

## 8.2 Exposición sucinta de las actuaciones realizadas en el curso del año 2020

En el curso de 2020 y sin perjuicio de atender diversas consultas y reclamaciones, así como de llevar a cabo el asesoramiento que le fue requerido, el DPD del Ministerio Fiscal realizó actuaciones que, en ocasiones, dieron lugar a recomendaciones dirigidas al Ministerio Fiscal como responsable del tratamiento. Como más significativas, cabe señalar las siguientes:

– Por la Unidad de Apoyo se efectuó consulta al DPD sobre la aplicación web denominada *Calculadora 988*, herramienta que mediante un algoritmo realiza la acumulación de condenas, de modo que se introducen los datos de las sentencias objeto de acumulación para un determinado interviniente y la aplicación realiza todas las combinaciones posibles de cómputo, mostrando el resultado de la combinación más favorable para el reo.

El algoritmo («calculadora»), definido por Fiscalía del Tribunal Supremo, se fundamenta en los arts. 988 LECrim. y 76 del CP, así como en el Acuerdo del Pleno no jurisdiccional de la Sala Segunda del Tribunal Supremo (27/06/2018).

Los datos introducidos en cada acumulación practicada quedan registrados y la aplicación permite guardarlos, de modo que posteriormente puedan ser reutilizados.

En principio, se determinó que solo podrían tener acceso a las acumulaciones realizadas en una determinada fiscalía y, por consiguiente, a los datos relativos a los intervinientes y las condenas registrados, los usuarios (fiscales y funcionarios) que los hubieran introducido en la aplicación, así como el resto de funcionarios y fiscales de esa u otras fiscalías (o los destinados en las secciones de ejecutorias en su caso).

La consulta que se efectuó se centró en la posibilidad de dar visibilidad, esto es, permitir el acceso y puesta a disposición, tanto a los órganos judiciales como a los usuarios de instituciones penitenciarias, de los datos personales introducidos y registrados en las acumulaciones de condenas practicadas por la fiscalía utilizando la aplicación web *Calculadora 988*.

En el informe emitido se concluyó que no existía inconveniente en la intercomunicación de datos entre Ministerio Fiscal y órganos judiciales respecto a las sentencias penales por medio de la aplicación a los fines para los que esta se ha diseñado, al permitir registrar, ordenar y conservar los datos relativos a sentencias penales, datos estos de los que ya efectivamente disponen tanto los órganos judiciales (por ser

ellos los que las generan y tienen la facultad de ejecutar lo juzgado, art. 117.3 CE y 2.1 LOPJ) como el Ministerio Fiscal (por intervenir en los procedimientos penales –art. 3.5 EOMF– al ser parte necesaria en la posterior ejecución, según la Instrucción 1/2010 FGE en virtud de las misiones que tiene encomendadas (art. 124 CE y los arts. 3.1, 3.9 y 4 EOMF).

No obstante, tras analizar la normativa vigente y atendiendo a la doctrina del Tribunal Constitucional sobre los requisitos y circunstancias de la cesión de datos entre Administraciones Públicas, se concluyó que no existía amparo normativo suficiente que diera cobertura a la autorización de acceso de la Administración penitenciaria a los datos introducidos en *Calculadora 988* por los órganos judiciales y por el Ministerio Fiscal, con carácter previo a que les hayan sido formalmente notificadas las correspondientes sentencias penales (ex art. 988 LECrim.), y ello sin perjuicio de que, mediando consentimiento de la concreta persona afectada, por el órgano judicial o por el Ministerio Fiscal y a los fines establecidos en dicho precepto, se pudiera llegar a autorizar la previa visibilidad de las sentencias penales respectivamente registradas en la mencionada herramienta informática.

