

8.2 Exposición sucinta de las actuaciones realizadas por el DPD en el curso del año 2022

En el curso de 2022 se puso de manifiesto el incremento de la actividad de la Unidad del Delegado de Protección de Datos al haberse registrado un total de 105 expedientes frente a los 73 del año anterior; expedientes que dan soporte a actuaciones iniciadas de oficio o a aquellas generadas como consecuencia de consultas y reclamaciones.

Entre las actuaciones realizadas, cabe reseñar las siguientes:

8.2.1 INFORMES DE ANTEPROYECTOS LEGISLATIVOS

El DPD en base a lo dispuesto en los artículos 38.1 y 39.1 a) del RGPD y en la Instrucción FGE 2/2019 y, en este caso, a fin de auxiliar en la función consultiva que corresponde al Consejo Fiscal [conforme a lo dispuesto en el art. 14.4 j) EOMF] y en cumplimiento de la función de asesoramiento en aquellas cuestiones relativas a protección de datos emitió diversos informes en aquellos aspectos de diversos proyectos legislativos que pudieran afectar a la estructura, organización y funciones del Ministerio Fiscal así como, en su caso, en relación a otros aspectos a fin de contribuir a la mejora de los mismos, entre otros los siguientes:

8.2.1.1 *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*

Dicho Anteproyecto tiene una singular importancia a los efectos de la modernización y adaptación de la realidad judicial española al marco tecnológico actual.

El APL define los servicios digitales que las Administraciones con competencia en materia de Justicia han de prestar de manera homogénea y de calidad en todo el territorio del Estado, servicios que se manifiestan indispensables para el funcionamiento correcto de la Justicia como, entre otros, la tramitación electrónica de los procedimientos, la itineración de expedientes electrónicos y la transmisión de documentos electrónicos entre cualesquiera órganos judiciales u oficinas fisca-

les y la interoperabilidad de datos entre cualesquiera tribunales, oficinas judiciales y fiscales.

Se recoge el principio general de tramitación electrónica orientada al dato, en virtud de ello se establece el principio general de una Justicia basada en datos, por lo que los sistemas de Justicia asegurarán la entrada y tratamiento de información en forma de metadatos, conforme a esquemas y datos comunes e interoperables.

Se pretende no solo la eliminación del papel físico, sino establecer el expediente judicial electrónico considerando a este como un conjunto de datos estructurados incluyendo así documentos, trámites, actuaciones electrónicas, o incluso grabaciones audiovisuales correspondientes a un procedimiento judicial.

En el informe por el DPD se pusieron de manifiesto, entre otras cuestiones las siguientes:

– En relación a los derechos de los ciudadanos relativos a la garantía de la seguridad y confidencialidad de los datos que figuren en los ficheros, sistemas y aplicaciones de la Administración de Justicia, en los términos establecidos en la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial, en las leyes procesales y en la presente ley, recogido en el apartado e) del art. 6.2 del APL se sugirió, con el fin de especificar a quien corresponde garantizar dicha seguridad y confidencialidad y en los mismos términos que dispone el art. 236 sexies LOPJ, se añadiese que correspondiera a la Administración competente cumplir con las responsabilidades que, como administración prestacional, tenga atribuidas en dicha materia.

– Respecto al acceso digital a la Administración de Justicia, en el artículo 17 del APL relativo al acceso al expediente judicial electrónico se recoge, básicamente, las previsiones contenidas en los arts. 234, 235 y 236 quinquies 2 LOPJ, relacionadas con derecho al acceso a los procedimientos por quienes sean parte o tengan interés legítimo, así como las limitaciones existentes al ejercicio de dicho derecho.

En congruencia con ello, se aconsejó la sustitución del verbo «podrán» del artículo 17.2 del APL por el verbo «deberán» ya que el acceso a actuaciones procesales, por quienes no son parte en el procedimiento y acrediten un interés legítimo y directo, en términos generales y a la vista de la vigente normativa de protección de datos requerirá, en términos generales, la previa seudonimización, anonimización u otra medida de protección de los datos de carácter personal que las mismos contuvieren.

– Sobre la tramitación electrónica de los procedimientos judiciales, se propuso una redacción alternativa del art. 31.1 APL, que a criterio del DPD, recogía una confusa mezcla entre registro de actividades de tratamiento y registro de operaciones, ya que los registros de actividades de tratamiento no se han establecido en la normativa de protección de datos (en este caso en la Directiva) para controlar el acceso a los equipos y dispositivos, sino para demostrar que se cumple lo dispuesto en la misma, por lo que los responsables y encargados deberán mantener registros relativos a todas las categorías de actividades de tratamiento que se lleven a cabo bajo su responsabilidad en los que se han de incluir la información que se recoge en el art. 30 RGPD y 32 LO 7/2021 y por otro lado, que la determinación de la justificación, la fecha y la hora de las operaciones, la persona que consultó o comunicó datos personales, así como la identidad de los destinatarios de dichos datos personales tiene como finalidad última incrementar la integridad y la seguridad de los datos personales.

– En relación al acceso a los sistemas de información por los órganos competentes dependientes del Consejo General del Poder Judicial, de la Fiscalía General del Estado y del Ministerio de Justicia que, según se recogía en el art. 31.4 APL, requería la puesta en conocimiento de la Administración prestacional del servicio, quien deberá autorizar el acceso para el cumplimiento de las funciones de inspección y control establecidas en las leyes y su normativa de desarrollo, se consideró que no era acorde con la normativa de protección de datos por lo que se propuso una redacción alternativa ya que tanto la Unidad de Protección de Datos del Ministerio Fiscal, como el Delegado de Protección de Datos, pueden ejercer labores de supervisión e inspección de procedimientos y por tanto tendrían legitimación para acceder a los sistemas de información sin autorización previa alguna.

– Sobre el Comité Estatal de la Administración Judicial Electrónica, y dado que se pretende potenciar dicho Comité como órgano de cogobernanza de la Administración digital de la Justicia y de impulso y coordinación del desarrollo de la transformación digital de la Administración de Justicia, se sugirió que al Ministerio Fiscal se le otorgase, en el APL, un mayor protagonismo de modo que su representante en el CTEAJE formase parte de la presidencia (en las mismas condiciones que los representantes del Ministerio de Justicia y del CGPJ) y ello teniendo en cuenta, por un lado que en la actualidad el Ministerio Fiscal tramita diligencias de naturaleza procesal y preprocesal, las cuales habrían de tener unos requisitos y gozar de garantías similares a las del expediente judicial electrónico (art.47 y 48 APL), porque

previsiblemente se asumirá, en un futuro más o menos cercano, la dirección de la instrucción de los procedimientos penales.

En relación con la modernización tecnológica se recordó por el DPD la existencia de la Comisión Nacional de Informática y Comunicaciones Electrónicas, órgano colegiado creado en virtud de RD 93/2006, de 3 de febrero, *por el que se regula el sistema de información del Ministerio Fiscal* y cuya puesta en marcha al parecer nunca se hizo realmente efectiva.

La Comisión Nacional de Informática, cuyo impulso se ha venido promoviendo por el DPD desde años atrás, tal como ya se puso de manifiesto en la Memoria 2021 (ejercicio 2020), no solo constituye un pilar fundamental para asegurar la unidad de actuación a través de medios informáticos y telemáticos 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.

– Sobre la textualización de las actuaciones orales, en el APL en el apartado 1 m) del artículo 4 relativo a los servicios electrónicos homogéneos de la Administración de Justicia se menciona la «posible» textualización de actuaciones orales registradas en soporte apto para la grabación y reproducción del sonido y la imagen.

