado, se exige, como medida adicional, la adopción de «políticas de protección de datos», «cuando sean proporcionadas en relación con las actividades de tratamiento».

[8] *Vid.* BIURRUN ABAD, F.J., «"Accountability" o responsabilidad proactiva en el Reglamento General de Protección de Datos», en *Actualidad Jurídica Aranzadi*, núm. 927, 2017, p. 28.

[9] Cómo afirma ESTEPA MONTERO, M., «El principio de responsabilidad proactiva o rendición de cuentas como informador del régimen jurídico de la protección de datos de las personas físicas», en *Anuario Jurídico y Económico Escurialense*, núm. LV, 2022, p. 76; «el Considerando 72 RGPD, la responsabilidad del tratamiento de datos personales realizado por el responsable del tratamiento o por su cuenta constituye un requisito *sine qua non*. Concretándose en la idea de que el responsable debe estar obligado a aplicar medidas oportunas y eficaces y ha de poder demostrar la conformidad de las actividades de tratamiento con el Reglamento, incluida la eficacia de las medidas. Por consiguiente, la clave del concepto se sitúa en la capacidad para demostrar la inocencia del responsable del tratamiento, en el sentido que aplicó las medidas precisas y eficaces para que se cumpliera la normativa en vigor. Nos encontramos, por consiguiente, con un concepto que se configura como el eje vertebrador

Constituyen manifestaciones del principio de responsabilidad y/o evidencias tangibles a los efectos de demostrar el cumplimiento del RGPD, los siguientes elementos: (i) la adopción de medidas de protección de datos desde el diseño y por defecto (art. 25 RGPD); (ii) la existencia y mantenimiento de un registro de actividades de tratamiento de datos personales (art. 30 RGPD); (iii) la implementación de medidas de seguridad del tratamiento adecuadas en función del estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como los riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas; (iv) la obligación de proceder sin dilación a la notificación de «quiebras de seguridad o brechas de datos personales», tanto a la autoridad de control como a los interesados (arts. 33 y 34 RGPD); (v) la realización de las preceptivas evaluaciones de impacto relativas a la protección de datos cuando sean pertinentes (art. 35 RGPD); (vi) la necesidad de recabar la autorización previa o de proceder a la realización de consultas previas a la autoridad de control cuando la puesta en marcha de un tratamiento entrañe un alto riesgo para los derechos y libertades fundamentales de la ciudadanía (art. 36 RGPD); (vii) el nombramiento y correcta implantación dentro de la organización de la figura del delegado de protección de datos; o (viii) la adhesión a códigos de conducta o mecanismos de certificación (arts. 20 y 42 RGPD)[10].

del resto de la regulación de la protección de datos personales, en cuanto noción de carácter horizontal que informa cada uno de los conceptos operativos del régimen jurídico aplicable […]La necesaria rendición de cuentas se ha de realizar, por consiguiente, en función de las circunstancias en las que se desarrolla el tratamiento de datos objeto de control. Lo que queda meridianamente claro si tenemos en cuenta que ya el propio artículo 24 al igual que el Considerando 74 del RGPD disponen, de manera expresa, como la gestión que se realice deberá tener en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como el riesgo de diversa probabilidad y gravedad para los derechos y libertades de las personas. A lo anterior, añade el referido precepto la exigencia de que las medidas que se apliquen sean revisadas y modificadas siempre que las nuevas circunstancias lo hagan necesario. Se trata, al mismo tiempo, de un concepto evolutivo que surge de la necesidad de las sociedades de alcanzar un nivel de eficacia y transparencia en la actividad pública y privada que dé garantías de respeto del Ordenamiento jurídico, así como de la necesaria consecución de unos estándares mínimos de calidad. De manera que se configura como un instrumento para la consecución de tales objetivos susceptible de ampliación y profundización en su contenido en función del grado de desarrollo tecnológico y social».

[10] Conviene precisar que nos encontramos ante una cuestión nuclear del modelo europeo de protección de datos de carácter personal. No en vano la reciente jurisprudencia del TJUE hace referencia de forma decidida ya, a veces de forma velada, otras de forma explícita, a este principio de responsabilidad proactiva consagrado en el art. 5.2 RGPD. En este sentido, es clara la STJUE de 16 de julio de 2020, Data Protection Commissioner/Facebook Ireland Ltd y Maximillian Schrems (asunto C-311/18), apartado 108; cuando afirma que «[e]n ausencia de una decisión por la que se constate la adecuación de la protección de los datos, el responsable o el encargado del tratamiento deben tomar medidas para compensar la falta de protección de datos en un tercer país mediante garantías adecuadas para el interesado. Tales garantías adecuadas pueden consistir en el recurso a normas corporativas vinculantes, a cláusulas tipo de protección de datos adoptadas por la Comisión o por una autoridad de control, o a cláusulas contractuales autorizadas por una autoridad de control. Esas garantías deben asegurar la observancia de requisitos de protección de datos y derechos de los interesados adecuados al tratamiento dentro de la Unión, incluida la disponibilidad por parte de los interesados de derechos exigibles y de acciones legales efectivas, lo que incluye el derecho a obtener una reparación administrativa o judicial efectiva y a reclamar una indemnización, en la Unión o en un tercer país. En particular, deben referirse al cumplimiento de los principios generales relativos al tratamiento de los datos personales y los principios de la protección de datos desde el diseño y por defecto […]».

Este principio de responsabilidad proactiva está ligado por estrechos lazos a otro concepto sumamente importante, cada vez más empleado por el legislador europeo cuando pretende regular el funcionamiento de sistemas y/o entornos complejos: la gestión del riesgo inherente a la puesta en marcha de operaciones de tratamiento de datos de carácter personal. A este respecto, conviene señalar que el RGPD contempla diferentes escenarios en función del riesgo que las diferentes operaciones de tratamiento llevadas a cabo por el responsable o el encargado del mismo puedan ocasionar para el pleno disfrute de los derechos y libertades fundamentales de la ciudadanía.

Así, en primer término, el art. 32 RGPD establece un repertorio de medidas técnicas y organizativas no limitante que el responsable y el encargado del tratamiento deberán adoptar teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como los riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, con el propósito de garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros: (a) la seudonimización y el cifrado de datos personales; (b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento; (c) la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico; y (d) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento. Asimismo, el Reglamento contempla la obligatoriedad de tener en cuenta los riesgos que presente el tratamiento de datos, en particular como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la

No obstante, este afamado pronunciamiento judicial no es el único que hace alusión al principio de responsabilidad proactiva. Así, la STJUE de 11 de noviembre de 2020, Orange România SA/Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (asunto C-61/19), apartado 52, señala lo siguiente: «los artículos 2, letra h), y 7, letra a), de la Directiva 95/46 y los artículos 4, punto 11, y 6, apartado 1, letra a), del Reglamento 2016/679 deben interpretarse en el sentido de que corresponde al responsable del tratamiento de los datos demostrar que el interesado ha manifestado su consentimiento para el tratamiento de sus datos personales mediante un comportamiento activo y que ha recibido, previamente, información respecto de todas las circunstancias relacionadas con ese tratamiento, con una formulación inteligible y de fácil acceso que emplee un lenguaje claro y sencillo, que le permita determinar sin dificultad las consecuencias de dicho consentimiento, de modo que se garantice que este se otorga con pleno conocimiento de causa. Un contrato relativo a la prestación de servicios de telecomunicaciones que contiene una cláusula conforme a la cual el interesado ha sido informado y ha consentido en la obtención y la conservación de una copia de su documento de identidad con fines de identificación no permite demostrar que esa persona haya dado válidamente su consentimiento para dicha obtención y dicha conservación, en el sentido de las referidas disposiciones, cuando: la casilla referente a dicha cláusula haya sido marcada por el responsable del tratamiento de datos antes de la firma del contrato, o cuando las estipulaciones contractuales de dicho contrato puedan inducir al interesado a error sobre la posibilidad de celebrar el contrato en cuestión pese a negarse a consentir en el tratamiento de sus datos, o cuando la libre elección de oponerse a dicha obtención y dicha conservación se vea indebidamente obstaculizada por ese responsable, al exigir que el interesado, para negarse a dar su consentimiento, cumplimente un formulario adicional en el que haga constar esa negativa».

comunicación o acceso no autorizados a dichos datos, cuando vaya a procederse a evaluar la adecuación del nivel de seguridad[11].

Por su parte, el art. 35 RGPD hace referencia a un segundo grupo de operaciones de tratamiento que presentan un alto riesgo para los derechos y libertades fundamentales de las personas físicas, las cuales están sometidas a la previa realización de una evaluación del impacto sobre la protección de datos personales (EIPD). Dicha evaluación deberá incluir como mínimo: (i) una descripción sistemática de las operaciones de tratamiento previstas y de los fines del tratamiento, inclusive, cuando proceda, el interés legítimo perseguido por el responsable del tratamiento; (ii) una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad; (iii) una evaluación ponderada de los riesgos para los derechos y libertades de los interesados; y (iv) las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales, y a demostrar la conformidad con el Reglamento, teniendo en cuenta los derechos e intereses legítimos de los interesados y de otras personas afectadas.

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[12]. En este sentido, para dotar de plena efectividad los postulados del RGPD urge avanzar en los procesos de construcción de una auténtica cultura de la protección de datos de carácter personal, cuestión en la que comienzan a incidir las principales autoridades independientes de control en la materia y cuyo reflejo es claramente visible en las legislaciones de aquellos Estados que, paulatinamente, han comenzado a reconocer una nueva generación de derechos digitales,

[11] Premisa que aparece reflejada, de igual forma, en el Considerando 78 RGPD, el cual reza como sigue: «[l]a protección de los derechos y libertades de las personas físicas con respecto al tratamiento de datos personales exige la adopción de medidas técnicas y organizativas apropiadas con el fin de garantizar el cumplimiento de los requisitos del presente Reglamento. A fin de poder demostrar la conformidad con el presente Reglamento, el responsable del tratamiento debe adoptar políticas internas y aplicar medidas que cumplan en particular los principios de protección de datos desde el diseño y por defecto. Dichas medidas podrían consistir, entre otras, en reducir al máximo el tratamiento de datos personales, seudonimizar lo antes posible los datos personales, dar transparencia a las funciones y el tratamiento de datos personales, permitiendo a los interesados supervisar el tratamiento de datos y al responsable del tratamiento crear y mejorar elementos de seguridad. Al desarrollar, diseñar, seleccionar y usar aplicaciones, servicios y productos que están basados en el tratamiento de datos personales o que tratan datos personales para cumplir su función, ha de alentarse a los productores de los productos, servicios y aplicaciones a que tengan en cuenta el derecho a la protección de datos cuando desarrollan y diseñen estos productos, servicios y aplicaciones, y que se aseguren, con la debida atención al estado de la técnica, de que los responsables y los encargados del tratamiento están en condiciones de cumplir sus obligaciones en materia de protección de datos. Los principios de la protección de datos desde el diseño y por defecto también deben tenerse en cuenta en el contexto de los contratos públicos».