Finalmente, se puso de manifiesto, vista la naturaleza, objeto, alcance y consecuencias de la operación de tratamiento de datos personales que, mediante el correspondiente algoritmo, efectúa la herramienta informática *Calculadora 988*, y aun cuando esa cuestión no fue objeto de la consulta efectuada al DPD, la exigencia que impone la normativa de protección de datos respecto de la adopción de medidas de índole técnica y organizativa necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, así como la realización de una evaluación de impacto en base a lo dispuesto en el art. 35.1 y 2 b del RGPD, que lo prevé expresamente respecto de las operaciones de tratamiento de datos relativos a condenas penales y específicamente en los casos en los que se tratan datos personales para adoptar decisiones relativas a personas físicas concretas a raíz del tratamiento de datos sobre condenas e infracciones penales o medidas de seguridad conexas (Considerando 91 RGPD).

– Por la Unidad de Apoyo se formuló consulta al DPD a raíz de que, en un borrador de convenio de cooperación educativa entre la Fiscalía General del Estado y una universidad, por esta se interpretaba, respecto de los datos personales por ella suministrados, que el Ministerio Fiscal tenía la condición de encargado de tratamiento de datos personales.

Tras analizar las definiciones recogidas en el art. 4 del RGPD y el Dictamen 1/2010 sobre los conceptos de «responsable del tratamiento» y «encargado del tratamiento», el *Grupo de Trabajo del artículo 29 sobre protección de Datos*, se informó en el sentido de que, en ningún caso, el Ministerio Fiscal se convierte en encargado de tratamiento por el hecho de suscribir acuerdos o convenios en los que se le comuniquen por transmisión datos personales tratados por otra entidad u organismo, sino que, como destinatario de estos, adquiere la condición de responsable de tratamiento lo que le obliga a cumplir las exigencias que, como a tal, la normativa de protección de datos impone.

En ese sentido, idéntica condición y obligaciones adquiere la universidad respecto de los datos personales que por la Fiscalía General del Estado le sean transmitidos en ejecución del referido convenio y ello sin perjuicio de la obligación, por parte de las personas beneficiarias del mismo, de suscribir el correspondiente compromiso de confidencialidad respecto de aquellos datos personales de los que pueden llegar a tener conocimiento en el curso de su ejecución.

– Por una fiscalía de comunidad autónoma se planteó consulta al DPD respecto de si procedía la supresión de datos personales derivados de unas diligencias preliminares que habían sido sobreesridas y obrantes en la Sección de Menores, con el fin de dar respuesta al titular de los mismos, el cual hacía diez años que había alcanzado la mayoría de edad y así lo había requerido; de igual modo se efectuaba consulta sobre el modo, en su caso, de llevar a efecto dicha cancelación.

Se informó que, en este caso concreto, el Ministerio Fiscal es el responsable de tratamiento de los datos personales [art. 48.3 LORPM (Ley 5/2000, de 12 de enero, reguladora de la responsabilidad penal de los menores) e Instrucción FGE 2/2019 (conclusión 5.<sup>a</sup>)], de lo que se deriva que las obligaciones que a este incumben, entre ellas dar respuesta a las solicitudes de los interesados en el ejercicio de sus derechos respecto de esta materia, se llevan a cabo por las distintas fiscalías y órganos fiscales (Conclusión 6.<sup>a</sup> y apartado 7.3 h) por lo que, en consecuencia, sobre la solicitud efectuada debía resolver el fiscal jefe de la fiscalía correspondiente.

La finalidad de preservar esos antecedentes en Fiscalía requería valorar previamente si los datos del interesado eran necesarios para el ejercicio de las funciones encomendadas al Ministerio Fiscal, llegándose a la conclusión, examinados los preceptos de aplicación, que los mismos habían dejado de ser útiles.