Por el DPD se sugirió que no se contemplase como una facultad sino como una obligación ya que la transcripción escrita por medios automatizados de juicios, audiencias o diligencias de instrucción de naturaleza personal (y fundamentalmente de estas últimas) resulta esencial para un eficiente y eficaz ejercicio de la función encomendada al Ministerio Fiscal (también para los jueces y tribunales que han de resolver los recursos) básicamente en el ámbito del proceso penal.

8.2.1.2 *Anteproyecto de Ley reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción por la que se transpone la Directiva (UE) 2019/1937 del Parlamento Europeo y del Consejo, de 23 de octubre de 2019, relativa a la protección de las personas que informen sobre infracciones del Derecho de la Unión (en adelante APL)*

El referido APL persigue intensificar y proteger la colaboración ciudadana cuando se facilita información que pueda ayudar a la investigación y consiguiente persecución de conductas ilegales, evitando

consecuencias indeseadas para quienes han comunicado prácticas corruptas y otras infracciones.

En el informe por el DPD se pusieron de manifiesto, entre otras cuestiones las siguientes:

– La primera de ellas era si la referida normativa, atendiendo al ámbito material y personal de aplicación del APL, resulta aplicable al Ministerio Fiscal.

Tras diversas consideraciones se concluyó que la normativa contenida en el APL es de aplicación al Ministerio Fiscal y que, al ser un órgano de relevancia constitucional (art. 2.1 EOMF), deberá contar con un canal interno de información con el fin de amparar a aquellas personas que en el entorno del Ministerio Público comuniquen irregularidades que afecten al interés general permitiendo también a la institución actuar y poner fin a la actividad ilícita advertida.

Dicho canal serviría para dar cauce a denunciar conductas delictivas o administrativas graves o muy graves que cometidas en el seno del Ministerio Fiscal, afectasen al interés público, así como en lo que se refiere a infracciones del Derecho de la Unión Europea, y visto el elenco de disposiciones de derecho que se recogen en el Anexo de la Directiva, quedaría circunscrita, básicamente, a aquellas relativas a la afectación al derecho a la privacidad y a la protección de los datos de carácter personal.

– Se valoró positivamente la referencia a la licitud del tratamiento de datos personales necesarios para la aplicación del APL que se contiene en su artículo 30 y ello sin perjuicio de que dicha legitimación ya venía contemplada tanto en la LO 3/2018.

– Por otro lado, en el art. 16 de la Directiva a transponer, respecto del deber de confidencialidad, y después de establecer en su apartado primero que «los Estados miembros velarán por que no se revele la identidad del denunciante sin su consentimiento expreso a ninguna persona que no sea un miembro autorizado del personal competente para recibir o seguir denuncias», expresamente recoge que «la identidad del denunciante y cualquier otra información prevista en el apartado 1 solo podrá revelarse cuando constituya una obligación necesaria y proporcionada impuesta por el Derecho de la Unión o nacional en el contexto de una investigación llevada a cabo por las autoridades nacionales o en el marco de un proceso judicial, en particular para salvaguardar el derecho de defensa de la persona afectada».

Al igual que la Ley Orgánica 19/1994, de 23 de diciembre, *de protección a testigos y peritos en causas criminales*, contempla el derecho de las partes intervinientes en el proceso a conocer la identidad de

los testigos en su art. 4.3, en el apartado 4 del artículo 2 del APL, se dispone que la protección que se dispensa a las personas físicas que informen «no excluirá la aplicación de las normas relativas al proceso penal, incluyendo las diligencias de investigación».

En virtud de todo ello, y teniendo en cuenta que la información de derechos a los denunciantes-informantes, ha de ser veraz y completa con el fin de que puedan tomar una decisión informada y libre en el momento de denunciar, el DPD sugirió modificar el párrafo segundo del apartado primero del artículo 31 APL en el siguiente sentido:

«A los informantes y a quienes lleven a cabo una revelación pública se les informará, además, de forma expresa, que su identidad será en todo caso reservada, que no se comunicará a las personas a las que se refieran los hechos relatados ni a terceros, y ello salvo en los supuestos contemplados en el apartado 3 del artículo 33.»

En consecuencia, se habría de modificar también el referido apartado 3 del artículo 33 APL, en el siguiente sentido:

«La identidad del informante sólo podrá ser comunicada a la Autoridad judicial, al Ministerio Fiscal o a la autoridad administrativa competente en el marco de una investigación penal, disciplinaria o sancionadora.

En el curso de procesos penales, de diligencias de investigación y de procedimientos de naturaleza disciplinaria, y en este último supuesto exclusivamente por infracciones graves o muy graves, dicha identidad podrá revelarse a las personas investigadas únicamente cuando resulte imprescindible para salvaguardar su derecho de defensa y tras resolución debidamente motivada.»

8.2.1.3 *El Anteproyecto de Ley Orgánica por la que se modifica la Ley Orgánica 2/2010, de 3 de marzo, de salud sexual y reproductiva y de la interrupción voluntaria del embarazo*

Tiene por objeto, entre otras cuestiones: garantizar la prestación del servicio de interrupción voluntaria del embarazo en los centros públicos hospitalarios, así como permitir a las mujeres tomar libremente las decisiones que atañen a su interrupción voluntaria del embarazo; permitir a las adolescentes de 16 y 17 años, así como a las mujeres con discapacidad, interrumpir voluntariamente su embarazo sin necesidad de consentimiento de sus representantes legales; esta-

blecer servicios de asistencia integral especializada y accesible para la promoción de la salud sexual y la salud reproductiva en todas las fases del ciclo vital.

En el informe por el DPD se realizaron algunas matizaciones, así:

– Respecto de la creación de un registro de personas objetoras de conciencia en cada Comunidad Autónoma, el APLO omite especificar la entidad que asumiría la responsabilidad de la gestión del mismo y tampoco establece los criterios que permitirían identificar a ese organismo al que atribuir esa condición de responsable, lo cual resulta preciso para determinar, sobre quien ha de recaer las obligaciones y exigencias que la normativa de protección de datos impone a los responsables del tratamiento.

Por ello se aconsejó que, en los términos expresados, se subsanase dicha omisión ya que carece del necesario rigor técnico referencias tales como a que sea el propio registro el que garantice el derecho a la confidencialidad de las personas profesionales sanitarias y el que se someta a la normativa de aplicación en materia de protección de datos de carácter personal (tal como se recoge en el apartado 3 del art. 19 ter).

– Por otro lado, y en lo que se refiere a la evaluación de impacto y de conformidad con lo dispuesto en el art. 35.1 RGPD, se apuntó que se incluyese que la misma habrá de realizarse antes de proceder al tratamiento dada la complejidad de este tipo de procesos y con el fin de evitar el riesgo de que se inicie el tratamiento de datos sin que se haya llevado a cabo la referida evaluación.

– En relación al artículo del APL relativo a la supresión de oficio de la totalidad de los datos de la paciente que figuren en los registros, se planteó la modificación del mismo, al resultar su redacción muy confusa.

– Finalmente, en lo que respecta al específico plazo de cinco años, se consideró que el legislador debería justificar las razones por las que se ha fijado ese concreto periodo de tiempo ya que, salvo razones expresas que así lo justificasen y dada la naturaleza de la prestación sanitaria en cuestión, el mismo debiera ser considerablemente más reducido y se alude al ejemplo de las acciones para exigir responsabilidad civil por las obligaciones derivadas de culpa o negligencia, que en principio serían las que corresponderían a aquellas producidas en un centro de salud pública o por sus profesionales sanitarios, prescriben por el transcurso de un año (art. 1968.2 CC).

