

N/REF: 0085/2021

Examinada su solicitud de informe, remitida a este Gabinete Jurídico, referente al Anteproyecto de Ley de Medidas de Eficiencia Digital del Servicio Público de Justicia, por la que se transpone al ordenamiento jurídico español la Directiva (UE) 2019/1151 del Parlamento Europeo y del Consejo, de 20 de junio de 2019, por la que se modifica la Directiva (UE) 2017/1132 en lo que respecta a la utilización de herramientas y procesos digitales en el ámbito del Derecho de sociedades, solicitado con carácter urgente de esta Agencia Española de Protección de Datos (AEPD) de conformidad con lo dispuesto en el artículo 47 de la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales (LOPDGDD), en relación con el artículo 57.1, letra c), 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 (Reglamento General de Protección de Datos), y 5 b) del Estatuto de la Agencia, aprobado por Real Decreto 389/2021, de 1 de junio, cúmpleme informarle lo siguiente:

Antes de entrar a analizar el texto sometido a informe es preciso señalar que, habida cuenta de la fundamentación legal del informe que inmediatamente va a evacuarse y su carácter preceptivo, a tenor de lo dispuesto en las normas que acaban de señalar, debería indicarse en la Exposición de Motivos de la norma que la misma ha sido sometida al previo informe de la Agencia Española de Protección de Datos.

Tal y como resulta de la Exposición de Motivos y de la Memoria de Análisis de Impacto Normativo, el anteproyecto continúa apostando por la transformación digital iniciada por las normas que lo han precedido, singularmente la Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información por parte de los ciudadanos y profesionales en sus relaciones con la Administración de Justicia, y cuyo proceso de implantación se ha visto acelerado como consecuencia de la Pandemia del COVID-19, con nuevas medidas en ámbitos como la celebración telemática de vistas y otros actos procesales, que se recogieron en la Ley 3/2020, de 18 de septiembre, de medidas procesales y organizativas para hacer frente al COVID-19 en el ámbito de la Administración de Justicia.

Con estos precedentes, el anteproyecto pretende ser «una herramienta jurídica completa, útil, transversal y con la capacidad suficiente para dotar a los Tribunales de un marco legal coherente y lógico en el que la relación digital se

descubra como una relación ordinaria y habitual, siendo la tutela judicial efectiva la misma, pero hallando bajo esta cobertura de normas y reglas, un nuevo cauce más veloz y eficaz, que coadyuvará a una mejor satisfacción de los derechos de los ciudadanos», por lo que el mismo «se erige como un instrumento para promover y facilitar:

- La intervención de los ciudadanos en las actuaciones judiciales mediante sistemas de intermediación digital, simplificándose la relación con la Administración de Justicia.
- La relación entre los distintos operadores (órganos judiciales, profesionales y colaboradores) con la Administración de Justicia, al ser todos ellos responsables, en su medida, del correcto funcionamiento del Servicio Público de Justicia (integrados bajo el empleo generalizado del Expediente Judicial Electrónico, herramienta central para comprender la Justicia Digital».

Asimismo, se persigue reducir los plazos para el dictado de una resolución judicial, para lo que «se potencia la tramitación tecnológica del expediente a través de la realización de actuaciones con gestión automatizada, recurribles y situadas sobre la base de criterios legales objetivos y públicos».

Por otro lado, otro de los objetivos importantes perseguidos es «la obtención inmediata y utilización inteligente de los datos» por lo que «se realiza una apuesta clara y decisiva por el empleo racional de los mismos como evidencia y certidumbre al servicio de la planificación y elaboración de estrategias que coadyuven a una mejor y más eficaz política pública de Justicia».

A este respecto, destaca que uno de los ejes vertebradores de la reforma es la «orientación al dato», ya que como señala la Exposición de Motivos, «se potencia el Expediente Judicial Electrónico mediante un cambio de paradigma, pasando de la orientación al documento a la orientación al dato. Esto supone un gran avance respecto de la Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia, que hace una década se planteaba como objetivo la transición del papel a lo digital, siendo así que se trata ahora de lograr mejoras sustanciales ya en el entorno de lo digital».

En definitiva, tal y como se resume en la MAIN, «el anteproyecto se erige como instrumento para:

ü Establecer las reglas y dar cobertura jurídica a la transformación digital del Servicio Público de Justicia, asegurando la existencia de una pluralidad de servicios digitales accesibles al ciudadano, orientando a los datos los sistemas de Justicia y reforzando la seguridad jurídica digital.

ü□Posibilitar el trabajo deslocalizado a Jueces/as, Fiscales, Letrados/as de la Administración de Justicia, Médicos Forenses y resto de funcionarios y funcionarias al servicio de la Administración de Justicia.

ü□Asegurar la interoperabilidad, tanto en la Administración de Justicia como de ésta con el resto de Administraciones Públicas; asegurando el tratamiento de datos a fines de estadística judicial, toma de decisiones y publicidad en formato de datos abiertos.

ü□Garantizar el derecho de acceso a la Justicia a todos los ciudadanos/as.

ü□Ofrecer el mejor servicio público posible a la ciudadanía, reduciendo las dificultades que pueden derivarse del uso de la propia tecnología».

Por otro lado, el anteproyecto procede, a la incorporación a nuestro Derecho de la Directiva (UE) 2019/1151 del Parlamento Europeo y del Consejo, de 20 de junio de 2019, por la que se modifica la Directiva (UE) 2017/1132 en lo que respecta a la utilización de herramientas y procesos digitales en el ámbito del Derecho de sociedades, conocida como “Directiva de digitalización de sociedades” o “Directiva de herramientas digitales”, que requiere la modificación del régimen de constitución telemática vigente en nuestro ordenamiento jurídico en algunos aspectos, para poder cumplir con el mandato del legislador europeo de contemplar un procedimiento íntegramente online, aplicable tanto al momento de constitución, como a las modificaciones societarias posteriores y al registro de sucursales por parte de solicitantes que sean ciudadanos de la Unión Europea. A ello responden las modificaciones que se introducen en el Código de Comercio, en el texto refundido de la Ley de Sociedades de Capital (TRLSC) y en el Reglamento del Registro Mercantil (RRM).

Por último, interesa destacar especialmente, por su afectación a esta Agencia, las modificaciones que la disposición final decimocuarta introduce en ciertos preceptos, todos ellos de rango ordinario, de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, con motivo de la corrección de errores del Reglamento Europeo sobre Protección de Datos publicada en el DOUE del día 4 de marzo de 2021, y en consecuencia la eliminación del apercibimiento del catálogo de sanciones a imponer a responsables y encargados, sustituyéndolo por la realización de un requerimiento. Además, la reforma introduce un nuevo artículo que habilita y regula la realización de actuaciones de investigación a través de sistemas digitales, y se aumenta de nueve a doce meses la duración máxima del procedimiento sancionador, y de doce a dieciocho meses la de las actuaciones previas de investigación. Por último, se introduce una previsión en cuanto a la notificación de la admisión a trámite en aquellos procedimientos con un elevado

número de reclamaciones, y el establecimiento de modelos obligatorios de reclamación ante la Agencia Española de Protección de Datos.

I

En lo que a la materia de protección de datos personales respecta, la norma a la que debe ajustarse el anteproyecto es el 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 por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos, RGPD), plenamente aplicable desde el 25 de mayo de 2018, así como a la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales y, en su caso, a la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales.

Tal y como resulta de los antecedentes destacados, el anteproyecto de ley objeto de informe contiene un ambicioso proyecto dirigido a la transformación digital del Servicio Público de Justicia, que va a tener una notable incidencia en los tratamientos de datos personales de las personas físicas, dada la amplitud con la que dicho concepto se recoge en el artículo 4.1. del RGPD, y que afectará, asimismo, a categorías especiales de datos, datos penales y sanciones administrativas, objeto de una mayor protección dada la mayor incidencia de dichos datos en los derechos, libertades e intereses de los afectados.

Por ello, la primera conclusión que se alcanza es que la protección de los datos personales debe figurar como uno de los principios básicos que ha de guiar la utilización de las tecnologías de la información en este ámbito, reiterándose en todos los artículos en los que se hace referencia a los principios aplicables en este ámbito. Asimismo, el derecho a la protección de datos personales debe recogerse como un derecho de la ciudadanía y de los profesionales que se relacionan con la Administración de Justicia.

II

Conforme al artículo 236 bis de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial:

1. El tratamiento de los datos personales podrá realizarse con fines jurisdiccionales o no jurisdiccionales. Tendrá fines jurisdiccionales

el tratamiento de los datos que se encuentren incorporados a los procesos que tengan por finalidad el ejercicio de la actividad jurisdiccional.