También se señaló que, motivos distintos que pueden justificar la conservación de los datos personales por el Ministerio Fiscal (por medio de la documentación y registros de la mencionada Sección de Menores), derivarían de la obligación de mantenerlos (incluso más allá de la fecha del sobreseimiento, de la mayoría de edad o de la prescripción del delito y de la medida) con el fin de acreditar la actividad del Ministerio Fiscal y el concreto desarrollo de las funciones que legalmente tiene asignadas, lo que se encuentra directamente vinculado no solo con la labor de supervisión por parte de los órganos de inspección del Ministerio Fiscal, sino con la obligación de conservar documentos que forman parte del patrimonio documental español (art. 49.2 de la Ley 16/85 del Patrimonio Histórico Español).

Tras analizar la concurrencia de intereses en juego, difícilmente se podía poner en duda que el derecho a la protección de los datos personales debía primar sobre la obligación de conservar esos datos, máxime cuando quedaba constancia del largo lapso de tiempo transcurrido desde que decayó la finalidad para la que se recabaron u obtuvieron y, por tanto, la base legal que legitimaba al Ministerio Fiscal para llevar a cabo su tratamiento.

Por todo ello, se indicó que era parecer del DPD que, tras la incoación del correspondiente expediente gubernativo, debía procederse, después de verificar y contrastar debidamente la identidad del solicitante, a acordar la supresión de los datos personales del interesado (entendiendo por tales todos aquellos que le identificaban directa o indirectamente) de las diligencias preliminares que le afectaban así como de cualquier otro registro obrante en la Fiscalía y ello sin perjuicio de que, una vez suprimidos esos datos y, fundamentalmente, a los fines dispuestos en la Ley 16/1985 de Patrimonio Histórico Español, se conservasen las correspondientes diligencias preliminares y su registro y se dejara debida constancia en ambos de las razones que habían motivado la supresión de los datos personales del interesado.

– A raíz de unos hechos que se produjeron en una fiscalía provincial que hubieran podido llegar a constituir un incidente de seguridad se sugirió a los órganos competentes de la Fiscalía General del Estado, a la vista del modo y plazos en que se adoptaron las correspondientes decisiones, se procediera a establecer, en el ámbito del Ministerio Fiscal en general y de la Fiscalía General del Estado en particular, un protocolo de actuación que permitiese una adecuada y pronta toma de decisiones respecto de posibles violaciones de seguridad.

– Se informó el convenio de colaboración entre el Consejo General del Poder Judicial y la Fiscalía General del Estado para aplicar los métodos adecuados de solución de conflictos y la justicia restaurativa

en el sistema de justicia, en el sentido de que debía incluirse alguna referencia al consentimiento, tanto de la víctima como del infractor, ya que este constituye la base legal que dota de licitud tanto a los sistemas de resolución de conflictos como al tratamiento de datos personales en este ámbito y ello por lo siguiente:

La resolución amistosa de conflictos, en general, como la mediación, en particular, se fundamenta en la libre decisión de las partes, víctima e infractor, quienes conforme a las exigencias de las letras b) y c) del apartado 1 del art. 15 Ley del Estatuto de la Víctima, han de prestar su consentimiento informado con carácter previo a producirse la derivación a la mediación.

Dicho consentimiento (tanto el de la víctima como el del infractor) es también relevante en lo que se refiere al derecho a la protección de datos personales, por cuanto constituye una exigencia ineludible para dotar de licitud al tratamiento de los datos personales de los intervinientes en el proceso de mediación. Ello es así porque el tratamiento de datos con ese fin se fundamenta en una base legal —en este caso el consentimiento—, distinta de aquella que justificó el inicial tratamiento de esos datos en el proceso penal [arts. 5.1.b) y 6 del RGPD].

Para que dicho consentimiento sea válido se habrá de realizar mediante una declaración o una clara acción afirmativa, expresada de manera libre, específica, informada e inequívoca (art. 4.11 RGPD y 6. 1 de la LO 3/2018, de 5 de diciembre de protección de datos personales y garantía de derechos digitales), máxime teniendo en cuenta que, en ocasiones, se podrán llegar a comunicar determinadas categorías especiales de datos (tales como los relativos a la salud) cuyo tratamiento se encuentra expresamente prohibido, salvo que por el interesado se preste un consentimiento explícito (art. 9.1 y 2 del RGPD).