8.2.2 CONSULTAS ELEVADAS AL DPD

8.2.2.1 *Colaboración en la elaboración de las conclusiones de diversas jornadas de especialistas*

Concretamente se colaboró en las conclusiones de cooperación internacional, víctimas y atención a las personas con discapacidad y mayores, y ello tras las consultas efectuadas por las distintas unidades de la Fiscalía General del Estado en aquello que afectaba a la protección de datos personales.

8.2.2.2 *Consulta respecto del acceso a datos personales de naturaleza jurisdiccional en los supuestos de delitos cometidos en territorio nacional por miembros de las fuerzas armadas norteamericanas, o de un elemento civil y las personas dependientes de los mismos, por parte del denominado «Grupo de Asuntos Jurisdiccionales» (en adelante GAJ) recogido en el art. 3 del Real Decreto 1524/2007, de 16 de noviembre, por el que se regula la organización y funcionamiento de la Sección Española del Comité Permanente Hispano-Norteamericano (CPHN)*

El objetivo era, tanto el de que en tiempo oportuno se pueda dirigir a la Fiscalía de la Audiencia Nacional la pertinente recomendación relativa a una posible cesión de jurisdicción, como el de asistir a la representante del Ministerio Fiscal en dicho Grupo, se hicieron diversas consideraciones:

– El art. 7 del Convenio entre el Reino de España y los Estados Unidos de América de Cooperación para la Defensa de 1 de diciembre de 1988 (revisado por los Protocolos de Enmienda de 10 de abril de 2002, 10 de diciembre de 2012 y 17 de junio de 2015) establece un Comité Permanente para asegurar la necesaria coordinación entre las Partes en el desarrollo del mismo y para estudiar y resolver, en su caso, las cuestiones que, en los respectivos países, plantee su aplicación y no puedan ser solucionadas dentro de la competencia de las autoridades españolas y estadounidenses directamente responsables. El referido Comité Permanente, continúa dicho artículo, estará constituido por dos Secciones, española y estadounidense.

– El GAJ, pese a que uno de sus componentes pertenece al Ministerio Fiscal, no es parte en el procedimiento a los efectos de lo dispuesto en la Ley de Enjuiciamiento Criminal ni tiene, a los efectos

prevenidos en los arts. 1 y 4 LO 7/2021, la consideración de autoridad competente.

– El GAJ, con el fin de poder emitir fundadamente sus recomendaciones, ha de disponer de suficiente información para lo cual, de no contar previamente con ella, precisa acceder a determinadas actuaciones y/o documentos obrantes en los procedimientos penales, lo cual supone el consiguiente tratamiento de datos personales.

– El tratamiento de datos que lleva a cabo el GAJ (preciso para la elaboración y emisión de recomendaciones para la cesión de jurisdicción) aunque sea para un fin distinto para el que fueron inicialmente recabados (investigación e instrucción del procedimiento penal) cuenta con base legal para su materialización, ya que la misión que tiene asignada se contempla en un Convenio Internacional que forma parte del derecho nacional (art. 6.3 L. O. 7/2021 y art. 96.1 CE).

– Como consecuencia de las funciones que tiene atribuidas en virtud del referido Convenio Internacional (arts. 39 y 40), el GAJ, pese a no ser parte en los procedimientos penales, tiene la condición de interesado ya que ostenta un interés legítimo para obtener copias simples de los escritos y documentos que consten en los autos, no declarados secretos ni reservados (art. 234. 1 y 2 en relación al 235 LOPJ).

– La solicitud para obtener dichos documentos ha de efectuarse por escrito y de forma motivada ante el órgano judicial correspondiente con el fin de que este, cuando así lo estime oportuno, adopte las medidas convenientes para la protección de los datos de carácter personal que los mismos contuvieren y con pleno respeto al derecho a la intimidad, a los derechos de las personas que requieran un especial deber de tutela o a la garantía del anonimato de las víctimas o perjudicados (arts. 234 y 235 LOPJ; art. 11 d) Real Decreto 1608/2005, de 30 de diciembre, por el que se aprueba el Reglamento Orgánico del Cuerpo de Secretarios Judiciales y arts. 2, 4 y 5 Reglamento 1/2005, de los aspectos accesorios de las actuaciones judiciales).

– La denegación de la solicitud por parte del órgano judicial, caso de producirse, podría ser impugnada tanto por el Grupo de Asuntos Jurisdiccionales dada su condición de interesado, por el propio investigado como parte del procedimiento, como, de estimarse oportuno, por el Ministerio Fiscal (art. 3.1 EOMF).

– El GAJ, de obtener del órgano judicial la información solicitada, estará obligado a tratar los datos de conformidad con la normativa de protección de datos (art. 236 quinquies 3) LOPJ), debiendo cumplir, en todo caso, los principios relativos al tratamiento (art. 6.1 LO 7/2021).

– El Grupo de Asuntos Jurisdiccionales, a la vista de lo dispuesto en la LO 7/2021, en principio, y salvo autorización del órgano judicial, no se encuentra facultado para comunicar a terceros información de naturaleza personal obrante en los documentos o actuaciones procesales que no esté debidamente anonimizada o seudonimizada, debiendo tenerse en cuenta que el acceso a los mismos por parte de la Sección Estadounidense podría suponer una transferencia internacional de datos personales contraria a la normativa vigente.

8.2.2.3 *Consulta efectuada por la Unidad Especializada de Extranjería en relación a la conformidad con la normativa de protección de datos respecto del volcado de datos personales contenidos en el Registro de Menores No Acompañados (RMENA) a la Plataforma de Registro de Protección Temporal (Temporary Protection Registration Platform)*

La consulta se enmarca en la autorización que a esos efectos solicitó la Secretaría General de la Comisaría de Extranjería y Fronteras, se hicieron diversas consideraciones:

El RMENA tiene por finalidad, básicamente, coordinar la intervención de las diferentes instituciones y administraciones para que actúen, desde la localización de los menores extranjeros que se encuentren sin familia en España, hasta su identificación, determinación de su edad, puesta a disposición del servicio público de protección de menores y documentación. Todo ello con el fin de facilitar su protección dada su situación de especial vulnerabilidad y desamparo.

La Plataforma de Registro de Protección Temporal fue creada en el marco del Derecho de la Unión en virtud de la Decisión de Ejecución 2022/382 de 4 de marzo y en base al acuerdo adoptado en el Consejo de Justicia e Interior de 28 de marzo 2022. Tiene por finalidad intercambiar información sobre las personas registradas para que aquellas que huyen de Ucrania puedan ser protegidas, beneficiarse de sus derechos en todos los Estados de la Unión Europea, preservar la unidad de las familias evitando que los miembros de una misma unidad familiar tengan estatutos diferentes, así como procurar que todos los Estados miembros realicen un esfuerzo equitativo.

En consecuencia, cabe concluir que el tratamiento ulterior en la Plataforma de Registro de Protección Temporal de los datos de los menores solicitantes de protección temporal obrantes en el RMENA resulta compatible con la finalidad para la que inicialmente se trataron

al no ser ajenos al ámbito de aplicación de este (ex art. 215.1 REX y 35.10 LEX) dada la identidad de los fines para los que se tratan los datos en ambos registros.