[12] En este punto, conviene recordar el lapidario pronunciamiento contenido en el Considerando 4 RGPD, según el cual «[e]l tratamiento de datos personales debe estar concebido para servir a la humanidad».

como ocurre en el caso del art. 83 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

3. EL SISTEMA EUROPEO DE PROTECCIÓN DE DATOS PERSONALES EN LA ENCRUCIJADA: A VUELTAS CON LA NUEVA REGULACIÓN EUROPEA EN MATERIA DE INNOVACIÓN DIGITAL

El 21 de abril de 2021, la Comisión Europea presentó su propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial (IA) con la finalidad de: (i) garantizar que los sistemas de IA introducidos y usados en el mercado de la UE sean seguros y respeten la legislación vigente en materia de derechos fundamentales y valores de la Unión; (ii) garantizar la seguridad jurídica para facilitar la inversión e innovación en IA; (iii) mejorar la gobernanza y la aplicación efectiva de la legislación vigente en materia de derechos fundamentales y los requisitos de seguridad aplicables a los sistemas de IA; y (iv) facilitar el desarrollo de un mercado único para hacer un uso legal, seguro y fiable de las aplicaciones de IA y evitar la fragmentación del mercado[13]. La propuesta plantea más dudas que certezas y tiene importantes implicaciones para el correcto funcionamiento del sistema europeo de protección de datos de carácter personal.

En palabras de la Comisión Europea, el marco normativo propuesto, pretende tanto garantizar la tutela de los derechos fundamentales de las personas situadas en la Unión frente a las amenazas y riesgos ligados al desarrollo de herramientas de inteligencia artificial (IA), como reforzar la innovación en el seno de la Unión Europea en materia de IA. Se presenta además por la Comisión como «el primer marco jurídico sobre la IA de la historia» y como una de las medidas «destinada a convertir a Europa en el centro mundial de una IA digna de confianza»[14].

La base jurídica de la propuesta es, en primer lugar, el art. 114 TFUE, que prevé la adopción de medidas para garantizar el establecimiento y el funcionamiento del mercado interior. Además, la propuesta también se basa en el art. 16 TFUE, en la medida en que contiene

[13] Se trata del primer marco jurídico sobre esta tecnología y está enfocado a garantizar la seguridad y los derechos fundamentales de las personas y las empresas, al mismo tiempo que pretende convertir a Europa en el centro mundial de la inteligencia artificial apostando por la inversión y la innovación. *Vid.* 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,* Bruselas, 2021, p. 3 [COM(2021) 206 final].

[14] Siguiendo a DE MIGUEL ASENSIO, P.A., «Propuesta de Reglamento sobre Inteligencia Artificial», en *La Ley Unión Europea*, núm. 92, 2021, p. 2; en gran medida la Propuesta se construye sobre el modelo de la legislación preexistente relativa a la seguridad de los productos.

normas específicas sobre la protección de las personas físicas en lo que respecta al tratamiento de datos personales, en particular las restricciones al uso de sistemas de IA para la identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de aplicación de la ley[15].

En cuanto al ámbito de aplicación de la propuesta, las autoridades de control en materia de protección de datos acogen con gran satisfacción el hecho de que se extienda a la puesta a disposición y el uso de sistemas de IA por parte de las instituciones, organismos o agencias de la UE. Sin embargo, la exclusión de la cooperación internacional con fines de aplicación de la ley del ámbito de aplicación de la propuesta suscita serias preocupaciones para el Comité Europeo de Protección de Datos (CEPD) y el Supervisor Europeo de Protección de Datos (SEPD), ya que tal exclusión crea un riesgo significativo de elusión (por ejemplo, terceros países u organizaciones internacionales que gestionan aplicaciones de alto riesgo a las que recurren las autoridades públicas de la UE).

Una de las grandes fortalezas de la propuesta normativa es la aplicación de un enfoque basado en los factores de riesgo[16]. Sin embargo, se observa que algunas de las disposiciones

[15] El CEPD y el SEPD recuerdan que, en consonancia con la jurisprudencia del TJUE, el art. 16 TFUE proporciona una base jurídica adecuada cuando la protección de los datos personales es una de las finalidades o uno de los componentes esenciales de las normas adoptadas por el legislador de la Unión. La aplicación del art. 16 TFUE también implica la necesidad de garantizar un control independiente del cumplimiento de los requisitos relativos al tratamiento de datos personales, como también exige el art. 8 CDFUE. *Vid.* COMITÉ EUROPEO DE PROTECCIÓN DE DATOS, *Dictamen conjunto 5/2021 sobre la 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),* adoptado el 18 de junio de 2021, p. 2

[16] La propuesta de Reglamento clasifica los sistemas de IA en cuatro niveles diferenciados atendiendo a un enfoque de riesgo, atendiendo, principalmente, a la severidad del daño y la probabilidad de que este ocurra, y, en consecuencia, a mayores cotas de riesgo mayor número e intensidad de obligaciones deberá respetar el responsable de los sistemas de IA: (i) riesgo inadmisible. Se prohibirá un conjunto muy limitado de usos especialmente nocivos de la IA que contravienen los valores de la Unión al violar los derechos fundamentales (por ejemplo, puntuación social por parte de los Gobiernos, explotación de los puntos débiles de los niños, uso de técnicas subliminales y, salvo contadas excepciones, determinados sistemas de identificación biométrica remota en directo en espacios públicos con fines policiales); (ii) Alto riesgo. Este nivel abarca, entre otras, tecnologías de IA empleadas en infraestructuras críticas, como transportes, que pueden poner en peligro la vida y la salud de los ciudadanos; formación educativa o profesional que pueden determinar el acceso a la educación y la carrera profesional o componentes de seguridad de los productos, como pudiera ser la aplicación de IA en cirugía asistida por robots. El reglamento también tiene en cuenta otros sistemas en áreas como la aplicación de las leyes, la administración de justicia o la gestión de la migración, el asilo y el control de fronteras. De conformidad con la regulación propuesta, los sistemas de alto riesgo deberán aportar un registro de la actividad para garantizar la trazabilidad de los resultados y deberán contar con sistemas adecuados de evaluación y mitigación de riesgo o responder a una alta calidad de los conjuntos de datos que alimentan el sistema, aportar documentación detallada sobre el sistema y su finalidad, proporcionar información clara y adecuada al usuario y tener un alto nivel de solidez, seguridad y precisión, así como contemplar medidas apropiadas de supervisión humana para minimizar el riesgo; (iii) Riesgo limitado. En este nivel se incluyen sistemas como chatbot o robots conversacionales, que deberán cumplir unas medidas específicas de transparencia. A este respecto, se establece la obligación de informar a los usuarios de que están interactuando con una máquina para poder tomar una decisión informada de continuar o no; y (iv) Riesgo mínimo o nulo. La propuesta de la Comisión permite el uso gratuito de aplicaciones tales como

de la propuesta excluyen los riesgos para grupos de personas o para la sociedad en su conjunto (por ejemplo, efectos colectivos de especial relevancia). Por ello, este enfoque deberá aclararse y el concepto de «riesgo para los derechos fundamentales» debe alinearse con la legislación europea en materia de protección de datos personales, en particular, con el RGPD, el Reglamento (UE) 2018/1725, la Directiva 2002/58/CE y la Directiva (UE) 2016/680, ya que en la propuesta normativa entran en juego numerosos aspectos relacionados con la protección de los datos personales. A continuación, se examinan algunos de los pasajes de la propuesta de Reglamento que generan un buen número de interrogantes, en la medida en que suponen una seria amenaza para la correcta tutela jurídica de la protección de datos de carácter personal.

Así, en primer término, tanto el CEPD como el SEPD coinciden en señalar que la clasificación de sistema de IA como de alto riesgo, a tenor de las previsiones contempladas en el art. 6 de la propuesta normativa, no significa necesariamente que este sea legal *per se* y que pueda ser desplegado por el usuario como tal, habida cuenta de que es posible que la persona responsable del tratamiento tenga que cumplir otros requisitos derivados de la legislación europea en materia de protección de datos. Además, las autoridades en materia de protección de datos insisten en subrayar la necesidad de proceder al cumplimiento de las obligaciones legales derivadas de la legislación de la Unión (incluida la protección de datos personales) como condición previa para que una solución de IA pueda acceder al mercado europeo como producto con el marcado CE[17].

En segundo lugar, el uso de la IA para la «clasificación social», tal como se prevé en el art. 5.1.c) de la propuesta puede dar lugar a discriminación y es contrario a los valores fundamentales de la UE. La propuesta solo prohíbe estas prácticas cuando se realizan «durante un período determinado de tiempo» o «por parte de las autoridades públicas o en representación de estas». Sin embargo, no se hace mención alguna a aquellas empresas privadas, como las redes sociales y los proveedores de servicios en la nube, los cuales como ha quedado patente en numerosas ocasiones pueden tratar grandes cantidades de datos personales y realizar

videojuegos basados en inteligencia artificial o filtros de correo basura. Ya que la amplia mayoría de los sistemas de IA entran en esta categoría, el proyecto de Reglamento no interviene aquí debido a su limitado riesgo sobre los derechos o la seguridad de los individuos. En torno a la propuesta de Reglamento sobre la Inteligencia Artificial, *vid.* HUERGO LORA, A., «El proyecto de Reglamento sobre la Inteligencia Artificial», en *Almacén de Derecho*, 2021. Disponible en: https://bit.ly/3wLmfxo

[17] Para poder comercializarse en la Unión Europea, muchos productos deben llevar obligatoriamente el marcado CE, que demuestra que el fabricante ha evaluado el producto y se considera que este cumple los requisitos de seguridad, sanidad y protección del medio ambiente exigidos por la UE. El marcado CE es obligatorio para los productos fabricados en cualquier lugar del mundo que vayan a **comercializarse en la UE,** de conformidad con el Reglamento (CE) n.º 765/2008 del Parlamento Europeo y del Consejo, de 9 de julio de 2008, por el que se establecen los requisitos de acreditación y vigilancia del mercado relativos a la comercialización de los productos y por el que se deroga el Reglamento (CEE) n.º 339/93.

clasificaciones sociales. Por consiguiente, se hace necesario que el futuro Reglamento sobre la IA acometa la prohibición de cualquier tipo de clasificación social.

Igualmente problemáticas resultan las disposiciones relativas a la identificación biométrica remota[18] de las personas en espacios de acceso público, la cual supone un riesgo elevado de intrusión en la vida privada de las personas, con graves efectos en las expectativas de la población de conservar el anonimato en los espacios públicos[19]. Por estas razones, el CEPD y el SEPD defienden de forma decidida una prohibición general del uso de la IA para el reconocimiento automatizado de rasgos humanos en espacios de acceso público, como los rostros, pero también la marcha, las huellas dactilares, el ADN, la voz, las pulsaciones de teclas y otras señales biométricas o conductuales, en cualquier contexto. También se recomienda prohibir los sistemas de IA que clasifiquen a las personas a partir de sus datos biométricos en grupos por razón de su origen étnico, sexo, orientación política o sexual u otros motivos de discriminación con arreglo al art. 21 CDFUE. Además, el CEPD y el SEPD consideran que «el uso de la IA para inferir emociones de una persona física es altamente indeseable y deberá prohibirse»[20].