2. El tratamiento de los datos personales en la Administración de Justicia se llevará cabo por el órgano competente y, dentro de él, por quien tenga la competencia atribuida por la normativa vigente.

Por lo tanto, hay que tener en cuenta que los tratamientos que se realizan en el ámbito de la Administración de Justicia pueden tener fines jurisdiccionales, lo que determina la competencia en materia de protección de datos del Consejo General del Poder Judicial y de la Fiscalía General del Estado, y fines no jurisdiccionales, competencia de esta AEPD (artículo 236 octíes de la LOPJ), por lo que sería deseable la participación coordinada de todas estas autoridades en el trámite de elaboración de la presente norma.

III

Sin perjuicio de lo anterior, para el adecuado cumplimiento de la normativa de protección de datos, debe partirse del principio de responsabilidad proactiva y de protección de datos desde el diseño y por defecto, que se recoge en el artículo 25 del RGPD:

1. Teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados.

2. El responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. Tales medidas garantizarán en particular que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas.

3. Podrá utilizarse un mecanismo de certificación aprobado con arreglo al artículo 42 como elemento que acredite el cumplimiento de las obligaciones establecidas en los apartados 1 y 2 del presente artículo.

A este respecto hay que tener en cuenta que el RGPD ha supuesto un cambio de paradigma al abordar la regulación del derecho a la protección de datos personales, que pasa a fundamentarse en el principio de «accountability» o «responsabilidad proactiva» tal y como ha señalado reiteradamente la AEPD (Informe 17/2019, entre otros muchos) y se recoge en la Exposición de motivos de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD): “la mayor novedad que presenta el Reglamento (UE) 2016/679 es la evolución de un modelo basado, fundamentalmente, en el control del cumplimiento a otro que descansa en el principio de responsabilidad activa, lo que exige una previa valoración por el responsable o por el encargado del tratamiento del riesgo que pudiera generar el tratamiento de los datos de carácter personal para, a partir de dicha valoración, adoptar las medidas que procedan”. Dentro de este nuevo sistema, es el responsable del tratamiento el que, a través de los instrumentos regulados en el propio RGPD como el registro de actividades del tratamiento, el análisis de riesgos o la evaluación de impacto en la protección de datos personales, debe garantizar la protección de dicho derecho mediante el cumplimiento de todos los principios recogidos en el artículo 5.1 del RGPD, documentando adecuadamente todas las decisiones que adopte al objeto de poder demostrarlo.

Asimismo, partiendo de dicho principio de responsabilidad proactiva, dirigido esencialmente al responsable del tratamiento, y al objeto de reforzar la protección de los afectados, el RGPD ha introducido nuevas obligaciones exigibles no sólo al responsable, sino en determinados supuestos, también al encargado del tratamiento, quien podrá ser sancionado en caso de incumplimiento de las mismas.

Por consiguiente, siendo los principales destinatarios de las obligaciones recogidas en el RGPD los responsables y encargados, no obstante, su observancia supone la necesidad de adopción de determinadas conductas por parte del legislador nacional, al objeto de garantizar el cumplimiento del RGPD y, en definitiva, la adopción de garantías suficientes para la protección del derecho fundamental, singularmente cuando se trate de tratamientos de datos personales legitimados como consecuencia del cumplimiento de obligaciones legales o para el cumplimiento de una misión de interés público o el ejercicio de potestades públicas, como ocurre en el presente caso.

Esta posibilidad está expresamente reconocida en los apartados 2 y 3 del artículo 6 del RGPD:

2. Los Estados miembros podrán mantener o introducir disposiciones más específicas a fin de adaptar la aplicación de las normas del presente Reglamento con respecto al tratamiento en cumplimiento del apartado 1, letras c) y e), fijando de manera más

precisa requisitos específicos de tratamiento y otras medidas que garanticen un tratamiento lícito y equitativo, con inclusión de otras situaciones específicas de tratamiento a tenor del capítulo IX.

3. La base del tratamiento indicado en el apartado 1, letras c) y e), deberá ser establecida por:

- a) el Derecho de la Unión, o
- b) el Derecho de los Estados miembros que se aplique al responsable del tratamiento.

La finalidad del tratamiento deberá quedar determinada en dicha base jurídica o, en lo relativo al tratamiento a que se refiere el apartado 1, letra e), será necesaria para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento. Dicha base jurídica podrá contener disposiciones específicas para adaptar la aplicación de normas del presente Reglamento, entre otras: las condiciones generales que rigen la licitud del tratamiento por parte del responsable; los tipos de datos objeto de tratamiento; los interesados afectados; las entidades a las que se pueden comunicar datos personales y los fines de tal comunicación; la limitación de la finalidad; los plazos de conservación de los datos, así como las operaciones y los procedimientos del tratamiento, incluidas las medidas para garantizar un tratamiento lícito y equitativo, como las relativas a otras situaciones específicas de tratamiento a tenor del capítulo IX. El Derecho de la Unión o de los Estados miembros cumplirá un objetivo de interés público y será proporcional al fin legítimo perseguido.

Asimismo, el artículo 4, después definir en su apartado 7 el «responsable del tratamiento» o «responsable» como “la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento” añade que “si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros”.

Por otro lado, el artículo 35 regula la evaluación de impacto relativa a la protección de datos (EIPD), señalando que “Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales. Una única evaluación podrá abordar una serie de operaciones de tratamiento similares que entrañen altos riesgos similares”. No obstante, dicho precepto prevé que la EIPD haya sido realizada previamente por el legislador en su apartado 10:

10. Cuando el tratamiento de conformidad con el artículo 6, apartado 1, letras c) o e), tenga su base jurídica en el Derecho de la Unión o en el

Derecho del Estado miembro que se aplique al responsable del tratamiento, tal Derecho regule la operación específica de tratamiento o conjunto de operaciones en cuestión, y ya se haya realizado una evaluación de impacto relativa a la protección de datos como parte de una evaluación de impacto general en el contexto de la adopción de dicha base jurídica, los apartados 1 a 7 no serán de aplicación excepto si los Estados miembros consideran necesario proceder a dicha evaluación previa a las actividades de tratamiento.

Asimismo, debe tenerse en cuenta que, en el caso de que la obligación venga impuesta por una norma de derecho interno, la misma deberá tener rango de ley, por exigirlo el artículo 53.1 de la Constitución, tal y como expresamente recoge el artículo 8.1 de la LOPDGDD, añadiendo que «podrá determinar las condiciones generales del tratamiento y los tipos de datos objeto del mismo, así como las cesiones que procedan como consecuencia del cumplimiento de la obligación legal. Dicha norma podrá igualmente imponer condiciones especiales al tratamiento, tales como la adopción de medidas adicionales de seguridad u otras establecidas en el capítulo IV del Reglamento (UE) 2016/679»

En estos casos, debe tenerse en cuenta la doctrina del Tribunal Constitucional sobre la necesidad de que la propia ley que legitime los tratamientos de datos personales recoja las garantías necesarias y que viene destacando, igualmente, el Tribunal de Justicia de la Unión Europea.

En este sentido, el Tribunal Constitucional, en sus sentencias 292/2000 de 30 noviembre y 76/2019 de 22 de mayo, sienta la doctrina conforme a la cual los límites al derecho fundamental a la protección de datos personales deben establecerse por una norma con rango de ley, previa ponderación por el legislador de los intereses en pugna atendiendo al principio de proporcionalidad, definiendo todos y cada uno de los presupuestos materiales de la medida limitadora mediante reglas precisas, que hagan previsible al interesado la imposición de tal limitación y sus consecuencias, y estableciendo las garantías adecuadas, siendo la propia ley la que habrá de contener las garantías adecuadas frente a la recopilación de datos personales que autoriza. El Tribunal Constitucional (TC) ha sido claro en cuanto a que la previsión de las garantías adecuadas no puede deferirse a un momento posterior a la regulación legal del tratamiento de datos personales de que se trate. Las garantías adecuadas deben estar incorporadas a la propia regulación legal del tratamiento, ya sea directamente o por remisión expresa y perfectamente delimitada a fuentes externas que posean el rango normativo adecuado. Solo ese entendimiento es compatible con la doble exigencia que dimana del artículo 53.1 CE (...). Es evidente que, si la norma incluyera una remisión para la integración de la ley con las garantías adecuadas establecidas en normas de rango inferior a la ley, sería considerada como una deslegalización que

sacrifica la reserva de ley ex artículo 53.1 CE, y, por este solo motivo, debería ser declarada inconstitucional y nula. (...). Se trata, en definitiva, de “garantías adecuadas de tipo técnico, organizativo y procedimental, que prevengan los riesgos de distinta probabilidad y gravedad y mitiguen sus efectos, pues solo así se puede procurar el respeto del contenido esencial del propio derecho fundamental”. Tampoco sirve por ello que para el establecimiento de dichas garantías adecuadas y específicas la ley se remita al propio RGPD o a la LOPDGGD.