Dicha conclusión se ve fortalecida por el expreso sometimiento de ambos tratamientos a la normativa europea de protección de datos; por la común naturaleza de los datos personales objeto de tratamiento así como por el hecho de que el tratamiento ulterior que se pretende encuentra su fundamento tanto en el derecho de la UE como en el derecho nacional y constituye una medida necesaria y proporcional en una sociedad democrática para garantizar, en el ámbito de la Unión, la debida y adecuada protección de personas desplazadas en situación de desamparo (incluidas los menores) y para procurar, también, su reagrupamiento familiar.

Conforme a lo expuesto y teniendo en cuenta el superior interés de los menores afectados, no se apreció impedimento para que se autorizase la transmisión a la Plataforma Europea de Protección Temporal de los datos del Registro MENA, referidos a nombre, apellido, nacionalidad, tipo de protección e identificador del sistema nacional de aquellos menores solicitantes de protección temporal que se hallen inscritos en el referido registro, sin indicación de su categorización como menor no acompañado. Así como, en el supuesto de una eventual coincidencia por el intercambio de datos que ofrece la Plataforma, ceder al Estado en el que se ha producido dicha coincidencia los datos personales adicionales que sean adecuados, pertinentes y limitados a lo necesario para una efectiva tramitación de la protección temporal.

No obstante, se recordó la obligación de garantizar a los interesados la efectiva aplicación de los principios establecidos en el art. 5 RGPD y, en particular, la información sobre ese ulterior tratamiento y sobre sus derechos, incluido el derecho de oposición (Considerando 50, arts. 13 y 21 RGPD).

8.2.2.4 *Consulta realizada por una asociación de fiscales sobre el tratamiento de datos efectuado por una Unidad de la Fiscalía General del Estado*

A lo cual se respondió que no era posible atender a dicha solicitud dado que la petición efectuada no resultaba acorde con la normativa vigente.

La función de asesoramiento que se otorga al DPD se regula, básicamente, en el RGPD, en las Directrices sobre Delegados de Protección de Datos del GT29 y en la Instrucción FGE 2/2019 la cual

traslada dicha regulación al ámbito del Ministerio Fiscal (apartado 8.2.3.4.). En virtud de dicha normativa, las funciones de informar, asesorar y emitir recomendaciones que se asignan al DPD se establecen únicamente en favor del responsable del tratamiento en cuya organización se encuentre integrado (en este supuesto el Ministerio Fiscal), quedando fuera de las facultades y competencias del DPD informar o asesorar a cualquier otro responsable de tratamiento, en este caso una asociación de fiscales, dado que estas gozan de personalidad jurídica propia y disponen de capacidad para determinar los fines y los medios de tratamiento (art. 54.1 EOMF y 4.7 RGPD).

8.2.2.5 *Consulta planteada por la Fiscal de Sala de la Unidad Especializada de Violencia sobre la Mujer en relación con la planteada por la responsable del Área contra la Violencia de Género (VioGén) del Ministerio del Interior; respecto a la posibilidad de que la Policía Judicial pudiera trasladar a las víctimas denunciantes información relativa a los antecedentes por violencia de género del agresor*

Con la finalidad de asistir a la Excma. Sra. Fiscal de Sala se señaló lo siguiente:

La Directiva (UE) 2016/680 *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*, dispone que «los datos personales deben recogerse con fines determinados, explícitos y legítimos dentro del ámbito de aplicación de la presente Directiva y no deben ser tratados para fines incompatibles con los fines de la prevención, la investigación, la detección o el enjuiciamiento de infracciones penales o la ejecución de sanciones penales, incluidas la protección y la prevención frente a las amenazas para la seguridad pública. Si el mismo u otro responsable del tratamiento trata datos personales con alguno de los fines previstos en el ámbito de aplicación de la presente Directiva distinto del fin para el que los datos fueron recopilados, dicho tratamiento debe permitirse con la condición de que el mismo esté autorizado con arreglo a la legislación aplicable y sea necesario y proporcionado para dicho otro fin» (Considerando 29).

El art. 11.1 de la LO 7/2021 establece que el tratamiento sólo será lícito en la medida en que sea necesario para los fines señalados en el artículo 1 y se realice por una autoridad competente en ejercicio de

sus funciones, y entre los fines señalados, incluye el de prevención de infracciones penales.

Por otro lado, el principio de minimización exige que, en cada caso, el tratamiento sea adecuado, pertinente y no excesivo en relación a la finalidad para la que son tratados [art. 6.1 a) LO 7/2021].

De igual modo, el RGPD dispone que «el tratamiento de datos personales debe estar concebido para servir a la humanidad. El derecho a la protección de los datos personales no es un derecho absoluto, sino que debe considerarse en relación con su función en la sociedad y mantener el equilibrio con otros derechos fundamentales, con arreglo al principio de proporcionalidad» (Considerando 4).

En virtud de todo ello y aplicando el conjunto de la normativa expuesta a la cuestión objeto de consulta la misma conduce a la exigencia de valorar si, en la operación de tratamiento consistente en comunicar a la víctima información sobre la existencia de antecedentes por violencia de su agresor, se cumple el principio de proporcionalidad manifestado en la normativa de protección de datos a través del principio de minimización.

Según la doctrina del Tribunal Constitucional, siguiendo la sentada por el Tribunal Europeo de Derechos Humanos, el citado principio exige la superación de un triple juicio, en el sentido de determinar si la medida adoptada 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), es decir, si la injerencia producida en el titular del derecho objeto de restricción por la medida es la mínima en aras al logro del fin legítimo perseguido con aquélla (entre otras, STC 26/1981, STC 178/1985 y STC 207/1996).

Se consideró que la transmisión de la información a la víctima en los términos que se plantea la consulta no puede llevarse a cabo de manera automática y/o generalizada, y que únicamente debiera realizarse una vez se concluya, tras el examen y valoración de las circunstancias particulares de cada caso, no solo que los referidos antecedentes suponen un factor de riesgo relevante, sino que comunicar esa concreta información a la víctima resulta necesario para prevenir, en ese supuesto concreto, la comisión de una infracción penal mediante la adopción de medidas adecuadas de protección o autoprotección.

Los criterios recogidos en dicho informe fueron acogidos tanto por la Fiscal de Sala de la Unidad Especializada de Violencia sobre la Mujer como en la posterior Instrucción 1/2023 de la Secretaría de Estado de Seguridad, *por la que desarrolla la obligación de comunicación a la víctima de los antecedentes del agresor en los denominados casos de «agresores persistentes» y otras medidas de protección y seguridad en los casos de violencia de género.*

8.2.3 RECLAMACIONES POR ACTUACIONES DEL MINISTERIO FISCAL

8.2.3.1 *Se incoó expediente gubernativo por la recepción de una comunicación de un ciudadano que decía ejercitar el derecho de oposición frente al tratamiento de sus datos personales por la página web del Ministerio Fiscal <https://www.fiscal.es> al entender que infringía la correcta interpretación del consentimiento del interesado realizada por el Comité Europeo de Protección de Datos, al asumir dicho consentimiento por la mera navegación en la página web sin que se exigiese ninguna acción del interesado. Dicho ciudadano también formuló, por los mismos motivos, una reclamación ante la AEPD*

Por el DPD se acusó recibo de dicha comunicación y se le informó que se había procedido a trasladar su petición a la Unidad de Apoyo de la Fiscalía General del Estado al ser esta la unidad a través de la cual el Ministerio Fiscal, como responsable del tratamiento, daría respuesta a su solicitud, lo cual efectivamente se materializó con posterioridad.