A lo anterior se ha de añadir que los apartados 1 y 2 del art. 7 del RGPD disponen que «cuando el tratamiento se base en el consentimiento del interesado, el responsable deberá ser capaz de demostrar que aquel consintió el tratamiento de sus datos personales» y que «si el consentimiento del interesado se da en el contexto de una declaración escrita que también se refiera a otros asuntos, la solicitud de consentimiento se presentará de tal forma que se distinga claramente de los demás asuntos, de forma inteligible y de fácil acceso y utilizando un lenguaje claro y sencillo. No será vinculante ninguna parte de la declaración que constituya infracción del presente Reglamento.»

Por otro lado, el consentimiento favorable a la mediación debe mantenerse vigente hasta su terminación, con o sin acuerdo. El

art. 15.3 de la LEVD prevé que la víctima y/o el infractor puedan revocar ese consentimiento en cualquier momento.

De igual modo, en el ámbito de la protección de datos, el art. 7.3 del RGPD dispone que «el interesado tendrá derecho a retirar su consentimiento en cualquier momento. La retirada del consentimiento no afectará a la licitud del tratamiento basada en el consentimiento previo a su retirada. Antes de dar su consentimiento, el interesado será informado de ello. Será tan fácil retirar el consentimiento como darlo».

– Se elaboró borrador de convenio entre el Ministerio Fiscal y la Agencia Española de Protección de Datos con el objetivo no solo de incrementar el nivel de colaboración sino también para que, por la AEPD, en el desarrollo de las funciones que la normativa de protección de datos le atribuye, tuviese en cuenta la condición de autoridad judicial del Ministerio Fiscal en el tratamiento de datos con fines jurisdiccionales. En la actualidad dicho convenio todavía no ha sido suscrito.

– En uso de las facultades conferidas en la normativa de aplicación la Instrucción FGE 2/2019, por el DPD del Ministerio Fiscal acompañado de la Fiscal Adjunta al DPD en la Comunidad de Madrid, que actuó en calidad de secretaria, se efectuó visita a la Fiscalía Especial contra la Corrupción y la Criminalidad Organizada, tras lo cual se emitieron los correspondientes informes, proponiendo las medidas correctoras que se estimaron oportunas.

– Se iniciaron actuaciones con el fin de promover de la unidad competente de la Fiscalía General del Estado, la implementación de un control de acceso a los edificios sedes de la Fiscalía General del Estado.

Con el fin de acelerar su implementación, por el DPD se facilitaron: la correspondiente ficha registro de esta actividad de tratamiento; la hoja de información de derechos a los interesados y un modelo de hoja de control de acceso con los datos a solicitar a las personas, ajenas a la FGE, que accedieran a la misma. De igual modo, se sugirió que para ello se utilizase una aplicación específica, aunque dicho registro, hasta en tanto se dispusiese de dicha aplicación, se podría llevar a cabo mediante la herramienta Excel o similar, debiendo tenerse en cuenta que al ordenador en el que se encuentre instalada se habrá de acceder mediante un nombre de usuario y una clave personal de uso individual, ello sin perjuicio de cualesquiera otras medidas de seguridad que se estime oportuno implantar. También se indicó que, dado que los referidos datos han de suprimirse en el plazo de un mes

por la unidad competente de la FGE, se deben establecer pautas de actuación internas con el fin de hacer efectiva dicha obligación.

– Se iniciaron actuaciones de seguimiento y supervisión de la actividad en materia de protección de datos, de las Comisiones Mixtas entre el Ministerio Fiscal y las comunidades autónomas con competencias transferidas en materia de justicia y el Ministerio Fiscal y el Ministerio de Justicia en el resto de comunidades autónomas.