[18] Como se desprende de la redacción conjunta del Considerando 8 y el art. 3.36) de la propuesta de Reglamento, se entiende por sistema de identificación biométrica remota, cualquier «sistema de IA destinado a identificar a personas físicas a distancia comparando sus datos biométricos con los que figuran en una base de datos de referencia, y sin que el usuario del sistema de IA sepa de antemano si la persona en cuestión se encontrará en dicha base de datos y podrá ser identificada».

[19] En este punto, conviene resaltar que el art. 5.1.d) de la propuesta establece una amplia lista de casos excepcionales en los que se permite la identificación biométrica remota «en tiempo real» en espacios de acceso público con fines de aplicación de la ley. En opinión de las autoridades de control, este enfoque adolece de defectos en varios aspectos. En primer lugar, no está claro qué deberá entenderse por «demora significativa» ni cómo deberá considerarse un factor atenuante, teniendo en cuenta que un sistema de identificación masiva es capaz de identificar a miles de personas en solo unas horas. Además, la intrusión del tratamiento no siempre depende de que la identificación se realice en tiempo real o no. Es probable que la identificación biométrica a distancia en el contexto de una protesta política tenga un efecto disuasorio significativo en el ejercicio de los derechos y libertades fundamentales, como la libertad de reunión y asociación y, más en general, en los principios fundacionales de la democracia. En segundo lugar, el carácter intrusivo del tratamiento no depende necesariamente de su finalidad. El uso de este sistema para otros fines, como la seguridad privada, representa las mismas amenazas para los derechos fundamentales al respeto de la vida privada y familiar y a la protección de los datos personales. Por último, incluso con las limitaciones previstas, el número potencial de personas sospechosas o autoras de delitos será casi siempre «lo suficientemente elevado» como para justificar el uso continuo de sistemas de IA para la detección de sospechosos, a pesar de las condiciones adicionales del art. 5, apartados 2 a 4, de la propuesta. El razonamiento que subyace a la propuesta parece omitir que, a la hora de supervisar los espacios abiertos, las obligaciones derivadas de la legislación de la UE en materia de protección de datos deben cumplirse no solo para las personas sospechosas, sino para todas aquellas que son objeto de seguimiento en la práctica.

[20] Excepto en determinados casos de uso bien especificados, a saber, con fines de salud o investigación (por ejemplo, pacientes para quienes el reconocimiento emocional es importante), siempre con las salvaguardias adecuadas y, por supuesto, con sujeción a todas las demás condiciones y límites de protección de datos, incluida la limitación de la finalidad. *Vid. Op. cit.* COMITÉ EUROPEO DE PROTECCIÓN DE DATOS, *Dictamen conjunto 5/2021…,* p. 13.

En cuarto lugar, lo que respecta a los espacios de pruebas (art. 53), es necesario clarificar su ámbito de aplicación y sus objetivos. A este respecto, parece lógico que la propuesta normativa también deba indicar claramente que la base jurídica de dichos espacios de pruebas deberá cumplir los requisitos establecidos en el marco de protección de datos existente.

Asimismo, la propuesta en su Título VI relativo a la «Gobernanza» asigna por medio de su art. 56 un papel predominante a la Comisión en el futuro «Comité Europeo de Inteligencia Artificial» (CEIA). Este papel entra en conflicto con la necesidad de que un organismo europeo de IA sea independiente de cualquier influencia política. Para garantizar su independencia, el futuro Reglamento sobre la IA deberá otorgar más autonomía al CEIA y garantizar que pueda actuar por propia iniciativa.

En sexto lugar, el art. 59 de la propuesta de Reglamento contempla la necesidad de que cada Estado miembro proceda al establecimiento o designación de autoridades nacionales competentes con el fin de garantizar la aplicación y ejecución de la futura norma, las cuales deberán organizarse de forma que se preserve la objetividad e imparcialidad de sus actividades y funciones. En nuestra opinión, la designación de las autoridades de protección de datos como autoridades nacionales de supervisión garantizaría un enfoque regulador más armonizado, contribuiría a una interpretación coherente de las disposiciones sobre tratamiento de datos y evitaría contradicciones en su aplicación entre los Estados miembros[21].

En séptimo lugar, la propuesta contempla la designación del SEPD como autoridad competente y de vigilancia del mercado para la supervisión de las instituciones, órganos y organismos de la Unión (arts. 63.6). No obstante, no se especifica el papel y las funciones del SEPD, en particular por lo que se refiere a su papel como autoridad de vigilancia del mercado. Tampoco el futuro Reglamento sobre la IA hace alusión con claridad a la necesaria independencia de las autoridades de supervisión en el ejercicio de sus funciones de supervisión y ejecución.

También son patentes las lagunas en lo que atañe a los mecanismos de cumplimiento normativo articulados por la propuesta de Reglamento. Así, en primer término, y a pesar de que los sistemas de IA de alto riesgo se fundamentan en el tratamiento de datos de carácter personal para cumplir su cometido, se establece un sistema de certificación sustentado sobre un mecanismo de evaluación/certificación de la conformidad (arts. 44 y ss.) que abarca los requisitos obligatorios aplicables a los sistemas de IA de alto riesgo, y se basa en

[21] Teniendo en cuenta la dispersión de los sistemas de IA en el mercado único y la probabilidad de que se produzcan casos transfronterizos, existe una necesidad crucial de una aplicación armonizada y una asignación adecuada de competencias entre las autoridades nacionales de supervisión. El CEPD y el SEPD sugieren que se prevea un mecanismo que garantice un punto de contacto único para las personas físicas afectadas por la legislación, así como para las empresas, para cada sistema de IA. *Vid. Op. cit.* COMITÉ EUROPEO DE PROTECCIÓN DE DATOS, *Dictamen conjunto 5/2021…,* p. 18.

normas europeas armonizadas con arreglo al Reglamento (UE) n.º 1025/2012 y en especificaciones comunes que debe establecer la Comisión. Dicho sistema de certificación carece de una relación lógica con la legislación de la UE en materia de protección de datos, no tiene en cuenta los principios de minimización de datos y protección de datos desde el diseño como uno de los aspectos que deben tenerse en cuenta antes de obtener el marcado CE[22]. Por consiguiente, el CEPD y el SEPD recomiendan que se modifique la propuesta para clarificar la relación entre los certificados expedidos en virtud del futuro Reglamento de IA y los certificados, sellos y marcas de protección de datos (arts. 42 y 43 RGPD). De igual forma, dichas Instituciones remarcan la conveniencia de que las autoridades de protección de datos participen en la elaboración y el establecimiento de normas armonizadas y especificaciones comunes[23].

Finalmente, en lo que respecta a los códigos de conducta, el art. 69 de la propuesta de Reglamento establece que tanto la Comisión, como los Estados miembros fomentarán y facilitarán la elaboración de códigos de conducta destinados a promover la aplicación voluntaria de los requisitos establecidos en el Título III, capítulo 2, a sistemas de IA distintos de los de alto riesgo, sobre la base de especificaciones y soluciones técnicas que constituyan medios adecuados para garantizar el cumplimiento de dichos requisitos a la luz de la finalidad prevista de los sistemas. De esta forma, la Comisión y el Comité Europeo de Inteligencia Artificial fomentarán y facilitarán la elaboración de códigos de conducta destinados a promover la aplicación voluntaria a sistemas de IA de los requisitos relativos, por ejemplo, a la sostenibilidad ambiental, la accesibilidad para personas con discapacidad, la participación de partes interesadas en el diseño y desarrollo de los sistemas de IA y la diversidad de los equipos de desarrollo, sobre la base de objetivos claros e indicadores clave de resultados para medir la consecución de dichos objetivos, sin clarificar en modo alguno si la protección de los datos personales debe considerarse entre los «requisitos adicionales» que pueden ser abordados por estos códigos de conducta, con el propósito de garantizar

[22] Sir ir más lejos, el Considerando 64 de la propuesta de Reglamento señala lo siguiente: «[p]uesto que los profesionales que realizan la certificación previa a la comercialización tienen una experiencia más amplia en el campo de la seguridad de los productos, y habida cuenta de la diferente naturaleza de los riesgos implicados, procede limitar, al menos en la fase inicial de aplicación del presente Reglamento, el alcance de las evaluaciones de la conformidad realizadas por terceros a los sistemas de IA de alto riesgo que no están asociados a productos. En consecuencia, el proveedor es quien, por norma general, debe llevar a cabo la evaluación de la conformidad de dichos sistemas bajo su propia responsabilidad, con la única excepción de los sistemas de IA que están destinados a utilizarse para la identificación biométrica remota de personas. En el caso de estos últimos, y en la medida en que no estén prohibidos, debe preverse que un organismo notificado participe en la evaluación de la conformidad».

[23] En opinión del CEPD y del SEPD, este mecanismo difiere en demasía del sistema de certificación destinado a garantizar el cumplimiento de las normas y principios de protección de datos, descrito en los arts. 42 y 43 RGPD. No está claro, por tanto, cómo pueden interactuar los certificados expedidos por los organismos notificados de conformidad con la propuesta con las certificaciones, sellos y marcas de protección de datos previstos en el RGPD, a diferencia de lo que se prevé para otros tipos de certificados. *Vid. Op. cit.* COMITÉ EUROPEO DE PROTECCIÓN DE DATOS, *Dictamen conjunto 5/2021…,* p. 23.

que las «especificaciones y soluciones técnicas» adoptadas no entren en conflicto con las normas y principios del actual marco de protección de datos de la Unión Europea.

En síntesis, la propuesta de Reglamento del Parlamento Europeo y del Consejo por el que se establecen normas armonizadas en materia de inteligencia artificial 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. La propuesta normativa está plagada de multitud de lagunas que, de forma sistemática, desoyen las normas y principios 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[24]. La propuesta de Ley de Inteligencia Artificial es un paso más en este proceso de debilitamiento de los valores, derechos y libertades fundamentales que dan forma a la noción de ciudadanía europea, toda vez que constituye un procedimiento legislativo viciado de origen, que adolece de la necesidad de incorporar la dimensión de la protección de datos de carácter personal desde el diseño, limitándose a incorporar el componente de la privacidad en último lugar, como si de un añadido se tratase. El sistema europeo de protección de datos personales se encuentra, por tanto, en la encrucijada. Sin embargo, existe otra forma de proceder, aún estamos a tiempo de acometer una verdadera revolución que permita blindar la tutela jurídica de los derechos de la

[24] Sirva como muestra de esta tendencia, la pregunta planteada a la Comisión Europea, con fecha 8 de julio de 2022, por Dña. Sandra Pereira, eurodiputada portuguesa perteneciente al Grupo de la Izquierda en el Parlamento Europeo, en relación a las negociaciones tripartitas sobre la Ley de Servicios Digitales [E-002500/2022], en la que se pone de relieve los esfuerzos lobistas ejercidos por las grandes corporaciones tecnológicas para influenciar los procesos legislativos tendentes a la aprobación del Código Digital Europeo: «[e]n la última sesión plenaria, votamos sobre el acuerdo alcanzado en el diálogo tripartito sobre la Ley de Servicios Digitales, un paquete que supuestamente ayudará a las grandes plataformas a abordar cosas como el contenido ilegal y la publicidad dirigida. Según algunos informes, más de 40 ONG y sindicatos preocupados por la transparencia, los derechos digitales y la democracia tuvieron problemas para obtener información sobre el proceso de negociación. Mientras tanto, nada se interpuso en el camino de las grandes multinacionales del sector, que mantuvieron su presión durante toda la negociación. Google, por ejemplo, ha declarado gastar al menos 6 millones de euros en lobby regulatorio en la UE y ha contratado a diez consultores para recopilar información, aunque es menos que Facebook, que ha contratado a 13. Por lo tanto, aunque es difícil para algunas organizaciones para estar al tanto de las negociaciones, las puertas siempre están abiertas para las multinacionales y sus intereses. ¿Puede la Comisión confirmar si se entregó información a las organizaciones antes mencionadas durante las negociaciones en cuestión? También me gustaría saber qué tipo de procedimiento suele establecer para que la información sobre el progreso sea accesible cuando se negocian grandes paquetes de este tipo». Más información, disponible en: https://bit.ly/3AhuODx

privacidad ante el mar de nuevos interrogantes y amenazas que se comienzan a otear en el horizonte digital.