Además, dicha ley deberá respetar en todo caso el principio de proporcionalidad, tal y como recuerda la Sentencia del Tribunal Constitucional 14/2003, de 28 de enero:

“En otras palabras, de conformidad con una reiterada doctrina de este Tribunal, la constitucionalidad de cualquier medida restrictiva de derechos fundamentales viene determinada por la estricta observancia del principio de proporcionalidad. A los efectos que aquí importan basta con recordar que, para comprobar si una medida restrictiva de un derecho fundamental supera el juicio de proporcionalidad, es necesario constatar si cumple los tres requisitos o condiciones siguientes: si la medida es susceptible de conseguir el objetivo propuesto (juicio de idoneidad); si, además, es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad); y, finalmente, si la misma es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto; SSTC 66/1995, de 8 de mayo [RTC 1995, 66] , F. 5; 55/1996, de 28 de marzo [RTC 1996, 55] , FF. 7, 8 y 9; 270/1996, de 16 de diciembre [RTC 1996, 270] , F. 4.e; 37/1998, de 17 de febrero [RTC 1998, 37] , F. 8; 186/2000, de 10 de julio [RTC 2000, 186] , F. 6).”

La misma doctrina sostiene el Tribunal de Justicia de la Unión Europea (TJUE). Así, si el art. 8 de la Carta Europea de los Derechos Fundamentales reconoce el derecho de toda persona a la protección de los datos de carácter personal que le conciernan, el art. 52.1 reconoce que ese derecho no es ilimitado y permite la limitación del ejercicio de esos derechos y libertades reconocidos por la Carta, limitación que deberá ser establecida por la ley y respetar el contenido esencial de los mismos.

Pues bien, la STJUE de 6 de octubre de 2020, en los casos acumulados C-511/18, C-512/18 y C-520/18, La Quadrature du Net y otros, (no disponible aún a esta fecha en español), en su apartado 175, recuerda que:

En cuanto a la justificación de dicha injerencia, cabe precisar que el requisito, previsto en el artículo 52, apartado 1, de la Carta, de que

cualquier limitación del ejercicio de los derechos fundamentales deba ser establecida por ley implica que la base legal que la permita debe definir ella misma el alcance de la limitación del ejercicio del derecho de que se trate (véase, en este sentido, la sentencia de 16 de julio de 2020, Facebook Ireland y Schrems, C-311/18, EU:C:2020:559, apartado 175 y jurisprudencia citada).

Igualmente, el apartado 65 de la Sentencia (STJUE) de la misma fecha 6 de octubre de 2020 (C-623/17), Privacy International contra Secretary of State for Foreign and Commonwealth Affairs y otros, con cita, como la anterior, de la sentencia Schrems 2, dice:

Cabe añadir que el requisito de que cualquier limitación del ejercicio de los derechos fundamentales deba ser establecida por ley implica que la base legal que permita la injerencia en dichos derechos debe definir ella misma el alcance de la limitación del ejercicio del derecho de que se trate (sentencia de 16 de julio de 2020, Facebook Ireland y Schrems, C-311/18, EU:C:2020:559, apartado 175 y jurisprudencia citada).

En definitiva, el apartado 175 de la STJUE de 16 de julio de 2020, C-311/2020, Schrems 2, dice:

Cabe añadir, sobre este último aspecto, que el requisito de que cualquier limitación del ejercicio de los derechos fundamentales deba ser establecida por ley implica que la base legal que permita la injerencia en dichos derechos debe definir ella misma el alcance de la limitación del ejercicio del derecho de que se trate [dictamen 1/15 (Acuerdo PNR UE-Canadá), de 26 de julio de 2017, EU:C:2017:592, apartado 139 y jurisprudencia citada].

Es pues, la misma ley que establece la injerencia en el derecho fundamental la que ha de determinar las condiciones y garantías, esto es, el alcance y la limitación, que han de observarse en dichos tratamientos,

Y en dicha STJUE de 16 de julio de 2020, Schrems 2, se añade (y se reitera posteriormente en las citadas sentencias de 6 de octubre de 2020):

176 Finalmente, para cumplir el requisito de proporcionalidad según el cual las excepciones a la protección de los datos personales y las limitaciones de esa protección no deben exceder de lo estrictamente necesario, la normativa controvertida que conlleve la injerencia debe establecer reglas claras y precisas que regulen el alcance y la aplicación de la medida en cuestión e impongan unas exigencias mínimas, de

modo que las personas cuyos datos se hayan transferido dispongan de garantías suficientes que permitan proteger de manera eficaz sus datos de carácter personal contra los riesgos de abuso. En particular, dicha normativa deberá indicar en qué circunstancias y con arreglo a qué requisitos puede adoptarse una medida que contemple el tratamiento de tales datos, garantizando así que la injerencia se limite a lo estrictamente necesario. La necesidad de disponer de tales garantías reviste especial importancia cuando los datos personales se someten a un tratamiento automatizado [véase, en este sentido, el dictamen 1/15 (Acuerdo PNR UE-Canadá), de 26 de julio de 2017, EU:C:2017:592, apartados 140 y 141 y jurisprudencia citada).

La STJUE de 6 de octubre de 2020, en el caso C-623/17, añade la mención de las categorías especiales de datos:

68 (...) Estas consideraciones son aplicables en particular cuando está en juego la protección de esa categoría particular de datos personales que son los datos sensibles [véanse, en este sentido, las sentencias de 8 de abril de 2014, Digital Rights Ireland y otros, C-293/12 y C-594/12, EU:C:2014:238, apartados 54 y 55, y de 21 de diciembre de 2016, Tele2, C-203/15 y C-698/15, EU:C:2016:970, apartado 117; dictamen 1/15 (Acuerdo PNR UE-Canadá), de 26 de julio de 2017, EU:C:2017:592, apartado 141].

Partiendo de las normas y de la doctrina jurisprudencial citada, esta Agencia viene señalando en sus informes más recientes la necesidad de que, por parte del legislador, al introducir regulaciones en nuestro ordenamiento jurídico que tengan especial trascendencia en los tratamientos de datos de carácter personal, se proceda previamente a un análisis de los riesgos que puedan derivarse de los mismos, incluyendo en la Memoria de Análisis de Impacto Normativo un estudio sistematizado del impacto que en el derecho fundamental a la protección de datos personales de los interesados han de tener los distintos tratamientos de datos que prevé la ley. En este sentido se han pronunciado el Informe 77/2020, relativo al Anteproyecto de Ley Orgánica de Lucha contra el Dopaje en el Deporte o el Informe 74/2020 referido al Anteproyecto de Ley de memoria democrática.

Como consecuencia de lo indicado, esta Agencia considera necesario que se realice, con intervención de los delegados de protección de datos del Ministerio de Justicia, el CGPJ y la FGE, un análisis de riesgos y, en su caso, una Evaluación de impacto en la protección de datos, que permita identificar las garantías necesarias que habría que trasladar al presente texto legal.

Sin perjuicio de lo anterior, esta AEPD considera necesario que en la norma se recojan, en un Título independiente dada su trascendencia, las

siguientes cuestiones referidas al cumplimiento de la normativa sobre protección de datos personales:

- 1) Identificación de los responsables y los encargados del tratamiento, determinando los roles que corresponden a los Juzgados y Tribunales, Ministerio de Justicia y Comunidades Autónomas con competencias en la materia.**
- 2) En relación con la legitimación de los tratamientos y, en su caso, el levantamiento de la prohibición para el tratamiento de categorías especiales de datos, la misma se recogerá, con carácter general, en la normativa procesal aplicable, que contendrá las garantías oportunas, por lo que en esta ley deberán preverse las garantías adicionales que deriven de los mayores riesgos que suponga la aplicación de las tecnologías de la información.**
Lo mismo ocurriría respecto de las comunicaciones de datos para finalidades distintas del propio proceso, como sería el caso de elaboración de políticas públicas, cuya legitimación deberá venir dada por las leyes especiales que regulen dichas políticas públicas. Por el contrario, en los tratamientos cuya legitimación sea la presente ley (por ejemplo, en materia de registros electrónicos) la misma deberá identificar y recoger todas las garantías necesarias.
- 3) Cumplimiento del principio de responsabilidad proactiva y de protección de datos desde el diseño y por defecto, estableciendo la obligación de elaborar las EIPD que sean necesarias para el desarrollo de los sistemas y la adopción de decisiones por el Comité Técnico Estatal de la Administración Judicial Electrónica, así como, en su caso, la obligación de formular consulta previa conforme al artículo 36 del RGPD.**
- 4) Obligación de adoptar las medidas técnicas y organizativas, así como las medidas de seguridad, que resulten necesarias en función del riesgo para los derechos y libertades de los afectados, incluyendo, entre ellas, el registro de los accesos, la anonimización, la pseudonimización y el cifrado. Si como consecuencia de la EIPD, las medidas a adoptar resultan agravadas respecto de las previstas en el ENS, prevalecerán las que resulten necesarias para la protección de datos personales. Dichas medidas se revisarán y actualizarán cuando sea necesario.**
- 5) Obligación de realizar, periódicamente, auditorías de protección de datos.**