– Se iniciaron actuaciones de supervisión, de ámbito nacional, con el fin de conocer si, vista la situación actual, resulta necesario establecer criterios uniformes, en cuya elaboración, en su caso, colaboraría el Delegado de Protección de Datos, a fin de hacer compatible la exigencia de periódicos expurgos documentales con la obligación de preservar el patrimonio documental del Ministerio Fiscal (art. 89.1 RGPD y 49.2 y 52 de la Ley del Patrimonio Histórico Español) y con el principio de limitación del plazo de conservación de los datos personales de los interesados [art. 5.1 e) RGPD].

– Se iniciaron actuaciones de supervisión de la observancia de la normativa de protección de datos personales con el fin de conocer las actuaciones realizadas en esta materia por todos los órganos, unidades fiscales y fiscalías en base a las pautas recogidas en el documento denominado «Estrategia Inicial sobre protección de datos en el ámbito del Ministerio Fiscal» (difundido en julio de 2019) y en la Instrucción 2/2019 de la Fiscalía General del Estado y, en concreto, sobre cómo se materializa en cada una de ellos el deber de información de derechos a los interesados.

– Se iniciaron actuaciones de supervisión con el fin de conocer actividad pasada y presente, así como los planes de actuación futura diseñados por la Comisión Nacional de Informática y Comunicaciones Electrónicas del Ministerio Fiscal, creada en virtud del Real Decreto 93/2006, de 3 de febrero, por el que se regula el sistema de información del Ministerio Fiscal, así como las actuaciones realizadas por el Comité Técnico de Apoyo.

La razón de ello se fundamenta en que la Comisión Nacional de Informática y Comunicaciones Electrónicas, órgano colegiado que se constituye en el seno del Ministerio Fiscal (diferente, por tanto, en composición, funciones y objetivos al Comité Técnico Estatal de la Administración Judicial Electrónica –CTEAJE– regulado en el RD 396/2013), no solo constituye un pilar fundamental para asegurar la unidad de actuación a través de medios informáticos y telemáticos, así como para el más eficaz cumplimiento de sus funciones constitucionales y estatutarias, sino que resulta esencial para el efectivo cumplimiento por parte del Ministerio Fiscal, como responsable

de tratamiento, de la vigente normativa de protección de datos personales.

De igual modo, se iniciaron actuaciones con el fin de conocer la labor del órgano competente de la Fiscalía General del Estado en el marco de la Política de la Seguridad de la Información de la Administración Judicial Electrónica (PSIJE) aprobada por el CTEAJE y fundamentalmente en relación a la participación en la redacción y aprobación de la PSIJE; la aprobación de los niveles de riesgos propuestos por las administraciones prestatarias; la aprobación de la categorización de los sistemas de información fiscal y la participación y actuaciones llevadas a cabo en el marco del Subcomité de Seguridad.

El fundamento de ello se encuentra en su relación con la protección de datos personales, ya que la Política de la Seguridad de la Información de la Administración Judicial Electrónica (PSIJE) aprobada por el CTEAJE se aplica a todos los sistemas de información y comunicación utilizados por la Administración de Justicia en general (incluyendo, por tanto, al Ministerio Fiscal); afecta a toda la información, tanto de naturaleza jurisdiccional como no jurisdiccional tratada por medios electrónicos, así como en soporte no digital que haya sido causa o consecuencia del tratamiento digital y es de obligado cumplimiento en el desarrollo de la actividad de las fiscalías por parte de todos sus integrantes.

– Se iniciaron actuaciones con el fin de promover de la unidad competente de la Fiscalía General del Estado la actualización de la web *fiscal.es* a la normativa vigente en materia de protección de datos. Para ello se procedió a establecer el diseño y contenido de dicho portal, así como, por estar directamente vinculado, a elaborar el inventario de registro de actividades de tratamiento del Ministerio Fiscal, procediéndose a elaborar el contenido de todos y cada uno de los registros, y ello con el fin de hacer efectiva, a la mayor brevedad posible, su publicación por medios electrónicos de conformidad con lo establecido en el art. 31.2 de la LO 3/2018.

