

015/2024

La redacción del Proyecto presenta, desde la perspectiva de la normativa reguladora del derecho fundamental a la protección de datos personales, tres cuestiones fundamentales.

La primera, la relativa a la base jurídica que ampararía los tratamientos de datos personales que llevaría a cabo la denominada “Solución Pública de Facturación Electrónica”, gestionada por la Agencia Estatal de Administración Tributaria (AEAT) -arts. 5 y 9- cuando los empresarios o profesionales que así lo elijan decidan utilizar dicha Solución Pública para emitir o recibir facturas.

La segunda, la relativa a la base jurídica que ampararía el tratamiento de datos por la mencionada Solución Pública de Facturación Electrónica consistente en la comunicación obligatoria a esta por todos los empresarios o profesionales que no utilicen dicha Solución Pública para emitir o recibir facturas -es decir, que utilizan para ello una solución privada-, de una copia fiel de cada factura (art. 5.4) en formato Facturae de modo que la Solución Pública, en su función de repositorio de facturas, almacene la información de todas las facturas electrónicas, la de sus copias y la de su pago efectivo completo (Disposición Adicional cuarta, DA 4ª).

En tercer lugar, cuál sería la circunstancia, de entre las relacionadas en el art. 9.2 RGPD, que levantaría la prohibición de tratamiento que contempla el art. 9.1 RGPD, por la citada Solución Pública de Facturación Electrónica de los datos personales de carácter sensible que se pueden incluir en las facturas.

I

En relación con la primera de las cuestiones mencionadas, cabe exponer la jurisprudencia tanto del Tribunal Constitucional como del Tribunal de Justicia de la Unión Europea (TJUE) en cuanto al principio de legalidad en los tratamientos de datos personales.

La sentencia del Tribunal Constitucional (STC) 76/2019, de 22 de mayo, contiene doctrina relevante sobre el derecho fundamental a la protección de datos personales, y aborda tanto las características como el contenido que ha de tener la normativa que pretenda establecer una injerencia en ese derecho fundamental.

*(...) Por mandato expreso de la Constitución, toda injerencia estatal en el ámbito de los derechos fundamentales y las libertades públicas ora incida directamente sobre su desarrollo (artículo 81.1 CE), ora limite o condicione su ejercicio (artículo 53.1 CE), precisa una habilitación legal (por todas, STC 49/1999, de 5 de abril, FJ 4). (...) Esta doble función de la reserva de ley se traduce en una doble exigencia: por un lado, la necesaria intervención de la ley para habilitar la injerencia; y, por otro lado, **esa norma legal** «ha de reunir todas aquellas características indispensables como garantía de la seguridad jurídica», esto es, «**ha de expresar todos y cada uno de los presupuestos y condiciones de la intervención**» (STC 49/1999, FJ 4). En otras palabras, «**no sólo excluye apoderamientos a favor de las normas reglamentarias [...], sino que también implica otras exigencias respecto al contenido de la Ley que establece tales límites**» (STC 292/2000, FJ 15).*

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

La STJUE de 6 de octubre de 2020, en los casos acumulados C-511/18, C-512/18 y C-520/18, La Quadrature du Net y otros, en su apartado 175, recuerda que:

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

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

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

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

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

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

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

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

176 Finalmente, para cumplir el requisito de proporcionalidad según el cual las excepciones a la protección de los datos personales y las limitaciones de esa protección no deben exceder de lo estrictamente necesario, la normativa controvertida que conlleve la injerencia debe establecer reglas claras y precisas que regulen el alcance y la aplicación de la medida en cuestión e impongan unas exigencias mínimas, de modo que las personas cuyos datos se hayan transferido dispongan de garantías suficientes que permitan proteger de manera eficaz sus datos

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

Aún más recientemente, en relación con este principio de legalidad, el TJUE, en sentencia de 21 de marzo de 2024, C-61/22, apartado 77, establece:

a) *Respeto del principio de legalidad*

77 En lo que se refiere al requisito, establecido en el artículo 52, apartado 1, primera frase, de la Carta, de que cualquier limitación del ejercicio de los derechos reconocidos por ella debe ser establecida por la ley, ha de recordarse que este requisito implica que el propio acto que permita la injerencia en dichos derechos debe definir el alcance de la limitación del ejercicio del derecho de que se trate, con la precisión de que, por un lado, este requisito no excluye que la limitación en cuestión se formule en términos lo suficientemente abiertos como para poder adaptarse a supuestos distintos, así como a los cambios de situación, y de que, por otro lado, el Tribunal de Justicia, en su caso, puede precisar, por vía de interpretación, el alcance concreto de la limitación en relación tanto con los propios términos de la normativa de la Unión de que se trate como con su estructura general y los objetivos que persigue, interpretados a la luz de los derechos fundamentales garantizados por la Carta (sentencia de 21 de junio de 2022, Ligue des droits humains, C-817/19, EU:C:2022:491, apartado 114).