- 6) Separar adecuadamente las responsabilidades en materia de protección de datos personales de las de seguridad de la información, incluyendo a los dpd de responsables y encargados en el Comité Técnico. Asimismo, dada la trascendencia de las funciones de dicho Comité, debería contar con un dpd propio que coordine a los anteriores en un Subcomité de protección de datos personales. Dicho subcomité debería ser el encargado de preparar, para su aprobación por el Comité, las políticas de protección de datos, incluyendo la identificación de finalidades, datos o categorías de datos que serán tratados según los casos, garantías, etc. así como los planes preventivos o de contingencia en caso de brechas de datos personales.
- 7) Respecto de las decisiones automatizadas, diferenciar no sólo en función de que requieran interpretación jurídica, sino también en función de la posibilidad de producir efectos jurídicos o afectar significativamente a las personas físicas. En este último caso, si pueden producir dichos efectos, deberá garantizarse la intervención humana, pudiendo ser el cauce adecuado el oportuno recurso conforme a la normativa procesal aplicable.
- 8) Debería incluirse una referencia expresa a que el tratamiento ulterior de la información a la que se haya accedido en el ámbito jurisdiccional, no jurisdiccional, de datos abiertos o de reutilización de la información, deberá cumplir la normativa de protección de datos personales.
- 9) Podría incluirse una referencia que vinculara las transferencias internacionales de datos a las bases jurídicas y garantías del RGPD.

Por otro lado, como garantías específicas a recoger en el articulado, y sin perjuicio de las que resulten del análisis de riesgos y de la EIPD, se pueden citar las siguientes:

- 1) En relación con los tratamientos para finalidades distintas a las del propio proceso, como la elaboración de políticas públicas, incluir con carácter general la necesaria anonimización de los datos, garantizando, en todo caso, el nivel de agregación suficiente que impida la identificación de personas físicas.
- 2) Asimismo, en relación con la transparencia y “datos abiertos”, deberán haberse anonimizado previamente.
- 3) En la sede judicial electrónica, además de incluir entre los principios la protección de datos, deberá constar toda la

información prevista en los artículos 13 y 14 del RGPD y cualquier otra que permita cumplir con el principio de transparencia, así como el inventario de tratamientos conforme al artículo 31.2 de la LOPDGDD. Asimismo, debería introducirse la información correspondiente en los distintos sistemas de registro de la información contemplados en el anteproyecto.

- 4) Debe delimitarse en la ley quiénes pueden tener acceso al expediente judicial electrónico, sin que pueda dejarse una decisión de tal relevancia al Comité Técnico.**
- 5) Debe revisarse y analizarse adecuadamente los riesgos derivados de los intercambios masivos de información.**
- 6) En el Tablón Edictal Judicial Único, prever las medidas que impidan su indexación por los motores de búsqueda, así como la limitación de acceso a la información edictal trascurrido el plazo prudencial para que la misma haya cumplido su finalidad.**
- 7) En materia de teletrabajo, incluir garantías de privacidad del trabajador.**

Por último, en relación con los sistemas de identificación digital y firma digital, deberán establecerse por ley, no siendo suficiente la habilitación reglamentaria.

IV

Para concluir, debe hacerse referencia a las modificaciones que la disposición final decimocuarta introduce en ciertos preceptos de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, con motivo de la corrección de errores del Reglamento Europeo sobre Protección de Datos publicada en el DOUE del día 4 de marzo de 2021, y en consecuencia la eliminación del apercibimiento del catálogo de sanciones a imponer a responsables y encargados, sustituyéndolo por la realización de un requerimiento. Además, la reforma introduce un nuevo artículo que habilita y regula la realización de actuaciones de investigación a través de sistemas digitales, y se aumenta de nueve a doce meses la duración máxima del procedimiento sancionador, y de doce a dieciocho meses la de las actuaciones previas de investigación. Por último, se introduce una previsión en cuanto a la notificación de la admisión a trámite en aquellos procedimientos con un elevado número de reclamaciones, y el establecimiento de modelos obligatorios de reclamación ante la Agencia Española de Protección de Datos.

Tal y como se reconocía en el Preámbulo de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de

protección de datos) ha supuesto una evolución desde el antiguo modelo de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, que estaba basado en una serie de obligaciones a las que los responsables y encargados del tratamiento habían de sujetarse, unidas al reconocimiento de potestades reactivas de las autoridades de protección de datos, hacia un nuevo modelo de responsabilidad proactiva, que exigirá a su vez una valoración dinámica de la actividad desarrollada por el sujeto obligado por la norma y la adopción de medidas tales como la privacidad desde el diseño y por defecto, la realización de evaluaciones de impacto en la protección de datos o la implantación de medidas de seguridad técnicas y organizativas ajustadas en cada momento al estado de la técnica y a los riesgos derivados del tratamiento.

El nuevo modelo de protección de datos de carácter personal ha tenido una incidencia notable en la organización y funciones tradicionales de la Agencia Española de Protección de Datos, así como en la tramitación de sus procedimientos, puesto que el Reglamento general de protección de datos refuerza las competencias de las autoridades de control que deberán contar con todas las funciones y poderes efectivos, incluidos los poderes de investigación, poderes correctivos y sancionadores, y poderes de autorización y consultivos previstos en el propio Reglamento y ha introducido los mecanismos que garanticen la necesaria coordinación y coherencia entre las diferentes autoridades de control europeas.

En este sentido, el Título VIII de la Ley Orgánica 3/2018, de 5 de diciembre, regula los «Procedimientos en caso de posible vulneración de la normativa de protección de datos», teniendo en cuenta que el Reglamento (UE) 2016/679 establece un sistema novedoso y complejo, evolucionando hacia un modelo de «ventanilla única» en el que existe una autoridad de control principal y otras autoridades interesadas. Asimismo, el Título IX, que contempla el régimen sancionador, parte de que el Reglamento (UE) 2016/679 establece un sistema de sanciones o actuaciones correctivas que permite un amplio margen de apreciación.

Después de más de dos años de la plena aplicación del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 y la entrada en vigor de la Ley Orgánica 3/2018, de 5 de diciembre, la experiencia adquirida demuestra la necesidad de introducir modificaciones en la tramitación de los procedimientos que tramita la Agencia Española de Protección de Datos en los supuestos de posible vulneración de la normativa de protección de datos, por las razones que se exponen a continuación.

En relación con el apercibimiento, el pasado 4 de marzo del año en curso se publicó en el Diario Oficial de la Unión Europea una corrección de errores del RGPD en la que, entre otras, se incluye la siguiente:

*“16) En la página 69, en el artículo 58, apartado 2, letras a) y b):
donde dice:*

«a) sancionar a todo responsable o encargado del tratamiento con una advertencia cuando las operaciones de tratamiento previstas puedan infringir lo dispuesto en el presente Reglamento;

b) sancionar a todo responsable o encargado del tratamiento con apercibimiento cuando las operaciones de tratamiento hayan infringido lo dispuesto en el presente Reglamento;»,

debe decir:

«a) dirigir a todo responsable o encargado del tratamiento una advertencia cuando las operaciones de tratamiento previstas puedan infringir lo dispuesto en el presente Reglamento;

b) dirigir a todo responsable o encargado del tratamiento un apercibimiento cuando las operaciones de tratamiento hayan infringido lo dispuesto en el presente Reglamento;»."

Aun cuando a simple vista la corrección de errores efectuada pueda parecer intrascendente, lo cierto es que tiene implicaciones jurídicas esenciales en la comprensión y configuración de los poderes correctivos establecidos en el RGPD en relación con el sistema de sanciones fijado en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD).

A la vista de la nueva redacción del artículo 58.2.b) del RGPD, se desprende que el apercibimiento no debe ser considerado una sanción y que el empleo del verbo "sancionar" en la versión en castellano del RGPD constituía un error que ahora ha sido corregido. En efecto, en la versión en inglés, el precepto afirma: *"to issue reprimands to a controller or a processor where processing operations have infringed provisions of this Regulation"*, expresión que ahora se traduce como "dirigir".