4. LA FUERZA EXPANSIVA DEL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS Y SU INFLUENCIA EN EL CONTEXTO INTERNACIONAL COMO MOTOR DE MODERNIZACIÓN DE LA LEGISLACIÓN EN MATERIA DE PRIVACIDAD

Como es sabido por todos, 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»[25], puede definirse como la capacidad que han tenido las Instituciones comunitarias de convertir sus normas y su legislación en prácticamente estándares globales, lo que 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.

4.1. El caso paradigmático de Iberoamérica y el protagonismo de la Red Iberoamericana de Protección de Datos

Como se ha señalado con anterioridad, el Reglamento General de Protección de Datos ha desempeñado un papel crucial en la difusión mundial del «modelo» europeo de protección de datos, ya que a menudo se usa para inspirar a terceros Estados que prevén adoptar o modernizar sus propias normas de tutela jurídica de la privacidad. En esta dificultosa tarea juega un papel esencial la Red Iberoamericana de Protección de Datos (RIPD), organización que surge con motivo del acuerdo alcanzado en el primer Encuentro Iberoamericano de Protección de Datos, durante la primera década del presente siglo[26].

[25] Término acuñado en 2012 por la profesora Anu Bradfrod de Columbia Law School. La tesis de Bradford es que la fuerza de la Unión Europea radica en su capacidad de crear un marco regulador común. Siguiendo las tesis de Bradford es la Unión Europea, y no Estados Unidos o China, quien domina el mundo en la medida en la que es capaz de generar la externalización involuntaria de regulaciones mediante los mecanismos globalizadores del mercado. *Vid.* BRADFORD, A., *The Brussels Effect: How the European Union Rules the World*, Oxford University Press, Nueva York, 2020, p. 3

[26] En junio de 2003, con ocasión del Encuentro Iberoamericano de Protección de Datos celebrado en La Antigua (Guatemala), se creó la Red Iberoamericana de Protección de Datos por impulso de la Agencia Española de

La RIPD se configura desde sus orígenes como un foro integrador de los diversos actores, tanto del sector público como privado, que desarrollen iniciativas y proyectos relacionados con la protección de datos personales en Iberoamérica, con la finalidad de fomentar, mantener y fortalecer un estrecho y permanente intercambio de información, experiencias y conocimientos entre ellos[27], así como promover los desarrollos normativos necesarios para garantizar una regulación avanzada del derecho a la protección de datos personales en un contexto democrático, tomando en consideración la necesidad del continuo flujo de datos entre países que tienen diversos lazos en común y una preocupación por este derecho[28].

Su actividad durante estas casi dos décadas de funcionamiento ha convertido a la RIPD en el principal promotor del diálogo e impulsor de iniciativas y políticas en la región, lo que ha significado que más de 350 millones de ciudadanos latinoamericanos (tras la reciente incorporación de Brasil[29]) dispongan en la actualidad de normas que permitan garantizar eficazmente el uso de su información personal y de autoridades especializadas con competencias para tutelar dichas garantías[30]. En concreto, desde 2003, se han promulgado leyes generales de protección de datos personales en Uruguay, México, Costa Rica, Perú,

Protección de Datos como un foro abierto a la incorporación de todos los países iberoamericanos, con el propósito de potenciar las iniciativas de intercambio de experiencias entre ellos y de reforzar su mutua y continua colaboración en materia de protección de datos. Poco después, en noviembre del mismo año, la Declaración de Santa Cruz de la Sierra (Bolivia), firmada tras la XIII Cumbre de Jefes de Estado y de Gobierno de Iberoamérica, plasmó en su art. 45 y a tan alto nivel, el reconocimiento expreso de la protección de datos como derecho fundamental y la labor de la Red Iberoamericana de Protección de Datos. Por otra parte, en el marco de la XXVII Conferencia Mundial de Protección de Datos, celebrada en Montreux (Suiza), en septiembre de 2005, se reconoció, asimismo, en su Declaración Final, la importancia de la labor desarrollada por la Red. Acerca del proceso de gestación de la Red Iberoamericana de Protección de Datos, *vid.* PIÑAR MAÑAS, J.L. y MONTULL CREMADES, M.A., *La Red Iberoamericana de Protección de Datos: Declaraciones y documentos*, Tirant lo Blanch, Valencia, 2006, 168 pp.

[27] En opinión de MARGARITA PORCELLO, A., «La protección de los datos personales en el entorno digital. Los estándares de protección de datos en los países iberoamericanos», en *Quaestio Iuris*, vol. 12, núm. 2, 2019, pp. 493-494; «la Red Iberoamericana de Protección de Datos se muestra como una de las posibles instancias de diálogo e interacción, ya que aparte de significativa representación de autoridades de protección de datos y de privacidad de países de la región y de organismos internacionales, ha previsto en sus reuniones la participación del sector privado y de observadores académicos».

[28] La Red promueve así un conjunto de técnicas de cooperación delimitadas en los arts. 16 a 19 del Reglamento de la RIPD, de conformidad con el texto aprobado el 30 de noviembre de 2018. Actualmente está compuesta por 34 miembros (16 miembros y 18 observadores), entre los que se encuentra la Agencia Española de Protección de Datos, la cual ostenta la secretaría permanente de la RIPD.

[29] La Lei Geral de Proteção de Dados LGPD) entró en vigor el 18 de septiembre de 2020, tras más de dos años de *vacatio legis* después de su aprobación en agosto de 2018. La LGPD o Ley 13.709, está fuertemente inspirada en el Reglamento General de Protección de Datos de la Unión Europea y tiene como finalidad regular el uso, la protección y la transferencia de datos personales en Brasil. La Ley pretende garantizar un mayor control de los ciudadanos sobre sus datos personales, exigiendo consentimiento explícito para su recolección y tratamiento, y obliga a ofrecer al usuario las opciones de visualizar, corregir y excluir dichos datos.

[30] En América Latina, Chile fue el primer país que adoptó una ley de este tipo en 1999, seguido de Argentina en el año 2000. Con posterioridad, varios países siguieron su ejemplo: Uruguay (2008), México (2010), Perú (2011), Colombia (2012), Brasil (2018), Barbados (2019) y Panamá (2019); estando estos últimos hitos normativos, en gran medida, fuertemente alineados con las disposiciones contenidas en el poderoso Reglamento (UE) 2016/679.

Nicaragua, Colombia, República Dominicana, Brasil y Panamá. Y existan actualmente iniciativas legislativas en tramitación en Chile, Ecuador y El Salvador. Asimismo, Argentina[31] y Uruguay[32] han obtenido el reconocimiento de la Comisión Europea como países con nivel de protección adecuada, a efectos de la realización de transferencias de datos personales entre dichos países y la Unión Europea.

En este sentido, no debe olvidarse que la protección de datos de carácter personal posibilita el crecimiento económico de estos países, promoviendo la adaptación de sus legislaciones en ámbitos que, como las transferencias internacionales de datos, son claves para el desarrollo de las transacciones comerciales entre Europa y América Latina, con lo que ello supone para sus procesos de internacionalización en esta área geográfica. Asimismo refuerza su gobernabilidad mediante el fortalecimiento de las instituciones encargadas del control del cumplimiento efectivo del derecho fundamental de protección de los datos personales, la profesionalización de la gestión de sus Administraciones y la capacitación permanente de sus autoridades y personal, fortaleciendo así los sistemas de garantías de los Derechos Humanos, a través del referido derecho fundamental, y otros conexos como el derecho a la dignidad de la persona, al honor, a la intimidad, a la seguridad jurídica, la libertad sindical o la libertad de información y expresión, como uno de los indicadores básicos del desarrollo y consolidación de los procesos democráticos en la región[33].

Desde el punto de vista regulatorio de la RIPD, conviene destacar varios hitos importantes. En primer término, con ocasión del V Encuentro Iberoamericano de Protección de Datos, se adoptaron las «Directrices para la Armonización de la Protección de Datos en la Comunidad Iberoamericana», con las que se pretendió establecer un marco armonizado de referencia

[31] *Vid.* Decisión 2003/490/CE de la Comisión, de 30 de junio de 2003.

[32] *Vid.* Decisión 2012/484/UE de la Comisión, de 21 de agosto de 2012.

[33] Cuestiones todas ellas que siguen impregnando la hoja de ruta de la RIPD. *Vid.* RED IBEROAMERICANA DE PROTECCIÓN DE DATOS*, Plan Estratégico 2021-2025: Nuevos tiempos para la privacidad. Nuevas estrategias*, Madrid, 2020, p. 1; donde se fijan los objetivos a los que estará orientada la Red durante el próximo ciclo de programación: (i) seguir impulsando los procesos regulatorios en la región, tanto en lo que se refiere a los países que aún no cuentan con normativa propia en la materia, como a los que ya disponen de ella, teniendo como marco de referencia los más recientes estándares internacionales en la materia, privilegiando especialmente los Estándares de Protección de Datos Personales para los Estados Iberoamericanos aprobados por la RIPD en 2017. En especial, se apoyará esta adaptación a los países iberoamericanos ya adecuados al marco europeo (Argentina y Uruguay), así como a aquellos otros que acuerden poner en marcha el correspondiente proceso de adecuación ante la Comisión Europea; (ii) promover marcos regulatorios de alcance supranacional o regional como instrumento clave para la consolidación en la región de un modelo iberoamericano de protección de datos adaptado a las necesidades y especificidades propias de la región y de los respectivos países. Esta colaboración se estrechará con aquellas organizaciones y entidades, tanto de alcance horizontal como sectorial, que contribuyan a este objetivo de integración regional. Para ello, se tendrá especialmente en cuenta el marco de cooperación del Convenio 108 del Consejo de Europa; y (iii) apoyar los procesos regulatorios y de adecuación ofreciendo el asesoramiento técnico de la RIPD y de sus Autoridades a las respectivas instancias gubernamentales y parlamentarias de los países de la región que así lo requieran.

que contribuya «a la emisión de iniciativas regulatorias de protección de datos personales en la región iberoamericana de aquellos países que aún no cuentan con estos ordenamientos, o en su caso, sirvan como referente para la modernización y actualización de las legislaciones existentes»[34].