Cabe finalizar este apartado con la STC 292/2000, de 30 de noviembre del Tribunal Constitucional, FJ 11.

La primera constatación que debe hacerse, que no por evidente es menos capital, es que la Constitución ha querido que la Ley, y sólo la Ley, pueda fijar los límites a un derecho fundamental. Los derechos fundamentales pueden ceder, desde luego, ante bienes, e incluso intereses constitucionalmente relevantes, siempre que el recorte que experimenten sea necesario para lograr el fin legítimo previsto, proporcionado para alcanzarlo y, en todo caso, sea respetuoso con el contenido esencial del derecho fundamental restringido (SSTC 57/1994, de 28 de febrero, FJ 6; 18/1999, de 22 de febrero, FJ 2).

*Justamente, si la Ley es la única habilitada por la Constitución para fijar los límites a los derechos fundamentales y, en el caso presente, al derecho fundamental a la protección de datos, y esos límites no pueden ser distintos a los constitucionalmente previstos, que para el caso no son otros que los derivados de la coexistencia de este derecho fundamental con otros derechos y bienes jurídicos de rango constitucional, el apoderamiento legal que permita a un Poder Público recoger, almacenar, tratar, usar y, en su caso, ceder datos personales, sólo está justificado si responde a la protección de otros derechos fundamentales o bienes constitucionalmente protegidos. Por tanto, si aquellas operaciones con los datos personales de una persona no se realizan con estricta observancia de las normas que lo regulan, se vulnera el derecho a la protección de datos, pues se le imponen límites constitucionalmente ilegítimos, ya sea a su contenido o al ejercicio del haz de facultades que lo componen. Como lo conculcará también esa Ley limitativa si regula los límites de forma tal que hagan impracticable el derecho fundamental afectado o ineficaz la garantía que la Constitución le otorga. **Y así será cuando la Ley, que debe regular los límites a los derechos fundamentales con escrupuloso respeto a su contenido esencial, se limita a apoderar a otro Poder Público para fijar en cada caso las restricciones que pueden imponerse a los derechos fundamentales, cuya singular determinación y aplicación estará al albur de las decisiones que adopte ese Poder Público, quien podrá decidir, en lo que ahora nos interesa, sobre la obtención, almacenamiento, tratamiento, uso y cesión de datos personales en los casos que estime convenientes y esgrimiendo, incluso, intereses o bienes que no son protegidos con rango constitucional.***

De ser ese el caso, la Ley habrá vulnerado el derecho fundamental en cuestión, ya que no sólo habrá frustrado la función de garantía propia de toda reserva de ley relativa a derechos fundamentales al renunciar a fijar por sí misma esos límites, dado que la reserva de Ley impone al legislador, además de promulgar esa Ley, regular efectivamente en ella la materia objeto de la reserva; sino también al permitir que el derecho fundamental ceda ante intereses o bienes jurídicos de rango infraconstitucional en contra de lo dispuesto en la propia Constitución, que no lo prevé así.

*Por esta razón, **cuando la Constitución no contempla esta posibilidad de que un Poder Público distinto al Legislador fije y aplique los límites de un derecho fundamental** o que esos límites sean distintos a los implícitamente derivados de su coexistencia con los restantes derechos y bienes constitucionalmente protegidos, es irrelevante que la Ley habilitante sujete a los Poderes Públicos en ese cometido a procedimientos y criterios todo lo precisos que se quiera, incluso si la Ley habilitante enumera con detalle los bienes o intereses*