La conceptualización jurídica y la terminología del RGPD no encaja ahora con el sistema de sanciones de nuestra LOPDGDD, provocando la necesidad de un cambio sustancial en lo que constituye *"dirigir un apercibimiento"*. En este sentido, partiendo de la traducción inicial del RGPD, la LOPDGDD consideró al apercibimiento como una sanción y no como una medida de carácter no sancionador, apartándose de la configuración tradicional del mismo en nuestro ordenamiento jurídico tras su inclusión en el apartado 6 al artículo 45 de la derogada Ley Orgánica 15/1999 de 13 de diciembre, de Protección de Datos de Carácter Personal por la Ley 2/2011, de 4 de marzo, de Economía Sostenible, tal y como reconoce la Sentencia del Tribunal Supremo de 29 de noviembre de 2013, (reiterada en otras como la Sentencia núm. 447/2016 de 23 septiembre):

«En consecuencia, el "apercibimiento" a que se refiere el precepto no constituye una sanción y tiene por objeto, exclusivamente, que el sujeto responsable "en el plazo que el órgano sancionador determine, acredite la adopción de las medidas correctoras que en cada

caso resultasen pertinentes", siendo tales medidas las que establezca en cada supuesto la Agencia Española de Protección de Datos. De manera que el artículo 45.6 de la LOPD no contempla la imposición de la sanción de apercibimiento, consistente en la amonestación que se hace al sujeto responsable de una infracción administrativa, haciéndole saber el reproche social que merece su conducta infractora.

Tal consideración se ve avalada también por el hecho de que el "apercibimiento", al que se refiere la norma, no se ve precedido de la tramitación de procedimiento sancionador, en cuyo seno se acuerde, y se contrapone abiertamente a la imposición de sanciones, tal y como indica expresamente el precepto, tanto al prever su aplicación en lugar de la apertura del procedimiento sancionador, como al exigir su procedencia, entre otros requisitos, que "el infractor no hubiere sido sancionado o apercibido con anterioridad".

En este sentido, resulta revelador el hecho de que el incumplimiento del apercibimiento o su desatención conlleve la apertura del correspondiente procedimiento sancionador por dicho incumplimiento.

En definitiva, nos encontramos ante una habilitación legal y expresa a la Agencia Española de Protección de Datos para sustituir la sanción que correspondería a la conducta infractora apreciada por un mero requerimiento para la adopción de determinadas medidas correctoras, al que se denomina "apercibimiento", que carece de naturaleza sancionadora.

Consecuentemente, el artículo 45.6 de la LOPD confiere a la Agencia Española de Protección de Datos una potestad que difiere sustancialmente de la sancionadora y que puede ejercer en lugar de esta cuando concurren las singulares y excepcionales circunstancias que contempla el precepto.

A ello debe añadirse que el fundamento de la atribución de tal potestad administrativa no puede ser otra más que la constatación de que bajo ciertas circunstancias que contempla el precepto, la cualificada disminución de la culpabilidad del imputado o de la antijuridicidad de hecho resulta tan extraordinaria que la conducta no merece la imposición de sanción ni, por ende, es objeto del reproche social que acompaña a esta medida [...]».

La corrección efectuada sobre el artículo 58.2.b) del RGPD, incluido dentro de los poderes correctivos de las autoridades de control (tasados en el texto normativo citado), no deja lugar a dudas sobre la voluntad reglamentaria de no configurar el apercibimiento como una sanción, por lo que, siendo dicha previsión aplicable directamente, debemos adaptar nuestro ordenamiento jurídico a la traducción correcta del RGPD, acomodando nuestra LOPDGDD a esta "medida adecuada", dirigiendo un apercibimiento siempre que concurren determinadas circunstancias.

En este sentido, el considerando 148 del RGPD señala:

«A fin de reforzar la aplicación de las normas del presente Reglamento, cualquier infracción de este debe ser castigada con sanciones, incluidas multas administrativas, con carácter adicional a medidas adecuadas impuestas por la autoridad de control en virtud del presente Reglamento, o en sustitución de estas. En caso de infracción leve, o si la multa que probablemente se impusiera constituyese una carga desproporcionada para una persona física, en lugar de sanción mediante multa puede imponerse un apercibimiento [...]»

Según el citado considerando, las infracciones deben ser castigadas con sanciones, de manera adicional o en sustitución de “medidas adecuadas”. Con la nueva redacción del artículo 58.2.b), el apercibimiento no puede ya ser considerado como una sanción, sino, al contrario, como una “medida adecuada”, un “poder correctivo” con el que cuenta la autoridad de control que carece de naturaleza sancionadora y al que puede acudir en lugar de la sanción. En concreto, en relación con los apercibimientos, el RGPD indica que procederán en caso de infracción leve, o si la multa que pudiera imponerse constituyese una carga desproporcionada para una persona física.

En lo que a las infracciones leves respecta, cabe señalar que no ha de entenderse por tales las así tipificadas, a efectos de prescripción, en la LOPDGDD, sino que la autoridad de control, en atención a las circunstancias concurrentes en cada caso, y según los factores agravantes y atenuantes contemplados en el artículo 83.2 del RGPD, podrá determinar la “levedad” de la infracción a efectos de su castigo con apercibimiento.

Desde un punto de vista práctico, esta nueva conceptualización del apercibimiento como una manifestación de poder correctivo no sancionador supondría un alivio de la carga de trabajo de la Subdirección General de Inspección de Datos Subdirección General de Inspección de Datos (SGID) al no acudirse en estos casos a la tramitación de un procedimiento sancionador.

En este contexto, debemos mencionar el exponencial crecimiento del trabajo de la SGID tanto en cantidad como en complejidad de los asuntos que tiene encomendados por mor de las competencias conferidas al respecto.

En cuanto a la cantidad, esta deviene en gran parte del incremento del número de reclamaciones interpuestas por interesados quienes cada vez son más conscientes de sus derechos, de los riesgos a los que están sometidos por el tratamiento de sus datos personales y de su vulneración, reclamando ante la Agencia Española de Protección de Datos.

Sobre este particular la reciente Resolución del Parlamento Europeo, de 25 de marzo de 2021, sobre el informe de evaluación de la Comisión sobre la ejecución del Reglamento General de Protección de Datos dos años después

de su aplicación (2020/2717(RSP)), pone de manifiesto que *“desde el inicio de la aplicación del RGPD, ha aumentado enormemente el número de reclamaciones recibidas por las autoridades de control; que ello demuestra que los interesados son más conscientes de sus derechos y desean proteger sus datos personales de conformidad con el RGPD”*.

A esta ecuación debemos añadir que en estos últimos años se ha producido la generalización del uso de nuevas tecnologías -algunas altamente intrusivas-, incluyendo el acceso masivo a internet y la utilización de redes sociales, lo que sumado al uso e intercambio masivo de datos también entre particulares o la computación ubicua (y móvil) ha disparado en número de reclamaciones.

Los riesgos son muy diversos, distintos y nuevos respecto de los que estábamos acostumbrados (como la usurpación de identidad, la elaboración de perfiles discriminatorios, la vigilancia permanente -englobando la geolocalización- o el fraude).

Al fin y al cabo, esta nueva realidad ahora presente fue uno de los motores que impulsaron el nuevo RGPD frente a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, que devino insuficiente para enfrentar el gran cambio tecnológico y social en el tratamiento de datos personales.

La Comisión Europea propuso la adopción del RGPD precisamente para enfrentar los desafíos planteados por las nuevas tecnologías y servicios.

Así se recoge finalmente en el considerando 6 del RGPD que dispone con meridiana claridad que *“La rápida evolución tecnológica y la globalización han planteado nuevos retos para la protección de los datos personales. La magnitud de la recogida y del intercambio de datos personales ha aumentado de manera significativa. La tecnología permite que tanto las empresas privadas como las autoridades públicas utilicen datos personales en una escala sin precedentes a la hora de realizar sus actividades. Las personas físicas difunden un volumen cada vez mayor de información personal a escala mundial. La tecnología ha transformado tanto la economía como la vida social, y ha de facilitar aún más la libre circulación de datos personales dentro de la Unión y la transferencia a terceros países y organizaciones internacionales, garantizando al mismo tiempo un elevado nivel de protección de los datos personales”*.

Pero es que, además, la implicación de la Agencia Española de Protección de Datos en la defensa del Derecho Fundamental a la Protección de Datos de Carácter personal en este nuevo contexto de constante desarrollo de

las tecnologías y de cambio en las costumbres sociales ha sido amplísima, como muestra el nacimiento del Canal Prioritario en septiembre de 2019.

Debemos también sumar el notable incremento de derechos conferidos por el RGPD a los interesados y el correlativo aumento de funciones impuestas por el RGPD a la Inspección dentro de la Agencia Española de Protección de Datos, en relación con las contenidas anteriormente en la LOPD.