Por el Delegado de Protección de Datos se realizaron actuaciones con el objeto de examinar la adecuación a la normativa de protección de datos de la información que se suministra en el portal *fiscal.es* en el apartado «Política de Cookies» de la subpágina «Aviso Legal», tras lo cual se solicitó a la Unidad de Apoyo que interesara de la administración prestacional que concretase la naturaleza de las *cookies* utilizadas en el portal *fiscal.es*. Se trataba de conocer si las mismas (o alguna de ellas) ya sean propias o de terceros, exigían el consentimiento de los usuarios y en caso de que así fuera, se habilitasen a la mayor brevedad, los medios para corregir dicha carencia de modo que el consentimiento se pudiera manifestar previamente al acceso al portal *fiscal.es*, de modo libre, específico, informado e inequívoco mediante una declaración o una clara acción afirmativa, así también para que la administración prestacional actualizara el contenido del apartado

«política de cookies» de modo que fuera conforme con las cookies efectivamente utilizadas y con la finalidad de las mismas.

Por otro lado, se puso de relieve, en respuesta remitida a la AEPD:

– Que la Unidad de Apoyo de la Fiscalía General del Estado respondió a la solicitud del ejercicio del derecho de oposición.

– Que el dominio *fiscal.es* es de la titularidad del Ministerio de Justicia –como expresamente se informa en la subpágina que contiene el «Aviso legal» (<https://www.fiscal.es/web/fiscal/aviso-legal>)– como prestador de servicios al Ministerio Fiscal, el cual en lo que respecta a dicho portal, únicamente es generador de su contenido y por tanto ajeno a su soporte tecnológico, siendo un usuario del servicio que le presta el Ministerio de Justicia.

Es por esta razón el Ministerio de Justicia el responsable del tratamiento de los datos personales obtenidos como consecuencia del acceso al dominio *fiscal.es* y, en consecuencia, el facultado para atender las solicitudes de ejercicio de derechos por parte de los interesados.

– Que el Ministerio Fiscal, en el marco de sus competencias, desde el instante que conoció las circunstancias que dieron lugar al ejercicio del derecho de oposición, aplicó todas las medidas técnicas y organizativas que estaban a su alcance al reclamar de la administración competente el cumplimiento de sus obligaciones (art. 236 sexies 2 LOPJ e Instrucción FGE 2/2019), para que estas se realizasen de acuerdo con la vigente normativa de protección de datos, e instó a que se llevasen a cabo diversas actuaciones, sin perjuicio de cualesquiera otras que se estimasen oportunas.

Por la AEPD se dictó Resolución desestimando la reclamación formulada, decisión contra la que se formuló recurso de reposición cuya resolución en la presente fecha no ha sido notificada.

8.2.3.2 *Se abrió expediente gubernativo a raíz de la recepción de una comunicación de la AEPD en la que un ciudadano reclamaba por la difusión a los medios de comunicación de sus datos personales por una Fiscalía.*

En el curso de las actuaciones se pudo constatar que la portavocía, a la vista del interés público del escrito de calificación, al referirse a un asunto de larga instrucción en el que figuraban como investigadas personas que habían ostentado cargos públicos, transcurrido un tiempo que consideró suficiente para que el juzgado por medio de *LexNet*

hubiese notificado dicho escrito a las partes afectadas procedió a remitir dicho escrito de conclusiones provisionales a diversos medios de comunicación, incluida la oficina de prensa del gabinete de comunicación del Tribunal Superior de Justicia correspondiente.

La portavocía, tras advertir, escaso tiempo después, que no figuraban disociados determinados datos personales, se puso en contacto con los referidos medios a fin de que no difundiesen otros datos personales distintos a los nombres de las personas con relevancia pública. De igual modo, una vez constatado que la noticia sobre el escrito de acusación había podido llegar a conocimiento de los implicados a través de los medios de comunicación antes que por la vía judicial, procedió a emitir, con posterioridad, dos comunicados de disculpa.

En relación a esta cuestión en la respuesta dirigida a la AEPD se señaló que la Secretaría Técnica de la Fiscalía General del Estado, el 6 de octubre de 2021, siguiendo las directrices sugeridas por el DPD, difundió a todos los órganos, unidades y fiscalías del Ministerio Fiscal el documento «Implementación de las recomendaciones del Delegado de Protección de Datos del Ministerio Fiscal en materia de comunicación», de lo que se infiere que el Ministerio Fiscal, como responsable (Instrucción FGE 2/2019), ha aplicado medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el RGPD (*ex art. 5.2*) procurando, de ese modo, conciliar el derecho de protección de datos personales con la facultad/deber de información a la opinión pública (art. 4.5 Estatuto Orgánico del Ministerio Fiscal).

De igual modo se trasladó que por el DPD se iniciaron actuaciones con el fin de instar al órgano competente de la Fiscalía General del Estado para que reclamara a la administración prestacional, una herramienta informática que auxiliase al Ministerio Fiscal en la tarea de anonimizar/seudonimizar los escritos y dictámenes que vayan a ser objeto de comunicación pública (o de difusión con finalidad distinta a la jurisdiccional) aquellos datos personales que no deban ser divulgados; aplicación informática que no se empleará para sustituir la valoración y el juicio de ponderación personal que, caso a caso, habrá de llevarse a cabo respecto de los derechos e intereses en juego.

Como medidas adicionales para evitar que pudiera reproducirse un hecho como el referido, por el DPD se recordó a la correspondiente Fiscalía el debido cumplimiento de sus obligaciones en materia de protección de datos personales en su relación con los medios de comunicación, por lo que se han reforzado en dicha Fiscalía los mecanismos de control de su portavocía.

Finalmente, se argumentó ante la AEPD que dicha autoridad de control carecía de competencia y ello en base a lo resuelto por el TJUE, en su Sentencia de 24 de marzo de 2022 en el asunto C-245/20. Dicha resolución, a la vista de que el artículo 55.3 RGPD establece que quedan fuera de la competencia de dicha autoridad de control las operaciones de tratamiento efectuadas por los tribunales en el ejercicio de su función judicial y de que el Considerando 20, a cuya luz debe leerse el referido artículo, precisa que ha de poder encomendarse el control de las operaciones de tratamiento efectuadas por los tribunales y otras autoridades judiciales «en ejercicio de su función judicial» a organismos específicos establecidos dentro del sistema judicial del Estado miembro de que se trate y no a la autoridad de control de ese Estado miembro, con la finalidad de «preservar la independencia del poder judicial en el desempeño de sus funciones incluida la toma de decisiones», concluye que la puesta a disposición de periodistas de documentos extraídos de un procedimiento judicial que contienen datos personales con el fin de permitirles informar mejor del desarrollo de ese procedimiento supone un tratamiento de datos con finalidad jurisdiccional por lo que al estar comprendido en el ejercicio de dicha función esa actuación queda fuera de la competencia de la autoridad de control del Estado miembro.

Por la AEPD se dictó Resolución en la que desestima la reclamación formulada y acoge los argumentos expuestos, por lo que asume así la condición de autoridad judicial del Ministerio Fiscal desde la perspectiva de la normativa de protección de datos lo cual, por otro lado, ha sido reconocido en la Ley Orgánica 7/2021 mediante las modificaciones de la LOPJ y del EOMF.