*invocables por los Poderes Públicos en cuestión, o que sus decisiones sean revisables jurisdiccionalmente (que lo son en cualquier caso, con arreglo al art. 106 CE). Esa Ley habrá infringido el derecho fundamental porque no ha cumplido con el mandato contenido en la reserva de ley (arts. 53.1 y 81.1 CE), al haber renunciado a regular la materia que se le ha reservado, remitiendo ese cometido a otro Poder Público, frustrando así una de las garantías capitales de los derechos fundamentales en el Estado democrático y social de Derecho (art. 1.1 CE). **La fijación de los límites de un derecho fundamental, así lo hemos venido a decir en otras ocasiones, no es un lugar idóneo para la colaboración entre la Ley y las normas infralegales, pues esta posibilidad de colaboración debe quedar reducida a los casos en los que, por exigencias prácticas, las regulaciones infralegales sean las idóneas para fijar aspectos de carácter secundario y auxiliares de la regulación legal del ejercicio de los derechos fundamentales, siempre con sujeción, claro está, a la ley pertinente (SSTC 83/1984, de 24 de julio, FJ 4, 137/1986, de 6 de noviembre, FJ 3, 254/1994, de 15 de septiembre, FJ 5).***

Y en el FJ 15:

*De igual modo, respecto al derecho a la protección de datos personales cabe estimar que la legitimidad constitucional de la restricción de este derecho no puede estar basada, por sí sola, en la actividad de la Administración Pública. Ni es suficiente que la Ley apodere a ésta para que precise en cada caso sus límites, limitándose a indicar que deberá hacer tal precisión cuando concorra algún derecho o bien constitucionalmente protegido. **Es el legislador quien debe determinar cuándo concurre ese bien o derecho que justifica la restricción del derecho a la protección de datos personales y en qué circunstancias puede limitarse y, además, es él quien debe hacerlo mediante reglas precisas que hagan previsible al interesado la imposición de tal limitación y sus consecuencias. Pues en otro caso el legislador habría trasladado a la Administración el desempeño de una función que sólo a él compete en materia de derechos fundamentales en virtud de la reserva de Ley del art. 53.1 CE, esto es, establecer claramente el límite y su regulación.***

II

Pues bien, de la lectura del Proyecto de Real Decreto (RD) sometido a Informe, y de la memoria de análisis de impacto normativo (MAIN) aportada, la justificación legal del mismo se contiene en la ley 18/2022, de 28 de septiembre, y en concreto en la modificación que realiza en su art. 12 del art. 2

bis de la Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información. Dicho art. 2 bis dice así:

Artículo 2 bis. Factura electrónica en el sector privado.

A efectos de lo dispuesto en esta ley:

1. Todos los empresarios y profesionales deberán expedir, remitir y recibir facturas electrónicas en sus relaciones comerciales con otros empresarios y profesionales. El destinatario y el emisor de las facturas electrónicas deberán proporcionar información sobre los estados de la factura.

2. Las soluciones tecnológicas y plataformas ofrecidas por empresas proveedoras de servicios de facturación electrónica a los empresarios y profesionales deberán garantizar su interconexión e interoperabilidad gratuitas. De la misma forma, las soluciones y plataformas de facturación electrónica propias de las empresas emisoras y receptoras deberán cumplir los mismos criterios de interconexión e interoperabilidad gratuita con el resto de soluciones de facturación electrónica.

3. Durante un plazo de cuatro años desde la emisión de las facturas electrónicas, los destinatarios podrán solicitar copia de las mismas sin incurrir en costes adicionales.

3 bis. El receptor de la factura no podrá obligar a su emisor a la utilización de una solución, plataforma o proveedor de servicios de facturación electrónica predeterminado.

4. Las empresas prestadoras de los servicios a que alude el artículo 2.2, deberán expedir y remitir facturas electrónicas en sus relaciones con particulares que acepten recibirlas o que las hayan solicitado expresamente. Este deber es independiente del tamaño de su plantilla o de su volumen anual de operaciones.

No obstante, las agencias de viaje, los servicios de transporte y las actividades de comercio al por menor solo están obligadas a emitir facturas electrónicas en los términos previstos en el párrafo anterior cuando la contratación se haya llevado a cabo por medios electrónicos.

5. El Gobierno podrá ampliar el ámbito de aplicación de lo dispuesto en el apartado 4 a empresas o entidades que no presten al público en general servicios de especial trascendencia económica en los casos en que se considere que deban tener una interlocución telemática con sus clientes o usuarios, por la naturaleza de los servicios que prestan, y emitan un número elevado de facturas.