Así, por ejemplo, y en relación con las actuaciones de investigación por iniciativa propia, hemos de citar las investigaciones derivadas de las notificaciones de las violaciones de seguridad de datos personales cuya comunicación es obligatoria para los responsables del tratamiento por mor del artículo 33 del RGPD.

Otro ejemplo lo encontramos en la instauración del mecanismo de ventanilla única (artículo 60 y siguientes del RGPD) que erige un sistema de cooperación y coherencia entre las distintas autoridades de control, que exige la participación y consulta de la Agencia Española de Protección de Datos. Un sistema complejo, en el que, en ocasiones, hay que tratar de llegar a un acuerdo sobre un asunto determinado - en el que se ven implicadas varias autoridades de control- a partir de las diferentes objeciones formuladas por una, varias o todas las autoridades de control a las que hay que contestar de manera motivada y pormenorizada; también se han de considerar los casos en los que hay que asistir a otras autoridades de control, lo que abarca las solicitudes de información y las medidas de control, las solicitudes para llevar a cabo autorizaciones y consultas previas, inspecciones e investigaciones.

A mayores, el incremento en el número de asuntos va acompañado de una mayor complejidad de estos, tanto desde el punto de vista material como procedimental, lo que requiere un mayor esfuerzo en su estudio, lo que precisa a su vez de un análisis mucho más pormenorizado.

Desde un punto de vista material, por un lado, ligado a la implantación del RGPD y de la LOPDGDD, que, no obstante, han transcurrido tres años desde su aplicabilidad, siguen exigiendo un extremo cuidado en el discernimiento y la comprensión de los supuestos de hechos enfrentados y en la aplicación e interpretación correcta de la normativa. Máxime cuando hay que tener en consideración las guías y directrices del CEPD y la jurisprudencia, tanto de tribunales estatales, de la Unión Europea, como de corte internacional (TEDH).

Por otro lado, como ya hemos indicado, nos enfrentamos a una realidad cada vez más enrevesada e intrincada de la que surgen supuestos de hecho más difíciles de analizar, unida a la implantación de tecnologías innovadoras y emergentes (en ocasiones por primera vez o de forma generalizada) o al continuo establecimiento de nuevos tipos de tratamientos con tecnologías ya

existentes. Junto con el necesario conocimiento jurídico se requiere ahora un extenso conocimiento tecnológico. Pensemos simplemente en la complejidad impuesta en los tratamientos que emplean la toma de decisiones algorítmica y la inteligencia artificial, el Big Data o el internet de las cosas.

A todo ello tenemos que añadir la casuística propia e intrínseca de la protección de datos de carácter personal, que impone la indagación, la investigación, el análisis y la individualización del supuesto concreto, sin que tales actuaciones puedan ser sustituidas por declaraciones o resoluciones generales.

Desde un punto de vista procedimental debemos hacer de nuevo una referencia a las dificultades prácticas y de tramitación producidas por la integración en nuestros propios procedimientos administrativos de los procedimientos específicos previstos para solventar las reclamaciones transfronterizas a través del mecanismo de ventanilla única.

Sin embargo, el notabilísimo incremento de funciones y de trabajo no ha supuesto un correlativo incremento de los medios disponibles materiales y personales, situación ampliamente reconocida en la Resolución del Parlamento Europeo, de 25 de marzo de 2021, sobre el informe de evaluación de la Comisión sobre la ejecución del Reglamento General de Protección de Datos dos años después de su aplicación (2020/2717(RSP)), cuando afirma de manera taxativa que *“muchas autoridades de protección de datos no son capaces de hacer frente al número de reclamaciones; que muchas de dichas autoridades carecen de personal y de recursos suficientes, así como de un número suficiente de expertos en tecnología de la información”*.

Manifiesta el Parlamento Europeo su gran preocupación por la falta de recursos de todo tipo señalando *“la importancia de que las autoridades de control de la Unión, así como el CEPD, dispongan de suficientes recursos financieros, técnicos y humanos para poder hacer frente rápida pero exhaustivamente a un número cada vez mayor de casos complejos y que requieren una gran cantidad de recursos, y para coordinar y facilitar la cooperación entre las autoridades nacionales de protección de datos, hacer seguimiento adecuadamente de la aplicación del RGPD y proteger los derechos y libertades fundamentales”*.

La certeza de lo que afirmamos se muestra con los números que facilita la Subdirección General de Inspección:

El incremento de entradas respecto del mismo periodo del año pasado, a fecha 30 de noviembre de 2021, es de un 35% considerando las reclamaciones, las notificaciones de brechas de seguridad de datos personales y los procedimientos transfronterizos. A este crecimiento en el número de casos hay que sumar el aumento en su complejidad, en algunos casos se trata de expedientes que dan lugar a varios

procedimientos administrativos con diferentes intervinientes y en otros se trata de asuntos novedosos sobre la interpretación del reglamento en la que las diferentes autoridades de control intentamos llegar a soluciones de consenso.

Durante el mes de noviembre de 2021, podemos comprobar cómo se han presentado 558 reclamaciones, obteniendo en número nada despreciable de 13.341 reclamaciones presentadas en total en lo que va de año (hasta el 30 de noviembre de 2021).

Comparando esta cifra con los datos de 2010, año en el que se dictaron 6.189 resoluciones, de seguir esta tendencia durante el último mes del año se produciría un incremento del 135%.

Sin embargo, en mayo de 2010 se encontraban ocupados 65 puestos de la Subdirección General de Inspección de Datos, mientras que en la actualidad dicha cifra sólo se ha incrementado en 7 personas, lo que supone un incremento de un 10,7%, a todo punto insuficiente. Además, no todas estas personas se dedican a tareas de inspección e instrucción, sino que hay un total de 14 personas que realizan labores administrativas y técnicas. También hay que considerar que hasta 2018 se contaba con 7 personas de una empresa externa que ya no están.

Así, en la Memoria de 2018 de la Agencia Española de Protección de Datos se hace una referencia a los recursos humanos disponibles para responder al cambio de contexto que supuso la aplicabilidad del RGPD desde mayo de 2018, indicando que “En diciembre de 2017 trabajaban en la Subdirección General de Inspección un total de 64 funcionarios repartidos en las diferentes áreas. En diciembre de 2018, ese número llegaba solo a 67 personas considerando las altas y bajas producidas en el ejercicio”.

Se constata, en cuanto al número de efectivos disponibles en la Subdirección General de Inspección de Datos, que no se ha producido un crecimiento de manera proporcional a las nuevas funciones y al incremento que estas han originado en el trabajo diario, sino más bien al contrario (un incremento del 135% frente a un 7%).

De este modo, la introducción de un procedimiento específico de apercibimiento, más flexible y rápido, con una duración máxima de seis meses, va a permitir agilizar la respuesta a las reclamaciones presentadas por los ciudadanos, al tiempo que reduce la carga de trabajo de la Agencia Española de Protección de Datos, al no acudir en estos casos a la tramitación de un procedimiento sancionador.

Además, este nuevo procedimiento, de tan sólo seis meses, supone un contrapeso en relación con la modificación también propuesta relativa al aumento del plazo de tramitación de los procedimientos sancionadores (que expondremos a continuación) en los que sí es preciso un mayor margen

temporal para su tramitación. Y, por ende, una respuesta más célere a las reclamaciones presentadas por los ciudadanos.

En conclusión, el establecimiento de este procedimiento supondrá la dinamización de las funciones encomendadas a la Subdirección General de Inspección de Datos Subdirección General de Inspección de Datos con un procedimiento más flexible y rápido que solvente eficazmente las reclamaciones presentadas por los interesados y ayude a soportar a la Subdirección General de Inspección de Datos la carga de trabajo adicional impuesta por el RGPD.

Por otro lado, la necesidad de garantizar la eficacia y la eficiencia en la actuación de la Agencia Española de Protección de Datos y el adecuado cumplimiento de las funciones que el Reglamento (UE) 2016/679 le encomienda, así como la introducción de este nuevo procedimiento de apercibimiento muestra la necesidad de realizar otras modificaciones para articular la forma de realizar inspecciones no presenciales, establecer una única forma de inicio de los procedimientos sancionadores (ya sean o no transfronterizos) y un incremento del plazo de tramitación del procedimiento sancionador y de las actuaciones previas de investigación.