8.2.3.3 *Se procedió a iniciar un expediente gubernativo a raíz de la recepción de una queja formulada por una ciudadana por el hecho de que en la notificación de desistimiento de incoación de expediente de menores dictado en unas diligencias preliminares de la sección de menores de una fiscalía provincial, se indicó el nombre y el domicilio del menor denunciado, lo que llevó a inferir a la reclamante, como madre del menor denunciante, que los datos personales de su hijo (nombre, fecha de nacimiento y dirección postal) hubieran podido también ser comunicados al menor denunciado*

Por el DPD se interesó la remisión de informe pormenorizado sobre lo acontecido, así como, en su caso, sobre las medidas correcto-

ras adoptadas, a raíz de lo cual la Fiscalía manifestó que efectivamente en el decreto de archivo por desistimiento figuran los datos de ambas partes, siendo el modelo que constaba en la aplicación por defecto, y que por error se notificó sin previamente eliminar los datos de las partes, y se señalaba que era la primera vez que sucedía algo semejante y que se había procedido a dictar nota de servicio dirigida a fiscales y funcionarios con el fin de evitar que volviera a suceder.

Ante las explicaciones facilitadas por la Fiscalía provincial a la reclamante, la misma remitió correo electrónico al DPD desistiendo de su reclamación.

No obstante, se recordó a la Fiscalía provincial la vigencia de la Nota Interna emitida por el DPD relativa a la implementación del principio de minimización en las actuaciones del Ministerio Fiscal y cláusula de protección de datos en notificaciones de decretos dictados por el Ministerio Fiscal, difundida en mayo de 2021 y de igual modo, a la vista del contenido de los hechos denunciados y de la información remitida por la Fiscalía provincial, la cual puso de manifiesto hechos relativos al funcionamiento del Ministerio Fiscal cuya supervisión corresponde a la Inspección Fiscal, se acordó remitir, a los efectos oportunos, testimonio de lo actuado a dicho órgano.

8.2.3.4 *Se incoó expediente gubernativo por la recepción de una comunicación en la que un miembro de la carrera fiscal reprocha la utilización por la Inspección Fiscal del dato relativo a su domicilio actual –el cual ella misma había facilitado previamente a dicha Unidad con otros fines– para la notificación de la incoación de unas diligencias informativas alegando que no había prestado el consentimiento para ello*

En la respuesta se puso de manifiesto lo siguiente:

La normativa nacional (art. 13.2 EOMF y art. 159 del RMF entonces vigente) dispone que la Inspección Fiscal de la Fiscalía General del Estado ejerce con carácter permanente sus funciones por delegación del Fiscal General del Estado, correspondiéndole el conocimiento sobre la regularidad del funcionamiento del Ministerio Fiscal, sobre las prácticas generales que se siguen en las fiscalías para el despacho y curso de los asuntos en que deba intervenir el Ministerio Fiscal, sobre el conocimiento de las condiciones, aptitudes y conducta de los funcionarios fiscales así como el examen de las quejas que se produzcan sobre el modo de proceder los/as fiscales.

Citadas competencias conllevan, ineludiblemente, el tratamiento por el Ministerio Fiscal de datos personales de los/as fiscales como consecuencia necesaria de la relación que se genera entre la Institución y los miembros que la componen en base a propósitos, específicos, explícitos, legítimos, estrechamente vinculados entre sí y que resultan imprescindibles para el cumplimiento de las misiones y funciones que la Institución tiene constitucional, legal y estatutariamente encomendadas, así como para poder atender y satisfacer los derechos de los/as fiscales como empleados públicos y, de ser preciso, para demandar el correcto cumplimiento de los deberes derivados de esa condición tal como lo exige el Estatuto Orgánico del Ministerio Fiscal.

En este aspecto, las finalidades, base jurídica y categoría de datos personales antes referidas explícitamente se contemplan en el RAT publicado en el portal web fiscal.es en relación con propósitos íntimamente relacionados entre sí y con el estatuto jurídico de los fiscales como son la tramitación de expedientes gubernativos, la gestión administrativa y económica de la plantilla, la supervisión de la regularidad en el funcionamiento del Ministerio Fiscal y las actuaciones de naturaleza disciplinaria.

En consecuencia, el tratamiento que realiza el Ministerio Fiscal de categorías de datos personales de la plantilla de fiscales tales como: nombre y apellidos, documento de identidad, teléfono, dirección electrónica y/o postal, así como, en su caso, determinadas categorías especiales de datos (p.ej. los relativos a la salud), además de atender al principio de minimización en el sentido de que son adecuados, pertinentes y limitados en lo necesario en relación con los fines para los que son tratados [art. 5.1 c) RGPD], encuentra su fundamento en propósitos legítimos íntimamente ligados entre sí, derivados todos ellos del cumplimiento de una obligación legal y de funciones realizadas en el interés público o en el ejercicio de poderes públicos por parte del Ministerio Fiscal en relación con el estatuto jurídico de los fiscales [art. 6.1 c) y e)].

A mayor abundamiento, la normativa de protección de datos permite también el tratamiento de datos personales con fines distintos de aquellos para los que hayan sido inicialmente recogidos cuando sea compatible con los fines de su recogida inicial, en cuyo supuesto no se requiere una base jurídica aparte, distinta de la que legitimó la obtención de los datos personales. Así, cuando el tratamiento para otro fin distinto de aquel para el que se recogieron los datos personales no esté basado en el consentimiento del interesado cabrá ese tratamiento ulterior cuando sea una medida necesaria y proporcionada en una sociedad democrática para salvaguardar determinados e importantes

intereses, entre otros, funciones de supervisión, inspección o reglamentación vinculada, incluso ocasionalmente, con el ejercicio de la autoridad pública (Dictamen 03/2013 del GT 29, Considerando 50 y arts. 6.4 y 23 RGPD).

El hecho de utilizar el dato de la dirección postal que se facilitó para obtener una licencia con el fin de materializar la notificación de la incoación de unas diligencias informativas –teniendo en cuenta, además, la inexactitud del dato relativo a su domicilio obrante en el expediente personal de la Fiscalía y de los impedimentos para la notificación electrónica– constituyó una medida idónea, necesaria y proporcionada vistas las exigencias impuestas, tanto por la norma como por la doctrina del Tribunal Constitucional, para llevar a cabo una efectiva notificación que garantizase el derecho a ser oído y evitar el perjuicio que una publicación edictal podría provocar. En consecuencia, dicha operación de tratamiento también fue acorde con el principio de minimización, así como con el principio de exactitud [art. 5.1 c) y d) RGPD].

En base a lo expuesto, por el DPD se consideró que el tratamiento consistente en la utilización por la Inspección Fiscal del dato relativo a la dirección postal actual para la notificación de la incoación de unas diligencias informativas no constituyó una actuación contraria a la normativa de protección de datos personales.

8.2.3.5 *Se procedió a abrir expediente gubernativo por la recepción de una queja en relación al proceder de la sección de menores de una fiscalía provincial al considerar el reclamante que al ser llamado a declarar su hijo menor de edad por su nombre y apellidos como testigo se había vulnerado la normativa de protección de datos respecto del mismo, así como de otros menores presentes que también se encontraban en la zona de espera compartida con el Juzgado de Menores*

En este caso se realizaron, entre otras, las siguientes consideraciones:

El tratamiento derivado de la aplicación de la Ley Orgánica 5/2000, de 12 de enero, *reguladora de la responsabilidad penal de los menores*, tiene una finalidad jurisdiccional (art. 236 bis 1 LOPJ).

El art. 681. 3 de la Ley de Enjuiciamiento Criminal, de aplicación supletoria en virtud de lo dispuesto en la Disposición Final Primera Ley Orgánica 5/2000, prohíbe la divulgación o publicación de infor-

mación relativa a la identidad de víctimas menores de edad y de datos que puedan facilitar su identificación de forma directa o indirecta.

La Ley Orgánica 5/2000, de 12 de enero, *reguladora de la responsabilidad penal de los menores*, respecto de los derechos de las víctimas y de las personas perjudicadas dispone que el Ministerio Fiscal velará en todo momento por la protección de los derechos de las víctimas y de las personas perjudicadas por las infracciones cometidas por las personas menores de edad (art. 4).