6. Las facturas electrónicas deberán cumplir, en todo caso, lo dispuesto en la normativa específica sobre facturación.

Así mismo, los sistemas y programas informáticos o electrónicos que gestionen los procesos de facturación y conserven las facturas electrónicas deberán respetar los requisitos a los que se refiere el artículo 29.2.j) de la Ley 58/2003, de 17 de diciembre, General Tributaria, y su desarrollo reglamentario.

7. Las empresas prestadoras de servicios a que alude el apartado 4 deberán facilitar acceso a los programas necesarios para que los usuarios puedan leer, copiar, descargar e imprimir la factura electrónica de forma gratuita sin tener que acudir a otras fuentes para proveerse de las aplicaciones necesarias para ello.

Deberán habilitar procedimientos sencillos y gratuitos para que los usuarios puedan revocar el consentimiento dado a la recepción de facturas electrónicas en cualquier momento.

8. El período durante el que el cliente puede consultar sus facturas por medios electrónicos establecido en el artículo 2.1.b) no se altera porque aquel haya resuelto su contrato con la empresa o revocado su consentimiento para recibir facturas electrónicas. Tampoco caduca por esta causa su derecho a acceder a las facturas emitidas con anterioridad.

9. Las empresas que, estando obligadas a ello, no ofrezcan a los usuarios la posibilidad de recibir facturas electrónicas o no permitan el acceso de las personas que han dejado de ser clientes a sus facturas, serán sancionadas con apercibimiento o una multa de hasta 10.000 euros. La sanción se determinará y graduará conforme a los criterios establecidos en el artículo 19.2 de la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza. Idéntica sanción puede imponerse a las empresas que presten servicios al público en general de especial trascendencia económica que no cumplan las demás obligaciones previstas en el artículo 2.1. Es competente para imponer esta sanción la persona titular de la Secretaría de Estado de Digitalización e Inteligencia Artificial.

10. El procedimiento de acreditación de la interconexión y la interoperabilidad de las plataformas se determinará reglamentariamente.

A su vez, la Disposición Final séptima, de nuevo citada por el Proyecto de RD, establece:

Disposición final séptima. Desarrollo reglamentario.

Se habilita al Gobierno para desarrollar reglamentariamente lo previsto en esta ley, en el ámbito de sus competencias.

En particular, en relación con lo dispuesto en el artículo 12 de esta ley, los Ministerios de Asuntos Económicos y Transformación Digital y de Hacienda y Función Pública, en el ámbito de sus competencias, determinarán los requisitos técnicos y de información a incluir en la factura electrónica a efectos de verificar la fecha de pago y obtener los periodos medios de pago, los requisitos de interoperabilidad mínima entre los prestadores de soluciones tecnológicas de facturas electrónicas, y los requisitos de seguridad, control y estandarización de los dispositivos y sistemas informáticos que generen los documentos.

Estos requisitos técnicos deberán tener en cuenta la realidad actual del uso de facturas electrónicas estructuradas basadas en estándares globales de forma que se minimice, en lo posible, el esfuerzo de cumplimiento y adaptación de las empresas que ya usan facturas electrónicas estructuradas basadas en dichos estándares.

El plazo para aprobar estos desarrollos reglamentarios será de seis meses a contar desde la publicación en el BOE de la presente ley.

Este desarrollo se realizará admitiendo como válidas, al menos, la lista de sintaxis contenida en la Decisión de Ejecución (UE) 2017/1870 de la Comisión, de 16 de octubre de 2017, sobre la publicación de la referencia de la norma europea sobre facturación electrónica y la lista de sus sintaxis de conformidad con la Directiva 2014/55/UE del Parlamento Europeo y del Consejo.

Previo a la aprobación del desarrollo reglamentario, el Gobierno abrirá un período de exposición pública del reglamento regulador de la factura electrónica, a efecto de presentación de alegaciones por parte de los interesados.

En definitiva, y como resulta del art. 1 del Proyecto de Real Decreto (PRD), este tiene por objeto el desarrollo del art. 2 bis de la ley 56/2007, en su redacción dada al mismo por el art. 12 de la ley 18/2022, y su contenido fundamental, a los efectos de este informe, consiste en la creación de la denominada “Solución Pública de Facturación Electrónica”, gestionada por la Agencia Estatal de Administración Tributaria (AEAT) -arts. 5 y 9- y la comunicación obligatoria a esta por todos los empresarios o profesionales que no utilicen dicha Solución Pública para emitir o recibir facturas -es decir, que utilizan para ello una solución privada-, de una copia fiel de cada factura (art. 5.4) en formato Facturae de modo que la Solución Pública se convierta en

repositorio de facturas. Se trata, por tanto, de una gestión llevada a cabo por una Administración Pública, que llevará acabo tratamientos de los datos personales que se contengan en las facturas.