– Se emitió dictamen, en cumplimiento de la función de asesoramiento al Ministerio Fiscal en aquellas cuestiones relativas a la protección de datos, en este caso, a fin de auxiliar en la función consultiva que corresponde al Consejo Fiscal en aquellos aspectos del proyecto legislativo que puedan afectar a la estructura, organización y funciones del Ministerio Fiscal en relación al Anteproyecto de Ley Orgánica de *protección de datos personales tratados para fines de prevención, detección, investigación o enjuiciamiento de infracciones penales y de ejecución de sanciones penales, así como de protección y prevención frente a las amenazas contra la seguridad pública* (APLO) con el

que se pretendía trasponer la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales y a la libre circulación de dichos datos, por la que se deroga la Decisión Marco 2008/977/JAI del Consejo.

Por el Consejo Fiscal, en su sesión de 28 de abril de 2020 se suscribió el referido dictamen incorporándose su contenido al informe (de 7 de mayo) evacuado por dicho órgano en cumplimiento de lo dispuesto en el art. 14.4 j) EOMF.

Por el DPD se analizó el APLO, realizándose observaciones, recomendaciones y propuestas de modificación, siendo las más significativas las siguientes:

a) Se valoró muy negativamente la remisión normativa por la que optaba el Anteproyecto en lo que respecta a los tratamientos de datos personales efectuado por el Ministerio Fiscal (y por los órganos judiciales competentes) dado que, en la actualidad, la regulación en materia de protección de datos en las normas procesales penales y en el EOMF es prácticamente inexistente, siendo insuficiente y desfasada la de la LOPJ.

En virtud de ello, se reclamó una adecuada y completa regulación de esta materia por considerarlo esencial al afectar no solo al ejercicio de las funciones del Ministerio Fiscal, sino a un derecho fundamental, en este caso, el de la protección de datos personales de los ciudadanos, del que también es garante el Ministerio Público. En el dictamen se consignaron, de modo concreto, todas aquellas cuestiones que debían ser reguladas.

b) Se propuso la modificación del artículo del APLO que recogía el deber de colaboración de las administraciones públicas, personas físicas y jurídicas con las autoridades competentes ya que, en su redacción original se otorgaba a las mismas una aparente autoridad de supervisión y control sobre el cumplimiento por parte de la autoridad requerente de la conveniencia y legalidad de lo solicitado.

Se consideró que dicha exigencia podría ser perturbadora, cuando además nada añadía a un deber preexistente fruto de exigencias legales, genéricas o específicas, o vinculado a las normas que legitiman a las autoridades competentes para ejercer sus funciones, no siendo razonable que el examen de legalidad sobre lo solicitado pueda trasladarse a los sujetos requeridos, ello sin perjuicio de que por las autori-

dades competentes, cumpliendo la normativa vigente, se deban respetar los principios que inspiran el derecho a la protección de datos personales.

c) En diversos apartados del dictamen se insistió en el hecho de que el Ministerio Fiscal realiza tratamientos de datos con fines jurisdiccionales, así como que debía de tenerse en cuenta su condición de autoridad judicial a los efectos de la Directiva y del RGPD.

d) Se consideró imprescindible una adecuada y completa regulación sobre el ejercicio de los derechos de los interesados como consecuencia de investigaciones y procesos penales.

En ese sentido se apuntó que, sin duda el ejercicio de los derechos reconocidos en la normativa de protección de datos por parte de las distintas categorías de interesados, es una materia compleja que hubiera requerido de un mayor esfuerzo que el realizado por el prelegislador en el APLO, ya que, básicamente, se remite a una normativa (la de la LOPJ) que no brinda suficiente cobertura legal al ejercicio de la totalidad de esos derechos, ofreciéndose, por tanto, una muy precaria solución dadas las singularidades que conlleva la tramitación de las diligencias y procesos de naturaleza penal.

e) Se insistió en la necesidad de la creación de la Unidad de Protección de Datos, (exigencia que se había venido reclamando por el DPD desde sus primeros informes del año 2018 y 2019) como órgano específico de supervisión el cual tendría, respecto del tratamiento de datos con fines jurisdiccionales realizado por el Ministerio Fiscal, las competencias y facultades que por la normativa de protección de datos se atribuya a la Agencia Española de Protección de Datos. Dicho órgano tendría que tener garantizada y reconocida estatutariamente la independencia en el ejercicio de sus funciones, con el fin de actuar con plena libertad y a resguardo de cualquier tipo de instrucciones o presiones.