A su vez, según la Directiva 2016/680 *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*, los riesgos para los derechos y libertades de los interesados, de diversa probabilidad y gravedad, pueden producirse, entre otras situaciones, cuando se traten datos personales de personas físicas vulnerables, en particular los niños; o debido a un tratamiento de datos capaz de provocar daños físicos, materiales o inmateriales, o puedan dar lugar a problemas de discriminación, pérdidas económicas, o menoscabo de la reputación (Considerando 51).

Por otro lado, corresponde a la Administración competente la obligación de suministrar los medios tecnológicos adecuados para que se proceda al tratamiento de los datos personales conforme a las disposiciones legales y reglamentarias. La Administración competente deberá cumplir con las responsabilidades que en materia de tratamiento y protección de datos personales se le atribuya como administración prestacional debiendo adoptarse las medidas organizativas adecuadas para que la Oficina judicial y fiscal realice un adecuado tratamiento de los datos personales (art. 236 sexies 1, 2 y 3).

El Ministerio Fiscal, por tanto, ha de tratar los datos personales de manera que se procure una seguridad adecuada, incluida la confidencialidad, lo que conlleva la adopción, dentro del marco de sus competencias, de aquellas medidas técnicas y organizativas que estén a su alcance para garantizar la misma (art. 6 LO 7/2021 y Considerando 60 Directiva 2016/680).

En esta línea, la Instrucción FGE 2/2019 si bien señala que el Ministerio Fiscal es el responsable del tratamiento de datos personales que realiza en el ejercicio de sus funciones, lo es exclusivamente dentro del marco de sus competencias y facultades, y le corresponde promover ante las administraciones prestacionales, la implementación de las medidas técnicas precisas para la protección de datos personales

desde el diseño y por defecto, tanto en el momento de determinar los medios de tratamiento como durante el propio tratamiento.

En virtud de ello por el DPD se interesó a la Fiscalía provincial la adopción de las medidas correctoras oportunas, por quien se iniciaron las gestiones tanto para reclamar a la administración prestacional competente aquellos medios técnicos adecuados con el fin de que los llamamientos de las personas citadas se pudieran realizar de manera anonimizada, como para que se dictaran instrucciones a fin de evitar los llamamientos de los comparecientes por medio de su nombre y apellidos en tanto no se dotase de dichos medios a la sección de menores.

8.2.4 OTRAS ACTUACIONES

8.2.4.1 *El DPD en el ejercicio de sus funciones de supervisión pudo constatar la ausencia en la Fiscalía General del Estado de una agenda de direcciones completa y actualizada de la totalidad de los correos electrónicos genéricos institucionales de las jefaturas de las fiscalías, unidades y órganos que componen el Ministerio Fiscal*

Ha observado que, dicha agenda se completaba con direcciones oficiales personales del o la fiscal jefe y/o de funcionarios/as que, o bien se encuentran al frente de la correspondiente secretaría o de aquellos encargados de hacer llegar los correos electrónicos a los/las fiscales jefes. Esta situación podía dar lugar a la comunicación de datos personales y/o información de naturaleza reservada a un destinatario distinto de aquel al que se deseaba enviar y ello como consecuencia de un cambio o cese no comunicado en los referidos puestos.

Con el fin de asegurar la correcta transmisión de información y evitar posibles incidentes de seguridad, se sugirió a la Unidad de Apoyo de la Fiscalía General del Estado que:

- Procediera a confeccionar una agenda actualizada de direcciones de correos electrónicos institucionales genéricos de todas las fiscalías, órganos y unidades que componen el Ministerio Fiscal.

- Instase a las jefaturas de las distintas fiscalías, órganos y unidades a que garanticen que las correspondientes direcciones estén activas y gestionadas, siempre que sea factible, por más de una persona con el fin de asegurar, de ese modo, que estén permanente y debidamente atendidas.

– Difundiese dicha agenda de direcciones a todas las fiscalías, órganos y unidades que componen el Ministerio Fiscal instando a su uso en las comunicaciones ordinarias entre las distintas jefaturas de las fiscalías, órganos y unidades, y ello sin perjuicio de la utilización de direcciones de correos institucionales personales cuando existan concretas o especiales circunstancias que así lo exijan.

8.2.4.2 *El DPD participó en el apartado correspondiente al derecho a la protección de datos personales de la Circular 2/2022, de 20 de diciembre, sobre la actividad extraprocesal del Ministerio Fiscal en el ámbito de la investigación penal*

8.2.4.3 *Por el DPD se iniciaron actuaciones con el fin de que por medio de la Unidad de Apoyo se desarrollase un programa informático para el registro, tramitación y resolución de los expedientes del DPD*

8.2.4.4 *Se solicitó a la FGE que se realizaran las actuaciones pertinentes para que por parte de la administración prestacional (ex art. 236 sexies 1 LOPJ), se proporcionara una herramienta informática que auxiliase a los/as fiscales en la tarea de anonimizar, de los escritos y dictámenes que vayan a ser objeto de comunicación pública, aquellos datos personales que no deban ser divulgados*

Se subrayó que la referida aplicación informática no podría emplearse para sustituir la valoración y el juicio de ponderación personal a la hora de conciliar la facultad/deber de información con el derecho a la protección de datos personales que, caso a caso, habrá de llevarse a cabo por los/as fiscales.

La Dirección General de Transformación Digital procedió, en el mes de agosto, a la incorporación de dicha herramienta en el Escritorio Integrado, la cual, no obstante, todavía es susceptible de ciertas mejoras.

8.2.4.5 *El DPD ha constado que los documentos firmados electrónicamente por los/as fiscales, una vez impresos –así como aquellos que son remitidos a través de la plataforma GEI-SER–, no pueden ser identificados como auténticos y son susceptibles de ser alterados*

Lo que implica un riesgo para las personas físicas en lo que se refiere al tratamiento de sus datos personales, instó a la Unidad de Apoyo como órgano competente, a fin de que procediera a llevar a cabo las actuaciones pertinentes para la implementación, en el plazo más breve posible, del sistema de Código Seguro de Verificación (CSV) para los documentos firmados electrónicamente por el Ministerio Fiscal.

8.2.4.6 *El DPD comprobó que en un número importante de los documentos firmados electrónicamente por los/las fiscales, se revela en el panel de firma (apartado que contiene los detalles de la firma digital) el número del Documento Nacional de Identidad (DNI) del fiscal firmante*

Lo cual se debe a que gran parte de las tarjetas de identificación electrónica no tienen incorporado un segundo certificado digital identificador del/la fiscal como miembro de la Carrera Fiscal. Por este motivo se interesó a la Unidad de Apoyo para que procediera a llevar a cabo las actuaciones oportunas para que fuera corregida la situación expuesta, de modo que toda la plantilla del Ministerio Fiscal disponga de certificado de firma digital correspondiente a la Carrera Fiscal, así como para recordar a todos/as que las firmas electrónicas de los documentos elaborados en el ejercicio de sus funciones deberán llevarse a cabo, únicamente, con el referido certificado digital para evitar que en los documentos firmados digitalmente aparezcan los números de DNI.