En relación con la base jurídica para el tratamiento de los datos personales, de entre las previstas en el art. 6 del RGPD, es la letra e) la que sería aplicable en el presente caso: *[cuando] el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento*. No sería válido el “interés legítimo” de la letra f) (véase inciso final del art. 6.1 RGPD), ni tampoco el consentimiento del interesado (véase Considerando 42 RGPD). El art. 8.2 de la LOPDGDD, a su vez, establece que

El tratamiento de datos personales solo podrá considerarse fundado en el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable, en los términos previstos en el artículo 6.1 e) del Reglamento (UE) 2016/679, cuando derive de una competencia atribuida por una norma con rango de ley

Ahora bien, y como puede observarse, ni el art. 2 bis de la ley 56/2007, en su redacción dada al mismo por el art. 12 de la ley 18/2022, ni la Disposición Final séptima de dicha ley, hacen mención alguna, ni siquiera de manera “abierta”, a la Solución Pública de Facturación Electrónica de manera que pudiera entenderse comprendida en la ley los tratamientos de datos que dicha Solución Pública deberá de llevar a cabo. El art. 2 bis citado hace referencia a la obligación de empresarios y profesionales de expedir, remitir y recibir facturas electrónicas en sus relaciones comerciales con otros empresarios y profesionales, pero no, en modo alguno, a que dichos tratamientos de datos puedan llevarse a cabo por una Solución Pública, integrada, o gestionada, en (por) la Administración Pública. Aun cuando fuera decisión voluntaria de dichos empresarios o profesionales la de expedir, remitir o recibir facturas electrónicas por la mediación de la Solución Pública, se requiere una ley para que dichos tratamientos de datos por la Solución Pública puedan ser considerados como que gozan de una base jurídica que otorgara licitud al tratamiento de datos en que consiste. Y dicha ley no existe, pues la ley 56/2007 (art. 2 bis) no da cobertura a estos tratamientos ya que dicha competencia de la Solución Pública no está “atribuida por una norma con rango de ley” (art. 8.2 LOPDGDD), que además, conforme a la jurisprudencia del TJUE referida, TJUE, establezca *ella misma* [la ley] reglas claras y precisas que regulen el alcance y la aplicación de la medida en cuestión e impongan unas exigencias mínimas, de modo que las personas cuyos datos se hayan transferido dispongan de garantías suficientes.

La segunda cuestión planteada está igualmente relacionada con la anterior, y consiste en cuál sería la base jurídica que permitiría a la Solución Pública de Facturación Electrónica tratar los datos personales que, con carácter obligatorio, han de comunicarse a aquellos empresarios o profesionales que hayan decidido no utilizarla previamente para emitir o recibir facturas.

Pues bien, el art. 8.1 LOPDGDD es igualmente claro, y requiere que la base jurídica para el tratamiento por obligación “legal” (art. 6.1.c) RGPD) esté, precisamente, establecida por una norma con rango de ley formal.

Artículo 8. Tratamiento de datos por obligación legal, interés público o ejercicio de poderes públicos.

1. El tratamiento de datos personales solo podrá considerarse fundado en el cumplimiento de una obligación legal exigible al responsable, en los términos previstos en el artículo 6.1.c) del Reglamento (UE) 2016/679, cuando así lo prevea una norma de Derecho de la Unión Europea o una norma con rango de ley, que podrá determinar las condiciones generales del tratamiento y los tipos de datos objeto del mismo así como las cesiones que procedan como consecuencia del cumplimiento de la obligación legal. Dicha norma podrá igualmente imponer condiciones especiales al tratamiento, tales como la adopción de medidas adicionales de seguridad u otras establecidas en el capítulo IV del Reglamento (UE) 2016/679.

Tal y como se ha expuesto en el epígrafe anterior, de la ley 56/2007 (art. 2 bis), cuyo desarrollo es el Proyecto de RD informado (art. 1 de este último), no resulta ninguna mención a dicha obligación que se impone a los empresarios y profesionales, en términos más o menos amplios, o que recojan las garantías para dichos tratamientos, etc. En definitiva, no parece existir base legal tampoco para estos tratamientos de datos personales.