En segundo lugar, destaca la aprobación de los Estándares Internacionales sobre Protección de Datos Personales y Privacidad (también conocidos como «Estándares de Madrid») en el seno de la XXXI Conferencia Internacional de Autoridades de Protección de Datos y Privacidad celebrada el 5 de noviembre de 2009 en Madrid, los cuales constituyeron, sin duda, un avance en la búsqueda de soluciones y disposiciones específicas que, sin perjuicio de ser objeto de ampliaciones mediante soluciones y disposiciones específicas «podrían aplicarse independientemente de las diferencias que puedan existir entre los diferentes modelos existentes de protección de datos y privacidad»[35].

Tiempo después, en el marco del XV Encuentro Iberoamericano de Protección de Datos, la RIPD presentó oficialmente los llamados «Estándares de Protección de Datos de los Estados Iberoamericanos»[36], con los que se pretende, entre otras cuestiones: (i) establecer un conjunto de principios y derechos comunes de protección de datos personales que los Estados Iberoamericanos puedan adoptar y desarrollar en su legislación nacional, con la finalidad de contar con reglas homogéneas en la región; (ii) garantizar el efectivo ejercicio y tutela del derecho a la protección de datos personales de cualquier persona física en los Estados Iberoamericanos, mediante el establecimiento de reglas comunes que aseguren el debido tratamiento de sus datos personales; (iii) facilitar el flujo de los datos personales

[34] Dicho documento tenía por objeto: (i) definir un conjunto de principios y derechos que garanticen la efectiva y uniforme protección de la privacidad a nivel internacional, en relación con el tratamiento de datos de carácter personal; y (ii) facilitar los flujos internacionales de datos de carácter personal, necesarios en un mundo globalizado. *Vid.* RED IBEROAMERICANA DE PROTECCIÓN DE DATOS, *Estándares de protección de datos personales,* Madrid, 2007, p. 3.

[35] *Vid.* AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, *Estándares Internacionales sobre Protección de Datos Personales y Privacidad,* Madrid, 2009, p. 35.

[36] Los estándares comprenden 24 considerandos, 9 capítulos y 45 artículos divididos en diez capítulos, a saber: el Capítulo I (Disposiciones generales) comprende los arts. 1 a 9; el Capítulo II (Principios de protección de datos personales) abarca desde el art. 10 al 23; el Capítulo III (Derechos del titular) del art. 24 al 32; el Capítulo IV (Encargado) comprende los arts. 33 al 35; el Capítulo V (Transferencias internacionales de datos personales) el art. 36; el Capítulo VI (Medidas proactivas en el tratamiento de datos personales) desde el art. 37 al 41; el Capítulo VII (Autoridades de control) el art. 42; el Capítulo VIII (Reclamaciones y Sanciones) el art. 43; el Capítulo IX (Derecho de indemnización) el art. 44 y el Capítulo X (Cooperación internacional) el art. 45.

Los Estándares de 2017 reconocen que el nuevo marco normativa de la Unión Europea en torno al RGPD «es un referente obligado y determinante para la elaboración de las legislaciones nacionales de protección de datos en Iberoamérica» (Considerando 8), lo que justifica en última instancia que su contenido reitere en buena parte los postulados del RGPD con matices y peculiaridades. *Vid. Op. cit.* MARTÍ DEL MORAL, A., «La protección de datos personales en Europa e Iberoamérica», en CERRILLO i MARTÍNEZ, A. (Dir.), *La Administración Digital,* Dykinson, Madrid, 2022, p. 192.

entre los Estados Iberoamericanos y más allá de sus fronteras, con la finalidad de coadyuvar al crecimiento económico y social de la región; y (iv) favorecer la cooperación internacional entre las autoridades de control de los Estados Iberoamericanos, con otras autoridades de control no pertenecientes a la región y autoridades y organismos internacionales en la materia. Una de las fortalezas de este último hito regulador de la RIPD, es que en su elaboración se tomaron como referencia diversos instrumentos internacionales y emblemáticos en materia de protección de datos personales como son las Directrices relativas a la protección de la intimidad y de la circulación transfronteriza de datos personales de la Organización para la Cooperación y Desarrollo Económicos; el Convenio 108 del Consejo de Europa, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal y su Protocolo; el Marco de Privacidad del Foro de Cooperación Económica Asia Pacífico, y el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, 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, entre otros[37].

4.2. La decisión de adecuación relativa a Japón y la creación de la mayor área mundial de flujos de datos seguros

Como es sabido por todos, el art. 44 RGPD propugna que *«[p]odrá realizarse una transferencia de datos personales a un tercer país u organización internacional cuando la Comisión haya decidido que el tercer país, un territorio o uno o varios sectores específicos de ese tercer país, o la organización internacional de que se trate garantizan un nivel de protección adecuado. Dicha transferencia no requerirá ninguna autorización específica»*[38].

Por tanto, una decisión de adecuación de la Comisión Europea[39] es un acto jurídico del derecho de la Unión Europea en virtud del cual se facilita, como garantía adecuada, la libre

[37] *Vid.* RED IBEROAMERICANA DE PROTECCIÓN DE DATOS, *Estándares de protección de datos personales,* Madrid, 2017, p. 4.

[38] De esta forma, como señalan USTARÁN, E. y GARCÍA, P., «Transferencias internacionales de datos», en RALLO LOMBARTE, A. (Dir.), *Tratado de protección de datos. Actualizado con la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales,* Tirant lo Blanch, Valencia, 2019, p. 460; en línea con el enfoque de su predecesora, la Directiva 95/46/CE, el Reglamento incorpora una serie de restricciones «ciertamente desafiantes» en el contexto de un mundo exponencialmente interconectado, digital y transfronterizo como el actual. Así pues, las transferencias internacionales de datos personales a cualquier Estado situado fuera del Espacio Económico Europeo (EEE) solamente podrán tener lugar con arreglo al Capítulo V RGPD: (i) en caso de que la Comisión haya dictado una decisión declarando que el tercer país en cuestión ofrece un nivel de protección de datos adecuado; (ii) a falta de tal decisión, si el responsable o el encargado del tratamiento que desea llevar a cabo la transferencia aporta garantías adecuadas, incluyendo la disponibilidad de derechos exigibles y acciones legales efectivas por parte de los interesados; y (iii) en ausencia de las anteriores, la transferencia podrá realizarse si entra en juego alguna de las excepciones contempladas en el art. 49 RGPD.

[39] Al evaluar la adecuación del nivel de protección, la Comisión tendrá en cuenta, en particular, los siguientes elementos (art. 45.2 RGPD): (a) el Estado de Derecho, el respeto de los derechos humanos y las libertades fundamentales, la legislación pertinente, tanto general como sectorial, incluida la relativa a la seguridad pública, la

circulación de datos personales a terceros países desde la UE, sin que sean necesarias garantías adicionales o cumplir otras condiciones[40]. En concreto, en materia de nivel adecuado en protección de datos, una decisión de la Comisión Europea es una decisión unilateral de ejecución, adoptada en virtud de la legislación sobre protección de datos personales y conforme a los criterios fijados en esta. El efecto de la decisión es constatar que un tercer Estado ofrece un nivel de protección de datos personales sustancialmente equivalente al que se garantiza en la Unión Europea, lo que implica considerar tanto la CDFUE como la propia legislación sobre protección de datos[41].

defensa, la seguridad nacional y la legislación penal, y el acceso de las autoridades públicas a los datos personales, así como la aplicación de dicha legislación, las normas de protección de datos, las normas profesionales y las medidas de seguridad, incluidas las normas sobre transferencias ulteriores de datos personales a otro tercer país u organización internacional observadas en ese país u organización internacional, la jurisprudencia, así como el reconocimiento a los interesados cuyos datos personales estén siendo transferidos de derechos efectivos y exigibles y de recursos administrativos y acciones judiciales que sean efectivos; (b) la existencia y el funcionamiento efectivo de una o varias autoridades de control independientes en el tercer país o a las cuales esté sujeta una organización internacional, con la responsabilidad de garantizar y hacer cumplir las normas en materia de protección de datos, incluidos poderes de ejecución adecuados, de asistir y asesorar a los interesados en el ejercicio de sus derechos, y de cooperar con las autoridades de control de la Unión y de los Estados miembros; y (c) los compromisos internacionales asumidos por el tercer país u organización internacional de que se trate, u otras obligaciones derivadas de acuerdos o instrumentos jurídicamente vinculantes, así como de su participación en sistemas multilaterales o regionales, en particular en relación con la protección de los datos personales.
La Comisión, tras haber evaluado la adecuación del nivel de protección, podrá decidir, mediante un acto de ejecución, que un tercer país, un territorio o uno o varios sectores específicos de un tercer país, o una organización internacional garantizan un nivel de protección adecuado de los datos personales. El acto de ejecución establecerá un mecanismo de revisión periódica, al menos cada cuatro años, que tenga en cuenta todos los acontecimientos relevantes en el tercer país o en la organización internacional. El acto de ejecución especificará su ámbito de aplicación territorial y sectorial, y, en su caso, determinará la autoridad o autoridades de control competente. El acto de ejecución se adoptará con arreglo al procedimiento establecido en el art. 5 del Reglamento (UE) n.º 182/2011.

[40] Con las «decisiones», el Tratado de Lisboa estableció un nuevo acto jurídico que vino a sumarse al catálogo de los ya existentes. Cabe distinguir dos categorías de decisiones: por un lado, decisiones dirigidas a determinados destinatarios y, por otro, decisiones generales que carecen de destinatario concreto (art. 288 TFUE). Mientras que las decisiones dirigidas a determinados destinatarios sustituyen las anteriores «decisiones» para regular casos concretos, las decisiones generales que carecen de destinatario específico abarcan una multitud de tipos de regulación que tienen una característica en común: no persiguen regular ningún caso concreto. *Vid.* DIETER-BORCHARDT, K., *El ABC del Derecho de la Unión Europea*, Oficina de Publicaciones de la Unión Europea, Bruselas, 2017, p. 111.