La razón de ello se justifica, por un lado, en que la protección de datos personales, como derecho moderno y activo que es, se basa en un sistema de controles y equilibrios para proteger a las personas cuando se tratan sus datos personales. El tratamiento debe cumplir con las exigencias esenciales de la protección de datos personales, que consisten, básicamente, en la existencia de una base legal para el tratamiento respecto a los derechos del interesado y en el establecimiento de una supervisión independiente; así, la Carta Europea de los Derechos Fundamentales, proclamada en Niza el 8 de diciembre de 2000 e incorporada a los Tratados constitutivos de la Comunidad Europea en el Tratado de Lisboa, declaró en su art. 8.3 que el respeto a las normas de protección de datos quedará sujeto al control de una autoridad independiente.

Y por otro en que la nueva normativa de protección de datos se ha de integrar, como cualquier otra, en el ordenamiento jurídico existente el cual, respecto de lo que aquí se trata, define al Ministerio Fiscal como órgano de relevancia constitucional con personalidad jurídica propia, independiente en el ejercicio de sus funciones de los distintos poderes del estado (art. 7 EOMF) e integrado con autonomía funcional en el Poder Judicial y que ejerce su misión por medio de órganos propios (art. 2.1 EOMF).

En relación a las autoridades de control, el RGPD dispone que cada Estado miembro establecerá que una o varias de ellas asuman la supervisión de la aplicación del Reglamento, así como que «las autoridades de control no serán competentes para controlar las operaciones de tratamiento efectuadas por los tribunales en el ejercicio de su función judicial» (art. 51.1 y 53.3). En España la condición de autoridad de control corresponde a la AEPD y a aquellas agencias existentes en determinadas comunidades autónomas, no obstante, la competencia de estas últimas no se extiende a la actividad del Ministerio Fiscal ya que su ámbito de actuación se limita exclusivamente al sector público autonómico [art. 57.1 a) LOPD].

De igual modo, la Directiva 2016/680 establece que «los Estados miembros dispondrán que cada autoridad de control no sea competente para controlar las operaciones de tratamiento efectuadas por los órganos jurisdiccionales en el ejercicio de su función judicial. Los Estados miembros podrán disponer que su autoridad de control no sea competente para controlar las operaciones de tratamiento efectuadas por otras autoridades judiciales independientes en el ejercicio de su función judicial» (apartado 2.º del art. 45).

El RGPD dispone que «a fin de preservar la independencia del poder judicial en el desempeño de sus funciones, incluida la toma de decisiones, la competencia de las autoridades de control no debe abarcar el tratamiento de datos personales cuando los tribunales actúen en ejercicio de su función judicial. El control de esas operaciones de tratamiento de datos ha de poder encomendarse a organismos específicos establecidos dentro del sistema judicial del Estado miembro, los cuales deben, en particular, garantizar el cumplimiento de las normas del presente Reglamento, concienciar más a los miembros del poder judicial acerca de sus obligaciones en virtud de este y atender las reclamaciones en relación con tales operaciones de tratamiento de datos» (Considerando 20).