IV

Por último, y sin perjuicio de lo anterior, los tratamientos de datos previstos por el Proyecto de RD consistirían en el tratamiento por la Solución Pública de Facturación de todos los datos incluidos en las facturas emitidas por los empresarios o profesionales a otros empresarios o profesionales, ya sea de manera directa, mediante la utilización de dicha solución por dichos empresarios o profesionales, ya de manera indirecta mediante la obligatoria remisión a esta de una “copia fiel de cada factura” [en sintaxis *Facturae*] (art. 5.4 Proyecto) de todos los datos de todas las facturas por aquellos empresarios o profesionales que no hubieren utilizado previamente a la Solución Pública

para emitir las, de modo que Solución Pública de Facturación sea un “repositorio universal y obligatorio” de todas las facturas electrónicas (art. 2.c) Proyecto RD).

El contenido de las facturas está regulado en el Reglamento por el que se regulan las obligaciones de facturación, aprobado por Real Decreto 1619/2012, de 30 de noviembre, en concreto en su art. 6, que contiene en la letra f) del apartado 1 “f) *Descripción de las operaciones, consignándose todos los datos necesarios para la determinación de la base imponible del Impuesto, tal y como ésta se define por los artículos 78 y 79 de la Ley del Impuesto, correspondiente a aquéllas y su importe, incluyendo el precio unitario sin Impuesto de dichas operaciones, así como cualquier descuento o rebaja que no esté incluido en dicho precio unitario*”.

Dentro de dichas operaciones la descripción podrá consistir, y muchas veces será así, en descripción de operaciones de personas físicas que pongan de manifiesto datos sensibles (de salud, una factura de un tratamiento médico, o de ideología, etc.). En definitiva, tratamientos posibles de datos de categorías especiales, regulados en el art. 9 RGPD, y que necesitan no sólo de una base jurídica para el tratamiento de dichos datos conforme al art. 6 RGPD, sino además de una circunstancia que conforme al art. 9.2 RGPD levante la prohibición de su tratamiento prevista con carácter general en el art. 9.1 RGPD. Dado que la norma proyectada no contempla siquiera como hipótesis la posibilidad de que estos tratamientos incluyan datos de categorías especiales, tampoco se regula en ella nada relativo a las posibles circunstancias que levantarían la prohibición de su tratamiento (art. 9 RGPD y 9 LOPDGDD).

V

En el ámbito de las categorías especiales de datos personales, como establece el Tribunal Constitucional en su STC76/2019, de 22 de mayo, ya referida ampliamente,

(...)

*el Reglamento general de protección de datos establece las garantías mínimas, comunes o generales para el tratamiento de datos personales que no son especiales. En cambio, **no establece por sí mismo el régimen jurídico aplicable a los tratamientos de datos personales especiales**, ni en el ámbito de los Estados miembros ni para el Derecho de la Unión. Por ende, **tampoco fija las garantías que deben observar los diversos tratamientos posibles de datos sensibles**, adecuadas a los riesgos de diversa probabilidad y gravedad que existan en cada caso; tratamientos y categorías especiales de datos que son, o pueden*

*ser, muy diversos entre sí. El reglamento se limita a contemplar la posibilidad de que el legislador de la Unión Europea o el de los Estados miembros, cada uno en su ámbito de competencias, prevean y regulen tales tratamientos, y a indicar las pautas que deben observar en su regulación. Una de esas pautas es que el Derecho del Estado miembro establezca **«medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado»** [artículo 9.2.g) RGPD] y que «se ofrezcan garantías adecuadas» (considerando 56 RGPD). Es patente que ese establecimiento de medidas adecuadas y específicas solo puede ser expreso. Si la norma interna que regula el tratamiento de datos personales relativos a opiniones políticas no prevé esas garantías adecuadas, sino que, todo lo más, se remite implícitamente a las garantías generales contenidas en el Reglamento general de protección de datos, no puede considerarse que haya llevado a cabo la tarea normativa que aquel le exige.*