[41] Desde la entrada en vigor de la Directiva 95/46/CE, solamente quince Estados han obtenido una decisión de nivel adecuado son (en orden alfabético): (i) Andorra; (ii) Argentina; (iii) Canadá; (iv) Estados Unidos de América; (v) Guernsey; (vi) Isla de Man; (vii) Islas Feroe; (viii) Israel; (ix) Japón; (x) Jersey; (xi) Nueva Zelanda; (xii) Reino Unido; (xiii) República de Corea, (xiv) Suiza; y (xv) Uruguay. Como referencia histórica, la Comisión Europea emitió otras dos decisiones de adecuación en la misma fecha. La primera de ellas, la decisión 2000/519/CE de la Comisión, del 26 de julio de 2000, fue formulada con arreglo a la directiva 95/46/CE del Parlamento Europeo y del Consejo, relativa a la protección adecuada de los datos personales en Hungría. El hecho de que Hungría accediese, en 2004, a la Unión Europea dejó sin efecto la citada decisión de adecuación. Y, en segundo lugar, se emitió la decisión 2000/520/CE de la Comisión, del 26 de julio de 2000, con arreglo a la directiva 95/46/CE del Parlamento Europeo y del Consejo. En este caso, la decisión se ocupaba de la adecuación de la protección conferida por los principios de puerto seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de Estados Unidos de América. Esta decisión fue la primera en la materia, y por

Así las cosas, con fecha 23 de enero de 2019, tiene lugar la Decisión de ejecución (UE) 2019/419 de la Comisión, sobre el nivel adecuado en protección de datos proporcionado por Japón[42]. Su trascendencia no solamente se limita a ser la primera decisión adoptada tras el 25 de mayo de 2018, fecha a partir de la que se aplica de manera efectiva el RGPD[43]. Además, es también la primera decisión de adecuación que se refiere a una transferencia mutua de datos personales entre la Unión Europea y Japón, constituyendo la mayor área mundial de flujos de datos seguros[44].

La decisión se divide en ciento noventa considerandos, cuatro artículos y dos anexos, refiriéndose estos últimos, respectivamente, a las reglas complementarias adoptadas por la

el momento única, anulada por el Tribunal de Justicia de la Unión Europea. *Vid.* RECIO GAYO, M., «Nivel adecuado para transferencias internacionales de datos», en *Derecho PUCP,* núm. 83, 2019, pp. 224-225.

[42] El acuerdo de adecuación mutua con Japón forma parte de la estrategia de la UE en el ámbito de la protección y los flujos internacionales de datos, anunciada en enero de 2017. *Vid.* COMISIÓN EUROPEA, *Intercambio y la protección de los datos personales en un mundo globalizado,* Bruselas, 2017, 19 pp. [COM(2017) 7 final]. La UE y Japón concluyeron con éxito sus conversaciones sobre la adecuación recíproca el 17 de julio de 2018. Acordaron entonces reconocer mutuamente como adecuados sus sistemas respectivos de protección de datos, lo cual permitirá a los datos personales circular de modo seguro entre la UE y Japón. De esta forma, en julio de 2017, el presidente Juncker y el primer ministro Abe se comprometieron a adoptar la decisión de adecuación, en el marco de la voluntad común de la UE y de Japón de promover normas estrictas de protección de datos en la escena internacional.

[43] Posteriormente le han seguido Reino Unido, conforme a la Decisión de ejecución (UE) 2021/1773 de la Comisión, de 28 de junio de 2021 y la República de Corea, mediante la Decisión de ejecución (UE) 2022/254 de la Comisión, de 17 de diciembre de 2021.
Especialmente llamativo es el caso de Reino Unido, el cual tras el Brexit aboga abiertamente por acometer una profunda reforma del régimen de protección de datos, mediante la revisión y actualización de la denominada *Data Protection Act* (2018), norma nacida para asegurar su plena compatibilidad con el RGPD. El propósito de las autoridades británicas no es otro que el de aprovechar las oportunidades que ha generado el Brexit para crear un nuevo marco normativo que, si bien siga garantizando protección de los ciudadanos, asegure un crecimiento continuado en el uso de los datos personales y a la vez reduzca las cargas que deben soportar las empresas en relación con la recogida y tratamiento de este tipo de información. De este modo, todo parece indicar que las autoridades británicas tienen en mente impulsar una revisión completa del marco impuesto por el RGPD que, probablemente conducirá a la instauración de un sistema menos exigente que el establecido por el RGPD, como se intuye a la vista de algunos pasajes contemplados en su *National Data Strategy* (2020). Es evidente que cualquier reforma del marco de protección de datos británico tendrá efectos colaterales para el sistema de privacidad europeo, y obligará, en primer lugar, a revisar la Decisión de ejecución (UE) 2021/1773 de la Comisión, de 28 de junio de 2021. En este sentido, no debe obviarse que, en virtud del art. 3.1 de la misma, la Comisión aplicará en todo momento el principio de vigilancia continuada respecto al mantenimiento en ese país de un nivel de protección equivalente al establecido bajo el RGPD. Adicionalmente, el art. 3.4 de la misma decisión, señala que en caso de que la Comisión considere que existen indicios de que ya no puede equipararse el mencionado nivel de adecuación, la institución europea podría suspender, revocar o modificar tal decisión. Lo mismo podría ocurrir en caso de que la Comisión considerara insuficiente el nivel de colaboración de las autoridades británicas en relación con el seguimiento del cumplimiento de los términos definidos en la decisión de adecuación.

[44] Así lo reflejan las palabras de VĚRA JOUROVÁ, Comisaria de Justicia, Consumidores e Igualdad de Género: «[e]sta decisión de adecuación crea la mayor área mundial de flujos de datos seguros. Los datos de los europeos se beneficiarán de unas normas de privacidad estrictas cuando sus datos se transfieran a Japón. Nuestras empresas también se beneficiarán de un acceso privilegiado a un mercado de 127 millones de consumidores. La inversión en la protección de la vida privada es rentable; este acuerdo servirá de ejemplo para las futuras asociaciones en este ámbito clave y ayudará a establecer normas mundiales».

autoridad de control japonesa, la Comisión de Protección de la Información Personal (CPIP), y a las declaraciones, garantías y compromisos oficiales asumidos por el Gobierno japonés frente a la Comisión Europea[45].

Tras una breve introducción, la Comisión Europea dedica un apartado a la normativa aplicable por parte de los operadores económicos al tratamiento de datos personales[46]. En él, se refiere al marco de protección de datos japonés: así, se ocupa de su ámbito de aplicación material y personal; de las salvaguardas, derechos y obligaciones que se refieren tanto a los principios de protección de datos como a los derechos de los interesados y a las obligaciones de quienes tratan datos personales; de la supervisión y control de la aplicación de la normativa por una autoridad de protección de datos independiente[47]; del acceso y

[45] El Anexo I se detiene en establecer una serie de reglas complementarias en virtud de la Ley sobre protección de la información personal (Ley nº 57/2003) relativas al manejo de datos personales transferidos desde la Unión Europea sobre la base de una decisión de adecuación. Por su parte, el Anexo II ofrece una visión general del marco jurídico para la recogida y utilización de información personal por parte de las autoridades públicas japonesas con fines coercitivos y de seguridad nacional.

[46] Sobre la base del art. 45 RGPD y las Directrices del Comité Europeo de Protección de Datos relativas a la evaluación de la adecuación del nivel de protección ofrecido por un tercer país. *Vid.* COMITÉ EUROPEO DE PROTECCIÓN DE DATOS, *Referencias sobre adecuación*, aprobado el 28 de noviembre de 2017, revisado por última vez y aprobado el 6 de febrero de 2018.

Conviene recordar que, con posterioridad a la Sentencia Schrems II, el CEPD ha facilitado una serie de orientaciones «para garantizar un nivel de protección de sus datos esencialmente equivalente, será ante todo necesario que [el exportador] conozca exhaustivamente sus transferencias. También deberá comprobar que los datos transferidos son adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que se transfieren y tratan en el tercer país. También deberá determinar el instrumento de transferencia en el que se está basando para las transferencias. Si el instrumento de transferencia no es una decisión de adecuación, deberá verificar caso por caso si el Derecho o la práctica del tercer país de destino menoscaban o no las garantías contenidas en el instrumento de transferencia del art. 46 RGPD en el contexto de sus transferencias. Cuando el instrumento de transferencia del art. 46 RGPD no logre por sí solo para los datos personales transferidos un nivel de protección esencialmente equivalente, las medidas complementarias pueden paliar la deficiencia. Si no es capaz de encontrar o aplicar medidas complementarias eficaces que garanticen que los datos personales transferidos gozan de un nivel de protección esencialmente equivalente, no deberá empezar a transferir datos personales al tercer país de que se trate sobre la base del instrumento de transferencia que haya elegido. Si ya está realizando transferencias, se le pedirá que suspenda o ponga fin inmediatamente a la transferencia de datos personales. La autoridad de control competente está facultada para suspender o poner fin a las transferencias de datos personales al tercer país si no se garantiza la protección de los datos transferidos que exige el Derecho de la Unión, en particular los arts. 45 y 46 RGPD y la Carta de los Derechos Fundamentales». *Vid.* COMITÉ EUROPEO DE PROTECCIÓN DE DATOS, *Recomendaciones 01/2020 sobre medidas que complementan los instrumentos de transferencia para garantizar el cumplimiento del nivel de protección de los datos personales de la UE,* adoptadas el 10 de noviembre de 2020, p. 43.

[47] En Japón, la autoridad encargada de supervisar la aplicación de la Ley sobre protección de la información personal y de hacerla cumplir es la CPIP. Esta está compuesta por un presidente y ocho comisarios nombrados por el primer ministro con el acuerdo de las dos cámaras de la Dieta. La duración del mandato del presidente y de cada uno de los comisarios es de cinco años, con la posibilidad de renovación (art. 64 LPIP). Los comisarios solo pueden ser destituidos por una causa justificada, en un conjunto limitado de circunstancias excepcionales, y no pueden ejercer activamente actividades políticas. Por otra parte, en virtud de la LPIP, los comisarios a tiempo completo deben abstenerse de ejercer cualesquiera otras actividades remuneradas, o actividades empresariales. Todos los comisarios están sujetos asimismo a normas internas que les impide participar en las deliberaciones en caso de un posible conflicto de intereses. La CPIP está asistida por una Secretaría, dirigida por un secretario general y creada

utilización por parte de las autoridades públicas japonesas de datos personales transferidos desde la Unión Europea, tanto a efectos de control de la aplicación del derecho penal como a efectos de seguridad nacional.

A continuación, los considerandos hacen referencia a la conclusión sobre el nivel de protección adecuado proporcionado por Japón para la transferencia de datos desde la Unión Europea. En los mismos no solamente se pone de relieve que *«la LPIP, complementada por las Reglas complementarias recogidas en el Anexo I, junto con las declaraciones, las garantías y los compromisos oficiales que figuran en el Anexo II, garantizan un nivel de protección de los datos personales transferidos desde la Unión Europea "sustancialmente equivalente" al que garantiza el Reglamento (UE) 2016/679, sino también que los mecanismos de supervisión y las vías de reparación previstas en el Derecho japonés permiten identificar y sancionar en la práctica las infracciones cometidas por los OEMIP destinatarios y ofrecen al interesado remedios legales para obtener acceso a los datos personales que le conciernen y, en su caso, su rectificación y supresión»* (Considerandos 171 y 172). Así mismo, se hace alusión a la actuación de las autoridades de protección de datos en la Unión Europea, en la medida en que pudieran recibir consultas o reclamaciones, de las que los Estados miembros deberán informar a la Comisión Europea (Considerando 178). Asimismo, se menciona que la información sobre cualquier novedad relevante para la decisión de adecuación debe ser proporcionada por las autoridades japonesas. Finalmente, se hace referencia a la supervisión continua por parte de la Comisión Europea de que Japón proporciona el nivel adecuado.