En primer lugar, se introduce un nuevo artículo 53 bis, relativo a la forma de realizar las actuaciones de investigación a través de sistemas digitales, para regular la posibilidad de realizar no sólo investigaciones presenciales, sino también remotas. La necesidad de implantar esta posibilidad a la hora de realizar una investigación, no prevista expresamente en la redacción inicial de la Ley, surge como consecuencia de diversos acontecimientos, como la dificultad de realizar investigaciones presenciales durante la pandemia del COVID-19 o la instauración del teletrabajo como una modalidad de prestación de servicios a distancia. Con la introducción de las inspecciones remotas se estaría dando solución a este impedimento, no sólo durante el tiempo indeterminado que dure la pandemia, sino con posterioridad a la misma, cubriendo cualquier contingencia exógena por la que las investigaciones no pudieran realizarse de forma presencial. Redundaría por tanto en la eficacia y efectividad del trabajo de la Agencia Española de Protección de Datos, cuya operatividad no se vería ralentizada por eventualidades y circunstancias ajenas a la misma, al tiempo que potenciaría y redundaría en el efectivo establecimiento de la Administración electrónica, y permite a la Agencia sumarse al camino fijado por otras Administraciones Públicas de permitir inspecciones remotas, como ocurre, por ejemplo, en el artículo 99.9 de la Ley 58/2003, de 17 de diciembre, General Tributaria introducido recientemente mediante la disposición final 1.1 del Real Decreto-ley 22/2020, de 16 de junio, por el que se regula la creación del Fondo COVID-19 y se establecen las reglas relativas a su distribución y libramiento o en el artículo 39 bis.4. de la Ley 15/2007, de 3 de julio, de Defensa de la Competencia, introducido por el artículo primero del Real Decreto-ley 7/2021, de 27 de abril, de transposición de directivas de la Unión Europea en las materias de competencia, prevención

del blanqueo de capitales, entidades de crédito, telecomunicaciones, medidas tributarias, prevención y reparación de daños medioambientales, desplazamiento de trabajadores en la prestación de servicios transnacionales y defensa de los consumidores.

De este modo, teniendo en cuenta las cuestiones ya citadas relativas al incremento de funciones y trabajo de la Subdirección General de Inspección de Datos, las inspecciones remotas auxiliarían de forma notable a facilitar el trabajo y a mejorar la eficiencia, la eficacia y la economía, aumentando el tiempo disponible para llevar a cabo otras tareas encomendadas. Su establecimiento, junto con las inspecciones presenciales, tendría una repercusión directa en el trabajo desempeñado por la Subdirección General de Inspección de Datos dinamizándolo de manera significativa. Asimismo, la implantación de las inspecciones remotas potenciaría y redundaría en el efectivo establecimiento de la Administración electrónica, auspiciando la accesibilidad, y favorecería, igualmente, el ejercicio de los derechos de los ciudadanos y el cumplimiento de sus obligaciones, con, además, un ahorro significativo de costes (desplazamientos y tiempo, entre otros) para el ciudadano y para la Agencia Española de Protección de Datos.

En este contexto hemos de considerar igualmente la instauración del teletrabajo como una modalidad de prestación de servicios a distancia en el que “el contenido competencial del puesto de trabajo puede desarrollarse, siempre que las necesidades del servicio lo permitan, fuera de las dependencias de la Administración, mediante el uso de tecnologías de la información y comunicación”, tal y como previene el artículo 47.bis del Real Decreto Legislativo 5/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto Básico del Empleado Público (TREBEP).

En este sentido, debemos destacar la implantación del teletrabajo en la Agencia Española de Protección de Datos que ha redundado en una mayor eficiencia de las funciones encomendadas por el ordenamiento jurídico, habiendo sido especialmente relevante su utilidad durante la pandemia de la COVID-19. Desde el programa piloto instaurado en 2017, pasando por su plasmación en el Marco de Actuación de Responsabilidad Social, hasta la actualidad, el teletrabajo en la Agencia Española de Protección de Datos se ha revelado como una organización del trabajo más flexible que sirve a la prestación más eficiente de los servicios públicos.

La implantación de esta modalidad de prestación de servicios ha de permitir que las competencias del puesto de trabajo puedan también ser desarrolladas telemáticamente, incluyendo las relativas a la inspección propias de la Agencia Española de Protección de Datos. Esto sería imposible si no se previese la posibilidad efectiva de realizar inspecciones remotas, con idénticas garantías que las presenciales.

Esta modificación se formula sin hurtar a los administrados de las garantías precisas que aseguren dentro del procedimiento “la transmisión y recepción seguras de los documentos e información que se intercambien, y, en su caso, recoger las evidencias necesarias y el resultado de las actuaciones realizadas asegurando su autoría, autenticidad e integridad”.

Asimismo, tal posibilidad no se impone, pues precisa de la conformidad del responsable o del encargado del tratamiento para su uso, así como para fijar la fecha y hora de su desarrollo. Y es que se ha considerado que no todos los administrados están obligados a relacionarse electrónicamente con las Administraciones Públicas o no disponen de los medios técnicos precisos para llevarlo a cabo. En conclusión, se han respetado los principios generales del sector público en cuanto a sus actuaciones y relaciones electrónicas.

En segundo lugar, se ha suprimido el tercer párrafo del apartado segundo del artículo 64 de la LOPDGDD en el que se recogía como forma de iniciación del procedimiento sancionador la adopción del proyecto de acuerdo de inicio del procedimiento sancionador, del que se debería dar conocimiento formal al interesado a los efectos de interrumpir la infracción (artículo 75 de la LOPDGDD).

Se pretende de esta forma que el procedimiento sancionador siempre se inicie mediante acuerdo de inicio de manera independiente a si nos encontramos en un procedimiento de ventanilla única o no. Y ello porque tal proyecto de acuerdo de inicio se somete a las objeciones de las distintas autoridades de control, pudiendo resultar que, tras un acuerdo con las mismas, el acuerdo de inicio diste bastante de lo establecido en el proyecto de acuerdo de inicio.

De esta forma no sólo se fija con precisión y de forma unívoca el inicio de un procedimiento sancionador sea o no transfronterizo. También se logra mayor seguridad jurídica para el ciudadano.

En tercer lugar, en el párrafo quinto del artículo 64.2 de la ley orgánica, se ha aumentado de nueve a doce meses la duración del procedimiento sancionador, con el fin de ajustarlo al incremento del número y de la complejidad de las reclamaciones y de los trámites que deben realizarse, con el objeto de garantizar la eficacia administrativa y la adecuada protección del derecho fundamental a la protección de datos de carácter personal.

Se precisa el incremento del plazo en atención a las razones esgrimidas anteriormente relativas al acrecentamiento de trabajo en la Subdirección General de Inspección de Datos, tanto en cantidad como en complejidad, derivado en especial de las nuevas funciones asignadas a las autoridades de control, a las nuevas obligaciones impuestas a los responsables y encargados del tratamiento que hay que supervisar y a los nuevos procedimientos derivados de la implantación de la ventanilla única en el RGPD, entre otras

cuestiones. Y es que, a los procedimientos sancionadores tramitados por la Agencia Española de Protección de Datos debemos añadir la singularidad, peculiaridades y trámites adicionales de los citados procedimientos internacionales.

Lo que en apariencia podría pensarse que supone una merma de las garantías de los ciudadanos no es así. Tanto en la Constitución Española (artículo 103) como en la LRJSP (artículo 3) se prima el principio de eficacia como uno de los principios generales que lideran la actuación administrativa; se liga en un segundo plano a otros principios, tales como el servicio efectivo a los ciudadanos, la agilidad de los procedimientos o la eficacia en el cumplimiento de los objetivos fijados. Mas, de ninguna manera va a resultar eficaz la actuación administrativa si con los medios de que dispone no se logra la consecución de los intereses perseguidos, en el caso de la Agencia Española de Protección de Datos, la defensa real del Derecho Fundamental a la Protección de Datos de Carácter Personal. La complejidad del trabajo desarrollado precisa de tiempo suficiente para investigar y dilucidar correctamente las reclamaciones presentadas y dar debida respuesta a los ciudadanos.

Tenemos que significar que, en todo caso, se trata un plazo máximo de duración del procedimiento, sin que este tenga que ser agotado.

A mayor abundamiento, el incremento del plazo de tramitación del procedimiento sancionador se compensa con el establecimiento de un procedimiento de apercibimiento que tiene una duración máxima de seis meses.

En cuarto lugar, se ha incluido en el artículo 65.5 de la ley orgánica una previsión específica para la notificación de la admisión a trámite en aquellos supuestos en que se presenten una elevado número de reclamaciones por distintos reclamantes derivadas de un mismo acontecimiento y que guarden entre ellas una identidad sustancial y los hechos denunciados se refieren al mismo presunto sujeto infractor que ha violado los mismos preceptos del Reglamento (UE) 2016/679 y de la Ley Orgánica 3/2018, de 5 de diciembre.