8.2.4.7 *Tras conocer que por medio de la aplicación del Sistema de registros administrativos de apoyo a la Administración de Justicia (SIRAJ) utilizada para la obtención de certificaciones de antecedentes penales se había producido, en algunos casos, el acceso a los antecedentes de esa persona cuando era menor de edad y que dicha circunstancia, podría suponer una infracción de la normativa de protección en lo que se refiere a los principios de minimización, de confidencialidad y, en su caso de limitación del plazo de conservación (art. 6 LO 7/2021), se sugirió a la Unidad de Apoyo que adoptase, en el marco de sus competencias, las medidas correctoras oportunas y procediera a informar sobre las mismas.*

8.2.4.8 *Solicitud de colaboración a la Inspección Fiscal así como de las fiscalías de las Comunidades Autónomas*

Se interesa dicha colaboración hasta en tanto no se cuente con una mayor dotación de medios personales y materiales que permitan llevar a cabo directa y periódicamente actuaciones de supervisión al PDP en las distintas fiscalías, órganos y unidades del Ministerio Fiscal, y se concreta en que con ocasión de las visitas de inspección efectuadas por aquellos órganos efectuadas, procedieran a recabar y posteriormente remitir copia de la documentación del expediente o expedientes gubernativos en el que se consignen las actuaciones realizadas para la implementación de la normativa de protección de datos (apartado 7.3 a) Instrucción 2/2019), así como las Notas de Servicio emitidas por las respectivas jefatura en dicha materia.

Una vez recibida dicha documentación, por el DPD se da traslado de la misma a los adjuntos territoriales al DPD para que, en el ejercicio de las funciones encomendadas, procedan como estimen conveniente con el fin de recabar información adicional a la correspondiente fiscalía sobre el debido cumplimiento de la Instrucción 2/2019, de la *Guía Básica de actuaciones en materia de protección de datos* y del resto de recomendaciones impartidas en esta materia, y en su caso realizar informe señalando las deficiencias detectadas y las oportunas sugerencias con el fin de que estas sean subsanadas.

En el curso de 2022, se han llevado a cabo dichas actuaciones respecto de las fiscalías de las comunidades autónomas de La Rioja y Navarra y de las fiscalías provinciales de Álava, Valladolid, Toledo, Málaga, Zamora, León, Guadalajara, Granada y Segovia.

8.2.4.9 *Por el DPD se participó en el Encuentro de delegados de protección de datos de la AGE, Órganos Constitucionales y Órganos de Relevancia Constitucional, que tuvo lugar en la sede de la AEPD en el mes de septiembre*

En dicho encuentro se trataron varios asuntos poniéndose de relieve la importancia del papel de los DPD en el actual marco normativo para su efectivo cumplimiento, se intercambiaron opiniones, así como buenas prácticas.

8.2.4.10 *En el ámbito de las funciones de concienciación y formación [ex art. 39.1 b)] el DDP participó en distintas actividades, así, entre otras:*

– Curso de Formación Inicial de la LX Promoción de la Carrera Fiscal.

- Reunión de Fiscales Superiores celebrada en el Pazo de Mariñán en la cual se impartió la ponencia «¿En qué consiste el derecho a la protección de datos?».
- En el curso organizado por CGPJ «Retos, perspectivas y tendencias de la protección de datos» se presentó la ponencia «La función de supervisión de las autoridades de protección de datos».
- En el curso «La protección del derecho al honor y a la propia imagen en el ámbito digital» organizado por el CEJ se impartió la ponencia «El derecho a la protección de datos y el Ministerio Fiscal».

8.2.5 ACTIVIDAD DE LOS ADJUNTOS TERRITORIALES AL DELEGADO DE PROTECCIÓN DE DATOS

La actividad de los adjuntos territoriales en el año 2022 ha venido marcada fundamentalmente, por la implementación en las fiscalías de la mencionada Guía Básica de actuaciones a desarrollar por las fiscalías, órganos y unidades del Ministerio Fiscal en materia de protección de datos.

Entre otras actuaciones de los distintos adjuntos al DPD cabe señalar las siguientes:

Por el adjunto en la Comunidad Autónoma de Andalucía se pone de relieve su participación en la resolución de diversas consultas; en la actualización de los manuales de organización; de puestos y de procedimientos de la oficina fiscal en los que se incluyeron recordatorios y recomendaciones en materia de protección de datos; en la elaboración de diversos convenios entre los que destaca el relativo al intercambio de información necesaria para el ejercicio de las competencias y de las obligaciones en materia de protección de menores, el de mediación penal en el ámbito provincial de Huelva y el de gestión de ruedas de reconocimiento en la demarcación de Córdoba.

Por el adjunto de Andalucía se hacen dos propuestas. Por un lado que por el órgano competente de la Fiscalía General del Estado se incluya en el baremo de productividad la actividad que realizan los adjuntos en materia de protección de datos y, por otro lado y con el fin de que los convenios formativos entre el Ministerio Fiscal y las distintas universidades se rijan por criterios semejantes, se elabore por la Unidad de Apoyo un modelo de convenio que contenga cláusulas uniformes para todos los acuerdos de esta naturaleza.

Por el adjunto en la Comunidad Autónoma de Canarias se subraya, la resolución de una consulta en relación con el modelo de impreso de prestación de consentimiento de las víctimas de delitos para que sus

datos puedan ser comunicados la Oficina Virtual de Protección de Víctimas de la dicha comunidad autónoma.

Por el de Extremadura se señala, su intervención resolviendo la consulta relativa a la legitimidad de la comunicación a la clínica médico forense de datos personales con ocasión de la tramitación de unas diligencias preprocesales. Añade que, con ocasión del examen de escritos de calificación constató en ocasiones, la inclusión del domicilio de testigos en determinadas fiscalías, lo que indicó para su corrección a las correspondientes jefaturas.

8.2.6 INFORME AL FISCAL GENERAL DEL ESTADO

El año 2022 culminó con la reunión del DPD con el Excmo. Sr. Fiscal General del Estado en la que, en cumplimiento de lo establecido en el artículo 38.3 RGPD y apartado 7.2 de la Instrucción FGE 2/2019, se informó sobre el grado de implementación de la normativa de protección de datos en el ámbito del Ministerio Fiscal y de las actuaciones del DPD en este ámbito y de la cual esta Memoria es fiel reflejo.

En dicha reunión, el DPD trasladó su criterio en relación con la actual estructura organizativa de la unidad del DPD que se recoge en la Instrucción FGE 2/2019 en lo que a los adjuntos territoriales se refiere, que se considera poco eficaz y operativa. Por ello se sugirió su reforma una vez se materialice la modificación del EOMF en relación a la Unidad de Protección de Datos –que actualmente sigue en trámite parlamentario– y se lleve a cabo el correspondiente desarrollo reglamentario.

La actual organización de la unidad del DPD, que pretendió asemejarse a las redes territoriales de las unidades especializadas, no satisface las exigencias que impone la normativa de la protección de datos respecto de las funciones del DPD del Ministerio Fiscal, ni tampoco respecto de aquellas atribuidas a la Unidad de Protección de Datos ya que todas ellas se podrían equiparar, salvando las distancias, a las que ejerce la Inspección Fiscal en su misión de supervisión y, a su vez, a las de la Secretaría Técnica en la labor de asesoramiento.

La nueva estructura que se propone pretende reforzar con los medios personales y materiales precisos al órgano central de la Unidad de Protección de Datos integrado en la Fiscalía General del Estado para que pueda ejercer sus funciones con independencia y atendiendo al principio de unidad de actuación.

Dado el reconocimiento legal en virtud de la LO 7/2021 de la Unidad de Protección de Datos se trasladó al Fiscal General del Estado la petición de que se arbitrasen los medios a fin de que esta se hiciera efectiva lo más pronto posible una vez que se aprobase la correspondiente reforma legal del EOMF en los términos que se recogieron en la Memoria del pasado año.