Por lo que se refiere a la revisión de la decisión, se predispone que, de conformidad con el art. 45.3 RGPD, se revise periódicamente si las constataciones relativas a la adecuación del nivel de protección garantizado por Japón siguen estando justificadas desde el punto de vista factual y legal (considerando 180). Adicionalmente, se refleja la potestad de la Comisión Europea de suspender la decisión de adecuación[48] si concluyera sobre la base de las comprobaciones periódicas y *ad hoc* o de cualquier información disponible que el nivel adecuado de protección no pudiera considerarse equivalente en lo esencial al de la Unión Europea (Considerando 184).

con el fin de llevar a cabo las tareas asignadas a la CPIP (art. 70 LPIP). Tanto los comisarios como el conjunto de los funcionarios de la Secretaría están sujetos a normas estrictas en materia de confidencialidad (arts. 72 y 82 LPIP).

[48] Si, transcurrido el plazo especificado, las autoridades japonesas competentes no logran demostrar satisfactoriamente que la Decisión sigue basándose en un nivel de protección adecuado, la Comisión debe, en aplicación del art. 45.5 RGPD, iniciar el procedimiento conducente a la suspensión parcial o total o a la derogación de la presente Decisión. Alternativamente, la Comisión debe iniciar el procedimiento tendente a la modificación de la presente Decisión, en particular sometiendo las transferencias de datos a condiciones adicionales o limitando el alcance de la constatación de adecuación únicamente a las transferencias de datos para los cuales esté asegurada la continuidad de la protección a tenor del art. 44 del RGPD.

4.3. La aprobación de la Ley de Protección de la Información Personal por parte de la República Popular China (中华人民共和国个人信息保护法) y su extraordinaria similitud con el RGPD

El 20 de agosto de 2021, el Comité Permanente de la XIII Asamblea Popular Nacional de la República Popular de China aprobó la Ley de Protección de la Información Personal[49] (en adelante, LPIP), la cual entró en vigor el 1 de noviembre de 2021, en el marco de un paquete normativo más ambicioso compuesto por la Ley de Ciberseguridad y la Ley de Seguridad de Datos, promulgadas recientemente.

La LPIP regula el tratamiento de la información personal de las personas físicas siguiendo un camino similar al experimentado en el continente europeo, no en vano, la citada norma guarda una extraordinaria similitud con el RGPD[50]. Como se desprende de su art. 1, la Ley nace con la finalidad de proteger los derechos e intereses en materia de información personal de las personas físicas[51], normalizar las actividades de tratamiento de la información personal y promover su uso racional.

A tal fin, la LPIP no solamente se aplicará a las actividades de procesamiento de información personal que se produzcan dentro de las fronteras de la República Popular China. El art. 3 LPIP es claro al señalar que la norma será igualmente de aplicación cuando la información personal de los ciudadanos chinos se procese fuera de la República Popular China con alguno de los siguientes propósitos: (i) proporcionar productos o servicios destinados a personas físicas que radican en el seno de la República Popular China; (ii) analizar o evaluar las actividades de las personas físicas dentro de las fronteras; u (iii) otras circunstancias previstas en leyes o reglamentos administrativos. Se establece así una suerte de alcance extraterritorial de la norma sobre ciertas actividades de tratamiento que tienen lugar fuera

[49] Dicha Ley es la primera de estas características en la República Popular China, dado que busca establecer el consentimiento de las personas para el procesamiento de su información personal, algo inédito hasta la fecha. La norma está compuesta por 74 artículos, dispuestos en ocho capítulos como sigue: Capítulo I: Disposiciones generales; Capítulo II: Normas de tratamiento de datos personales; Sección 1: Disposiciones ordinarias; Sección 2: Disposiciones para el tratamiento de información personal sensible; Sección 3: Disposiciones especiales sobre el tratamiento de información personal por parte de las autoridades estatales; Capítulo III: Reglas sobre el suministro transfronterizo de información personal; Capítulo IV: Derechos de las personas físicas en las actividades de tratamiento de datos personales; Capítulo V: Deberes de los encargados de los datos personales; Capítulo VI: Autoridad de control encargada del cumplimiento de los deberes y responsabilidades en materia de protección de datos personales; Capítulo VII: Responsabilidad jurídica; y Capítulo VIII: Disposiciones complementarias. El texto original de la norma se encuentra disponible en: https://bit.ly/3OUQXNt

[50] En efecto, como insiste en señalar buena parte de la doctrina, «esta nueva Ley tiene una clara influencia del Reglamento General de Protección de Datos, pero también incluye novedosas diferencias». *Vid.* BĂDIN, L. y ROBLES ALBERO, J.R., «Nueva Ley de Privacidad en China: aspectos más relevantes», en *La Ley privacidad*, núm. 10, 2021, p. 4.

[51] De conformidad con su art. 2, los datos personales de las personas físicas gozan de protección legal; ninguna organización o individuo puede infringir los derechos e intereses de las personas físicas vinculados con su información personal.

de las fronteras de la República Popular China y que conciernen a interesados que están ubicados en dicho país, como sucede en el caso del RGPD.

De igual forma, los arts. 5 a 7 LPIP contemplan que en el tratamiento de información personal debe seguir los principios de licitud, lealtad, necesidad y buena fe, limitación del tratamiento y minimización de datos, publicidad y transparencia[52]. Adicionalmente, el art. 9 LPIP establece que los responsables del tratamiento deberán rendir cuentas acerca de las actividades de tratamiento realizadas (responsabilidad proactiva) y adoptarán las medidas necesarias para garantizar la seguridad de la información personal objeto de tratamiento.

Por su parte, el art. 9 LPIP introduce una suerte de principio de «responsabilidad proactiva», al señalar que los responsables del tratamiento de información personal deberán adoptar las medidas necesarias para salvaguardar la seguridad de los datos personales que manejen.

Especialmente relevantes resultan las previsiones contenidas en el art. 13 LPIP, en el que se enumeran las diferentes bases legales que permitirán acometer actuaciones de tratamiento de datos, a saber: (a) cuando se haya obtenido el consentimiento de los interesados; (b) cuando sea necesario para celebrar o cumplir un contrato en el que el individuo sea una parte interesada, o cuando sea necesario para llevar a cabo la gestión de recursos humanos de acuerdo con normas y estructuras laborales legalmente formuladas y contratos colectivos legalmente celebrados; (c) cuando sea necesario para cumplir con los deberes y responsabilidades legales u obligaciones legales; (d) cuando sea necesario para responder a incidentes repentinos de salud pública o proteger la vida y la salud de las personas físicas, o garantizar la seguridad de su propiedad en condiciones de emergencia; (e) cuando sea necesario procesar información personal dentro de un alcance razonable para implementar informes de noticias, supervisión de la opinión pública y otras actividades similares para el interés público; (f) cuando se trate de datos personales divulgados por las propias personas o de otra forma ya divulgados lícitamente, dentro de un alcance razonable de conformidad

[52] De conformidad con el art. 6 LPIP, el tratamiento de información personal deberá tener una finalidad clara y razonable, y utilizar medios que afecten de la menor forma posible a los derechos e intereses individuales. A este respecto, el art. 17 LPIP establece que quienes procesen información personal deberán, antes de hacerlo, notificar, utilizando un lenguaje claro y de fácil comprensión, expresamente lo siguiente: (i) el nombre y método de contacto del responsable; (ii) la finalidad, los métodos de procesamiento, las categorías de IP procesada y el período de retención; (iii) los métodos y procedimientos para que las personas ejerzan sus derechos; y (iv) los elementos adicionales que dispongan las leyes o reglamentos administrativos. . A su vez, el art. 19 LPIP señala que la información deberá ser conservada por el período más breve necesario para cumplir con el propósito informado.

Por su parte, el art. 8 LPIP introduce el principio de calidad de la información personal, al consignar que los responsables del tratamiento garanticen la calidad de la información y eviten los efectos adversos que puede generar, sobre los derechos e intereses individuales, el tratamiento de información personal incompleta o inexacta.

con las disposiciones de la Ley; y (g) cuando exista cualquier otra circunstancia prevista en las leyes y reglamentos administrativos[53].

De igual forma, el art. 21 LPIP introduce la figura del «encargado de tratamiento», al prever que cuando los responsables de las operaciones de procesamiento de la información personal encomienden el tratamiento de datos personales, deberán: (i) celebrar necesariamente un acuerdo con la persona encargada en el que se reflejen al menos la finalidad del tratamiento encomendado, el plazo, el método de tratamiento, las categorías de datos personales objeto de tratamiento, las medidas de protección a adoptar, así como los derechos y deberes de ambas partes, etc.; y (ii) llevar a cabo la supervisión de las actividades de tratamiento de información personal por parte del encargado[54].

Llamativas son también las previsiones relativas a las transferencias de información personal contenidas en la norma objeto de estudio. A este respecto, el art. 38 LPIP establece que cuando los responsables del tratamiento necesiten proporcionar información personal fuera de las fronteras de la República Popular China, deberán cumplir una de las siguientes condiciones: (a) superar una evaluación de seguridad dirigida por el Departamento de Ciberseguridad e Informatización del Estado, de conformidad con las previsiones del art. 40 LPIP; (b) someterse a un proceso de certificación de protección la información personal realizada por un organismo especializado de acuerdo con las disposiciones del Departamento de Ciberseguridad e Informatización del Estado; (c) celebrar un contrato con la parte receptora de la información personal en el extranjero, de conformidad con un contrato estándar formulado por el Departamento de Ciberseguridad e Informatización del Estado, en el que se reflejen los derechos y responsabilidades a los que quejan sujetos ambas partes; y (d) estar en disposición de cumplir otras condiciones previstas en leyes, reglamentos administrativos o directrices formuladas por el Departamento de Ciberseguridad e Informatización del Estado[55].

[53] De conformidad con otras disposiciones contenidas en la Ley, cuando se traten datos personales se deberá obtener necesariamente el consentimiento individual, salvo cuando medie alguna de las bases legales contenidas en los incisos b) a g) del art. 13 LPIP.

[54] Así mismo, el citado precepto continúa su exposición señalando que los encargados de tratamiento utilizarán la información personal de conformidad con el clausulado del acuerdo suscrito con el responsable del tratamiento, lo que impide tratar la información personal con fines o métodos distintos a los estipulados en el acuerdo de encargo de tratamiento. Si, por cualquier circunstancia, el contrato de encargado de tratamiento no produjera efectos, fuera decretado nulo, hubiera sido cancelado o rescindido, el encargado de tratamiento deberá devolver o eliminar la información personal al responsable del tratamiento, no pudiendo retenerla en su poder. Adicionalmente, se prevé que el encargado del tratamiento de la información personal no pueda proceder a la cesión de la misma a terceras personas sin el previo consentimiento del responsable del tratamiento.

[55] Dichas disposiciones deben aplicarse cuando los tratados o acuerdos internacionales que la República Popular China haya celebrado o suscrito contengan disposiciones relevantes, tales como condiciones para el suministro de datos personales fuera de las fronteras del Estado. Los responsables del tratamiento de la información personal deben adoptar las medidas necesarias para garantizar que las operaciones de tratamiento de la información

En lo que respecta a los derechos subjetivos de los interesados en relación con las operaciones de tratamiento de información personal, se reconocen los derechos de acceso, limitación y oposición (art. 44 LPIP), así como el derecho a solicitar la rectificación de la información incompleta o inexacta[56] que esté siendo objeto de tratamiento de datos personales (art. 46 LPIP).