Un ejemplo muy significativo es el que deviene de las violaciones de seguridad de datos personales. Otro aquel en el que la Agencia Española de Protección de Datos ha tenido conocimiento por varias vías de unos hechos que infringen la normativa de protección de datos.

En tales supuestos, cuando la Agencia Española de Protección de Datos ya se encuentre investigando los hechos concernidos en el acontecimiento producido o hubiera acordado el inicio de un procedimiento sancionador, se indicará, en la notificación al reclamante de la admisión a trámite de su reclamación, el número de expediente en el seno del cual estos hechos se

están investigando y la dirección web en la que se publicará la resolución que ponga fin al mismo.

La fundamentación de la inclusión de estos aspectos en la notificación de la admisión a trámite de la reclamación la encontramos en la previsión del artículo 57.1. f) del RGPD, en el que se indica, de entre las funciones atribuidas a las Autoridades de Control que les corresponde “tratar las reclamaciones presentadas por un interesado o por un organismo, organización o asociación de conformidad con el artículo 80, e investigar, en la medida oportuna, el motivo de la reclamación e informar al reclamante sobre el curso y el resultado de la investigación en un plazo razonable, en particular si fueran necesarias nuevas investigaciones o una coordinación más estrecha con otra autoridad de control”. Asimismo, el artículo 77.2 del RGPD establece que “La autoridad de control ante la que se haya presentado la reclamación informará al reclamante sobre el curso y el resultado de la reclamación, inclusive sobre la posibilidad de acceder a la tutela judicial en virtud del artículo 78”.

Con esta previsión, se da cumplimiento, en el mismo acto de notificación de la admisión a trámite de la reclamación, al deber de informar al reclamante del curso y resultado de la investigación. Por tanto, se concentran en un solo acto trámites que actualmente se realizan por separado. Esto supone una ganancia de eficacia, en atención a los recursos limitados, especialmente los personales, de los que dispone la Agencia Española de Protección de Datos.

En quinto lugar, se ha modificado, en el artículo 67 de la LOPDGDD, el plazo de las actuaciones previas de investigación de doce a dieciocho meses, por idénticas razones que las ya recogidas con anterioridad y porque, además, con las modificaciones introducidas en la LOPDGDD y la iniciación del procedimiento sancionador o de apercibimiento con acuerdo de inicio, en todo caso, parte de las actuaciones realizadas en el marco de la ventanilla única se van a integrar en las actuaciones previas de investigación.

En sexto lugar, el segundo párrafo del artículo 75 de la LOPDGDD ha sido suprimido en consonancia con la eliminación del tercer párrafo del artículo 64.2 de la LOPDGDD.

En séptimo lugar, se modifica el apartado 2 del artículo 77, relativo a las medidas a adoptar cuando cometan una infracción las categorías de responsables o encargados a los que el mismo se refiere, para suprimir la referencia a la sanción de apercibimiento, al no tratarse de una sanción, tal y como se ha señalado anteriormente, añadiendo la obligación de declarar expresamente la infracción cometida y manteniendo la necesidad de establecer las medidas correctivas que proceda adoptar, de las que queda excluida la imposición de multa administrativa prevista en el artículo 58.2.i. del RGPD, tal y como ocurre en la actualidad. Se trata, por consiguiente, de una modificación puramente formal, derivada de la no consideración del apercibimiento como

sanción, pero que no modifica sustancialmente el régimen aplicable a los sujetos incluidos en el ámbito de aplicación del artículo 77.

Por último, se introduce una nueva disposición adicional a los efectos del establecimiento de modelos obligatorios de presentación de reclamaciones ante la Agencia Española de Protección de Datos. Así, el artículo 66.6 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (a partir de ahora, LPAC), permite que “Cuando la Administración en un procedimiento concreto establezca expresamente modelos específicos de presentación de solicitudes, éstos serán de uso obligatorio por los interesados”.

Si bien no podemos entender *strictu sensu* que las reclamaciones que pueden presentar los afectados ante la Agencia Española de Protección de Datos sean solicitudes administrativas, en los términos del artículo 66 de la LPAC, es cierto que tal precepto puede ser aplicado supletoriamente a los procedimientos tramitados por la Agencia Española de Protección de Datos (art. 110 de la LRJSP), en todo lo que no esté previsto en los mismos (artículos 63 y siguientes de la LOPDGD).

Es preciso establecer modelos específicos de presentación de reclamaciones ante la Agencia Española de Protección de Datos que sean de uso obligatorio, puesto que, dada la especialidad y complejidad de la materia, facilitará y simplificará sin lugar a duda la presentación de reclamaciones por parte del afectado. Los modelos que se establezcan servirán de guía a los interesados a la hora de presentar una reclamación.

En este sentido, el mandato del legislador impone a las autoridades de control el facilitar la presentación de las reclamaciones contempladas en el artículo 57.1.f) del RGPD. Específicamente, el artículo 57.2 del mismo texto legal determina que *“cada autoridad de control facilitará la presentación de las reclamaciones contempladas en el apartado 1, letra f), mediante medidas como un formulario de presentación de reclamaciones que pueda cumplimentarse también por medios electrónicos, sin excluir otros medios de comunicación”*. Y ello partiendo de la previsión contenida en el considerando 141 del RGPD.

El legislador señala particularmente como una buena práctica acometer y establecer formularios para presentar las reclamaciones, habilitando una vía sencilla para dinamizar la presentación de reclamaciones, proporcionando a los ciudadanos mayores facilidades en sus relaciones con la Agencia Española de Protección de Datos.

Además, redundará en la eficacia administrativa (art. 103.1 de la CE) al recibir la Agencia Española de Protección de Datos debidamente cumplimentada la reclamación de que se trate, evitando trámites posteriores que dilatan el procedimiento y dificultan la resolución en plazo (en atención al

elevadísimo volumen de asuntos que tramita la Agencia Española de Protección de Datos).

Todo ello sin perjuicio de que, tal y como reza el art. 66.4 de la LPAC, *“Los solicitantes podrán acompañar los elementos que estimen convenientes para precisar o completar los datos del modelo, los cuales deberán ser admitidos y tenidos en cuenta por el órgano al que se dirijan”*.

A mayor abundamiento, el establecimiento de modelos obligatorios de presentación de reclamaciones ante la Agencia Española de Protección de Datos aliviará la carga de trabajo de la Subdirección General de Inspección de Datos a la que hemos hecho referencia anteriormente. Servirán al propósito de obtener una clasificación previa y automatizada de las reclamaciones presentadas, ahorrando costes administrativos.

En cuanto a la presentación electrónica de la reclamación o el ejercicio de derechos, ésta se realizará en la sede de la Agencia Española de Protección de Datos; a través del procedimiento habilitado electrónicamente se guiará a los afectados, facilitándoles a través del formulario normalizado la presentación al indicarles el suministro de los datos y documentación que fuera preciso, simplificando todo el proceso.

Por otro lado, se hace necesario regular la sustitución de la persona titular de la Presidencia de la Agencia Española de Protección de Datos en los supuestos de ausencia, vacante o enfermedad, así como en los de abstención o recusación, respecto de sus funciones relacionadas con los procedimientos regulados por el Título VIII de la Ley Orgánica 3/2018, de 5 de diciembre, ya que el Consejo de Estado, en su dictamen 683/2020, relativo al proyecto de Real Decreto por el que se aprueba el Estatuto de la Agencia Española de Protección de Datos considera que, en su redacción actual, el ejercicio de esas funciones está reservado por ley a la Presidencia y no cabe, por tanto, su delegación ni la suplencia en su ejercicio. De este modo, si no se procede a su regulación en la ley orgánica, se afectaría negativamente al ejercicio de las competencias de la Agencia y a su independencia, ya que en el supuesto de que dichas circunstancias se produjeran, se impediría su actuación en los casos de posible vulneración de la normativa de protección de datos. En este punto, hay que tener en cuenta que el nuevo procedimiento de designación de la persona titular de la Presidencia requiere, con la finalidad de garantizar su independencia, la realización de unos trámites complejos y la obtención de las correspondientes mayorías reforzadas en el Congreso de los Diputados, lo que puede demorar en exceso su provisión, como lo pone de manifiesto la situación actual, en la que el mandato de la Directora de la Agencia expiró en julio de 2019, sin que a la fecha se hayan iniciado los trámites para el nombramiento de la persona titular de la Presidencia.

Todas las modificaciones propuestas afectan a preceptos del Título VII que no tienen el carácter de orgánicos, conforme a la disposición adicional

primera de la Ley Orgánica 3/2018, por lo que su modificación se puede realizar mediante ley ordinaria. Igualmente, el nuevo artículo 53 bis y la disposición adicional vigésima tercera tienen el carácter de ley ordinaria.