En el mismo sentido, la Directiva 2016/680 establece que «los Estados miembros pueden disponer que la competencia de la autoridad de control no abarque el tratamiento de datos personales realizado por

otras autoridades judiciales independientes en el ejercicio de su función jurisdiccional, por ejemplo, la fiscalía, y en todo caso, el cumplimiento de las normas de la presente Directiva por los órganos judiciales independientes debe estar sujeto siempre a una supervisión independiente de conformidad con el artículo 8, apartado 3, de la Carta», añadiendo, que las competencias de la autoridad de control «no deben afectar a las normas específicas previstas para los procesos penales, incluidos la investigación y el enjuiciamiento de infracciones penales, ni a la independencia del poder judicial» (Considerandos 80 y 82).

En consecuencia y con independencia de los términos utilizados en el RGPD (poder judicial, tribunales, otras autoridades judiciales), lo que el legislador europeo pretende es garantizar la separación de poderes y la independencia en el ejercicio de funciones jurisdiccionales, razón por la cual la supervisión de los tratamientos de datos de esa naturaleza deberá ser realizada por «organismos específicos establecidos dentro del sistema judicial» del estado miembro y no por entidades de control vinculadas al poder ejecutivo (aunque de ellas se predique su independencia) ya que, también los tratamientos de los datos personales incorporados o derivados de un proceso jurisdiccional se encuentran sometidos a un régimen jurídico singular coexistiendo, en ese ámbito, el derecho a la protección de datos personales con otros derechos fundamentales.

La LOPJ reconoce al CGPJ como organismo específico de supervisión respecto de los tratamientos de datos con finalidad jurisdiccional disponiendo que ejercerá, respecto de los tratamientos efectuados con fines jurisdiccionales y los ficheros de esta naturaleza, las competencias que la Ley Orgánica 15/1999, de 13 de diciembre, atribuye a la Agencia Española de Protección de Datos (apartado primero art. 236 *nonies*). En la actualidad se ha de entender que dicha remisión se realiza a la LOPDGDD.

A su vez, la LOPDGDD dispone que el tratamiento de datos llevado a cabo con ocasión de la tramitación por los órganos judiciales de los procesos de los que sean competentes, así como el realizado dentro de la gestión de la Oficina Judicial, se regirán por lo dispuesto en el RGPD y en la presente Ley Orgánica, sin perjuicio de las disposiciones de la LOPJ que le sean aplicables y que, cuando se trate de órganos judiciales u oficinas judiciales, el ejercicio de las facultades de inspección por la AEPD se efectuará a través y por mediación del Consejo General del Poder Judicial (art. 2.4 y 53.3).

Por otro lado, el art. 171 de la LOPJ dispone que el CGPJ ejerce la superior inspección y vigilancia sobre todos los Juzgados y Tribunales

para la comprobación y control del funcionamiento de la Administración de Justicia.

De la lectura conjunta de los antes mencionados preceptos se ha de concluir que la competencia del CGPJ, como autoridad supervisora de los tratamientos con fines jurisdiccionales, se limita a aquellos realizados por los juzgados y tribunales en el ejercicio de su función jurisdiccional, razón por la que el Ministerio Fiscal, al no ser órgano judicial, queda fuera de ese marco de competencia funcional.

Por las mismas razones (salvaguarda de la autonomía funcional y proscripción de injerencias externas) la función de autoridad de control en los tratamientos de datos con fines jurisdiccionales realizados por el Ministerio Fiscal, tampoco debe ser asumida por la AEPD y ello pese a que han sido varias las ocasiones en las que en el pasado se realizaron actuaciones que comprometieron la independencia del Ministerio Fiscal.

En este aspecto, ha de tenerse en cuenta que si la AEPD tiene encomendada la supervisión del derecho de protección de datos personales, en el ámbito jurisdiccional es el Ministerio Fiscal el garante, tanto de ese como de otros derechos fundamentales (art. 124 CE, 1 y 3.3 EOMF), los cuales no se deben ver comprometidos en el ejercicio de las facultades de inspección encomendadas a una entidad administrativa cuando, además, en el curso de la misma, se podrían llegar a conocer no solo los datos personales objeto de protección, sino también la naturaleza del conflicto que se dirime.