Asimismo, la norma también contempla entre las disposiciones una serie de obligaciones para los responsables del tratamiento de la información personal. De esta forma, en virtud del art. 51 LPIP, los responsables del tratamiento deberán, en función de la finalidad del tratamiento de los datos personales, determinar las metodologías de tratamiento, las categorías de datos personales, así como la influencia que dichas operaciones de tratamiento pueden ejercer sobre los derechos e intereses de las personas, los posibles riesgos de seguridad existentes, etc. Adicionalmente, deberán adoptar las siguientes medidas para garantizar que el tratamiento de la información personal se ajuste a las disposiciones de las leyes y los reglamentos administrativos, y evitar el acceso no autorizado, así como la fuga, distorsión o pérdida de la información personal: (i) diseñar estructuras internas de gestión y reglas de funcionamiento; (ii) implementar la gestión categorizada de información personal; (iii) adoptar las medidas técnicas de seguridad correspondientes, tales como encriptación, anonimización, etc.; (iv) determinar razonablemente los límites operativos para el tratamiento de la información personal e impulsar la formación continuada y la capacitación en materia de seguridad de los empleados; (v) fomentar la implementación de planes de respuesta a incidentes de seguridad de la información personal; y (vi) adoptar las restantes medidas previstas en las leyes o reglamentos administrativos.

Con la finalidad de supervisar estas exigencias, así como las restantes obligaciones y deberes impuestos por la normativa objeto de estudio[57], el art. 60 LPIP designa como

personal desarrollada por la parte receptora extranjera alcancen el estándar de protección de información personal provisto en la LPIP.

[56] Por su parte, el art. 45 LPIP dibuja los contornos propios de lo que podríamos definir como un atisbo de derecho a la portabilidad de la información personal, toda vez que reconoce el derecho de los interesados de consultar y copiar aquellos datos personales que estén siendo objeto de operaciones de tratamiento, debiendo los responsables y encargados de tratamiento proporcionar la misma de manera oportuna, añadiendo además que *«cuando las personas soliciten que su información personal sea transferida a otro responsable de tratamiento de información personal que ellos designen, cumpliendo las condiciones del Departamento de Ciberseguridad e Informatización del Estado, los responsables de la información personal deberán proporcionar un canal para transferirla».*

[57] Entre las funciones del Departamento de Ciberseguridad e Información del Estado (art. 62 LPIP), destacan las siguientes: (i) formular normas y estándares concretos de protección de la información personal; (ii) formular reglas y estándares especializados de protección de información personal para pequeños responsables del tratamiento de información personal y nuevas tecnologías y nuevas aplicaciones para el tratamiento de información personal sensible, reconocimiento facial, inteligencia artificial, etc.; (iii) apoyar la investigación, el desarrollo y la adopción generalizada de tecnología de autenticación de identidad electrónica segura y conveniente, y promover la construcción de servicios públicos de autenticación de identidad en línea; (iv) avanzar en la

autoridad encargada de la planificación y coordinación integral de las labores de protección de datos personales y las labores de supervisión y gestión conexas al Departamento de Ciberseguridad e Informatización del Estado[58].

Finalmente, la norma destina su Capítulo VII a determinar el régimen de responsabilidad jurídica y el marco sancionador frente a aquellos supuestos de tratamiento de la información personal que vulneren las disposiciones contempladas en el instrumento jurídico objeto de estudio. De esta forma, el art. 66 LPIP establece la posibilidad de que las autoridades encargadas de proteger la información personal puedan ordenar la corrección, confiscar ingresos y ordenar la suspensión provisional o la terminación de la prestación de servicios. En lo que a sanciones pecuniarias se refiere, cuando se rechacen o rehúsen adoptar las medidas correctivas propuestas por la autoridad competente, se impondrá adicionalmente una multa que, en ningún caso, podrá superior el 1 millón de yuanes (el equivalente a 145.355 euros). Así mismo, se prevé una sanción económica que oscilará entre los 10.000 y los 1000.000 yuanes para aquellas personas que resulten directamente responsable de la infracción de la norma[59].

Sin embargo, cuando las infracciones de la LPIP revistan carácter grave, los departamentos provinciales o de nivel superior que cumplen con los deberes y responsabilidades de protección de la información personal podrán ordenar la corrección, confiscar ingresos ilegales e imponer una multa por un importe no superior a 50 millones de yuanes (el equivalente a 7.267.769 de euros) o del 5 % de los ingresos anuales[60].

En suma, pese a las profundas diferencias políticas, institucionales y culturales existentes, resulta innegable reconocer el semejante parecido que guarda la novedosa LPIP de la

construcción de sistemas de servicios para socializar la protección de la información personal y apoyar a las organizaciones relevantes para lanzar servicios de evaluación y certificación de la protección de la información personal; y (v) perfeccionar los mecanismos de denuncia y reclamaciones en materia de protección de la información personal.

[58] Paralelamente, el citado precepto reconoce la existencia de otras autoridades que desempeñaran, de igual forma, dentro de sus respectivos ámbitos competenciales, labores de protección, supervisión y gestión de la información personal. Nos estamos refiriendo a los departamentos pertinentes del Consejo de Estado y a los gobiernos populares a nivel de condado (art. 61 LPIP). Dichas autoridades reciben el nombre de «Departamentos que cumplen con los deberes y responsabilidades de protección de la información personal».

[59] Se establece así una sanción directa para el responsable del tratamiento que oscilará entre los 1.453 y los 14.535 euros.

[60] También podrán ordenar la suspensión de las actividades comerciales relacionadas con el tratamiento de información personal o el cese del negocio para su rectificación, e informar al departamento competente correspondiente para la cancelación de las licencias administrativas o comerciales. Al igual que ocurría en el supuesto anterior, la persona que resulte directamente responsable de la infracción, así como el restante personal directamente responsable serán sancionados económicamente con una cuantía que oscilará entre los 100.000 y el 1 millón de yuanes. También puede decretarse la prohibición de ocupar cargos de dirección, supervisión, gerencia de alto nivel, u oficial de protección de información personal durante un período determinado.

República Popular China con el RGPD, hito normativo trascendental que ha sido capaz de irradiar sus elevados estándares de tutela jurídica de la privacidad, traspasando ampliamente los contornos propios de las fronteras europeas, hasta llegar a convertirse en el estándar internacional en la materia[61].

5. CONCLUSIONES

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.

En efecto, 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.

[61] *Vid.* DOMÍNGUEZ ÁLVAREZ, J.L., *Tratado de protección de datos personales: pasado, presente y futuro de la tutela jurídica de los derechos de la privacidad*, Colex, A Coruña, 2023, p. 259.

Finalmente, conviene reseñar que 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.

6. REFERENCIAS BIBLIOGRÁFICAS

- AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, *Estándares Internacionales sobre Protección de Datos Personales y Privacidad,* Madrid, 2009.
- BĂDIN, L. y ROBLES ALBERO, J.R., «Nueva Ley de Privacidad en China: aspectos más relevantes», en *La Ley privacidad*, núm. 10, 2021.
- BIURRUN ABAD, F.J., «"Accountability" o responsabilidad proactiva en el Reglamento General de Protección de Datos», en *Actualidad Jurídica Aranzadi*, núm. 927, 2017.
- BRADFORD, A., *The Brussels Effect: How the European Union Rules the World*, Oxford University Press, Nueva York, 2020.
- 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,* Bruselas, 2021 [COM(2021) 206 final].
  * *Intercambio y la protección de los datos personales en un mundo globalizado,* Bruselas, 2017 [COM(2017) 7 final].
- COMITÉ EUROPEO DE PROTECCIÓN DE DATOS, *Dictamen conjunto 5/2021 sobre la 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),* adoptado el 18 de junio de 2021.
  * *Recomendaciones 01/2020 sobre medidas que complementan los instrumentos de transferencia para garantizar el cumplimiento del nivel de protección de los datos personales de la UE,* adoptadas el 10 de noviembre de 2020.

* *Referencias sobre adecuación*, aprobado el 28 de noviembre de 2017, revisado por última vez y aprobado el 6 de febrero de 2018.

- DE MIGUEL ASENSIO, P.A., «Propuesta de Reglamento sobre Inteligencia Artificial», en *La Ley Unión Europea*, núm. 92, 2021.
- DIETER-BORCHARDT, K., *El ABC del Derecho de la Unión Europea*, Oficina de Publicaciones de la Unión Europea, Bruselas, 2017.
- DOMÍNGUEZ ÁLVAREZ, J.L., *Tratado de protección de datos personales: pasado, presente y futuro de la tutela jurídica de los derechos de la privacidad*, Colex, A Coruña, 2023.
- ESTEPA MONTERO, M., «El principio de responsabilidad proactiva o rendición de cuentas como informador del régimen jurídico de la protección de datos de las personas físicas», en *Anuario Jurídico y Económico Escurialense*, núm. LV, 2022.
- GRUPO DE TRABAJO DEL ARTÍCULO 29, *Dictamen 3/2010, sobre el principio de responsabilidad,* adoptado el 13 de julio de 2010 [WP 173].
- HUERGO LORA, A., «El proyecto de Reglamento sobre la Inteligencia Artificial», en *Almacén de Derecho*, 2021.
- MARGARITA PORCELLO, A., «La protección de los datos personales en el entorno digital. Los estándares de protección de datos en los países iberoamericanos», en *Quaestio Iuris*, vol. 12, núm. 2, 2019.
- MARTÍ DEL MORAL, A., «La protección de datos personales en Europa e Iberoamérica», en CERRILLO i MARTÍNEZ, A. (Dir.), *La Administración Digital,* Dykinson, Madrid, 2022.
- PIÑAR MAÑAS, J.L. «Hacia un nuevo modelo europeo de protección de datos», en PIÑAR MAÑAS, J.L. (Dir.), Reglamento general de protección de datos: hacia un nuevo modelo europeo de privacidad, Reus, Madrid, 2016.
- PIÑAR MAÑAS, J.L. y MONTULL CREMADES, M.A., *La Red Iberoamericana de Protección de Datos: Declaraciones y documentos*, Tirant lo Blanch, Valencia, 2006.
- RECIO GAYO, M., «Nivel adecuado para transferencias internacionales de datos», en *Derecho PUCP,* núm. 83, 2019.
- RED IBEROAMERICANA DE PROTECCIÓN DE DATOS*, Plan Estratégico 2021-2025: Nuevos tiempos para la privacidad. Nuevas estrategias*, Madrid, 2020.
  * *Estándares de protección de datos personales,* Madrid, 2017.
  * *Estándares de protección de datos personales,* Madrid, 2007.
- USTARÁN, E. y GARCÍA, P., «Transferencias internacionales de datos», en RALLO LOMBARTE, A. (Dir.), *Tratado de protección de datos. Actualizado con la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales,* Tirant lo Blanch, Valencia, 2019.