En consecuencia, y tal y como exige el Tribunal Constitucional, la norma que establezca unas determinadas injerencias en el derecho fundamental a la protección de datos personales de los interesados de categorías sensibles requiere que dicha norma, en primer lugar, sea una norma con rango de ley, y que, además:

a) especifique el interés público esencial o la causa que justifica el levantamiento de la prohibición de tratamiento que fundamenta la restricción del derecho fundamental (FJ 7 de la STC 76/2019). La ley habrá de explicitar de manera expresa cuál es la causa de entre las previstas en el art. 9.2 RGPD que fundamenta la injerencia al derecho fundamental a la protección de datos personales y ello, el Tribunal Constitucional, con cita de su STC 292/2000, rechaza que dicha identificación de los fines legítimos de la restricción pueda realizarse mediante conceptos genéricos o fórmulas vagas.

b) en segundo lugar, dicha ley habrá de regular pormenorizadamente las injerencias al derecho fundamental estableciendo reglas claras sobre el alcance y contenido de los tratamientos de datos que autoriza. Es decir, habrá de establecer cuáles son los presupuestos y las condiciones del tratamiento de datos personales relativos a las categorías especiales de datos personales que pueden incluirse en dichos registros mediante reglas claras y precisas (STC 76/2019, FJ 7 b)

c) Y, por último, la propia ley habrá de contener las garantías adecuadas frente a la recopilación de datos personales que autoriza. El TC ha sido claro en cuanto a que:

*[/]a previsión de las garantías adecuadas **no puede deferirse a un momento posterior a la regulación legal** del tratamiento de datos personales de que se trate. **Las garantías adecuadas deben estar***

incorporadas a la propia regulación legal del tratamiento, ya sea directamente o por remisión expresa y perfectamente delimitada a fuentes externas que posean el rango normativo adecuado. Solo ese entendimiento es compatible con la doble exigencia que dimana del artículo 53.1 CE (...). Es evidente que, si la norma incluyera una remisión para la integración de la ley con las garantías adecuadas establecidas en normas de rango inferior a la ley, sería considerada como una deslegalización que sacrifica la reserva de ley ex artículo 53.1 CE, y, por este solo motivo, debería ser declarada inconstitucional y nula. (...)

Tampoco sirve que para el establecimiento de dichas garantías adecuadas y específicas se pretenda remitirse al propio RGPD o a la LOPDGDD. En este sentido, hay que resaltar que la calificación como datos de categoría especial implica, necesariamente, la observancia de una especial cautela a la hora de determinar si es posible llevar a cabo un tratamiento de datos de esta naturaleza. No sólo no existe una base legal que permita considerar lícito el tratamiento de datos conforme al art. 6 RGPD y 8 LOPDGDD, sino que tampoco se plantea el Proyecto (aun cuando sin rango legal) que pudieran tratarse datos de dicha naturaleza (de categoría especial) ni por tanto qué circunstancias concurren conforme al art. 9.2 RGPD que pudieran dar lugar al levantamiento de la prohibición de dichos datos personales prevista en el art. 9.1 RGPD. Dicha ley deberá, además especificar el interés público esencial que justifica la restricción del derecho a la protección de datos personales y en qué circunstancias puede limitarse, estableciendo las reglas precisas que hagan previsible al interesado la imposición de tal limitación y sus consecuencias, sin que sea suficiente, a estos efectos, la invocación genérica de un interés público. Y dicha ley deberá establecer, además, las garantías adecuadas de tipo técnico, organizativo y procedimental, que prevengan los riesgos de distinta probabilidad y gravedad y mitiguen sus efectos.

En este sentido, esta AEPD considera, por tanto, que sería muy conveniente que el proyecto (sin perjuicio de los comentarios realizados en los epígrafes II y III de este Informe en cuanto al rango formal de la norma) contuviera un análisis de los riesgos y la evaluación de los impactos de estos (EIPD) en los tratamientos de datos personales, que permitiera no sólo determinar en la norma las medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado, sino establecer del mismo modo las circunstancias esenciales que permiten un tratamiento lícito de dichos datos personales, como recuerdan y requieren las sentencias del TC y del TJUE a que se ha hecho referencia. La MAIN no hace referencia a datos personales, y por tanto no analiza estos riesgos, ni evalúa el impacto de los riesgos que pudieran existir en el derecho fundamental a la protección de datos.

Cabe recordar que el art. 25 RGPD establece la necesidad de la protección de datos “desde el diseño” de los tratamientos, y la necesidad de tener en cuenta los riesgos que se derivan de estos.

Artículo 25

Protección de datos desde el diseño y por defecto

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

Dicho análisis, evaluación de impacto y establecimiento en la norma de las circunstancias que permiten y las medidas adecuadas y específicas que legitiman la incidencia en el derecho fundamental a la protección de datos personales debería de llevarse a cabo con la ayuda del Delegado de Protección de datos correspondiente. Y dicho análisis de riesgos y EIPD habrían de llevarse a cabo incluso en el caso de que la norma que regulase los tratamientos de datos personales tuviera rango de ley.

Esta Agencia viene recomendando repetidamente en sus informes que el prelegislador, en aquellos casos, como el presente, en que los tratamientos puedan tener como base jurídica el art. 6.1.c) o e) del RGPD (esto es, tratamientos cuya base es una obligación legal o una misión de interés público), y venga establecida por el Derecho de la Unión o en el Derecho del Estado miembro que se aplique al responsable del tratamiento y tal Derecho regule la operación específica de tratamiento o conjunto de operaciones en cuestión, como es el caso de las operaciones de tratamiento impuestas por el proyecto que se informa, haga uso de la posibilidad que establece el art. 35.10 RGPD de modo que sea el propio órgano proponente de la disposición general, quien realice en el curso del procedimiento de creación de la norma una evaluación de impacto relativa a la protección de datos (EIPD) como parte de una evaluación de impacto general en el contexto de la adopción de dicha base jurídica. Dicha EIPD habrá de incorporarse, como permite -casi debería decirse que lo impone, pero en cualquier caso no lo prohíbe- el art. 2.1, letra g), del Real Decreto 931/2017, de 27 de octubre, por el que se regula la Memoria del Análisis de Impacto Normativo. Este precepto es, además, suficientemente

expresivo de la voluntad del legislador de incluir en la MAIN, dentro del concepto “Otros impactos”, el análisis del “impacto que tendrá para la ciudadanía y para la Administración el desarrollo o uso de los medios y servicios de la Administración digital que conlleve la norma”.

g) Otros impactos: La memoria del análisis de impacto normativo incluirá cualquier otro extremo que pudiera ser relevante a criterio del órgano proponente, prestando especial atención a los impactos de carácter social y medioambiental, al impacto en materia de igualdad de oportunidades, no discriminación y accesibilidad universal de las personas con discapacidad y al impacto que tendrá para la ciudadanía y para la Administración el desarrollo o uso de los medios y servicios de la Administración digital que conlleve la norma

Dicho análisis de riesgos o la EIPD no parece haberse llevado a cabo por el órgano proponente del proyecto.

Esta Agencia recuerda, asimismo, que el reiterado Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS) establece que la política de seguridad del sistema de información deberá examinar y tener en cuenta “los riesgos que se derivan del tratamiento de los datos personales” (art. 12.1.f)), así como que en caso de que los sistemas de información traten datos personales (como es el caso), en todo caso, prevalecerán las medidas a implantar como consecuencia del análisis de riesgos y, en su caso, de la evaluación de impacto en caso de resultar agravadas respecto de las previstas en el citado real decreto (art. 3.3).

En definitiva, esta AEPD recomienda que se lleven a cabo, y se incorporen a la MAIN el análisis de riesgos (art. 24 y 25 RGPD) y la evaluación de impacto relativa a la protección de datos (art. 35 RGPD), en su caso, lo que permitirá, a la vista de ello, al propio prelegislador, determinar no sólo las medidas de seguridad necesarias en los sistemas de información, sino las garantías específicas que se requieran para afrontar los riesgos derivados del tratamiento de los datos que el proyecto de Real Decreto establece (ver art. 35.7.d) RGPD). Al no haber una EIPD en el presente caso, no se conocen cuáles son esos riesgos que derivan de los tratamientos de datos personales que establece la norma, por lo que tampoco en la norma se recogen las posibles medidas y garantías que paliarían esos riesgos

Corresponde, cabe recordar, al responsable del tratamiento, en virtud del principio de responsabilidad proactiva (art. 24.1 RGPD) el establecimiento de las medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el RGPD, teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, y que ello habrá de hacerlo “desde el diseño” del

tratamiento (art. 25.1 RGPD), integrando las garantías en el tratamiento, y ello aconsejaría que las garantías para minimizar los riesgos, una vez conocidos y ponderados en la EIPD tras el análisis de riesgos, se incorporen a la propia norma.

Desde un punto de vista práctico, esta Agencia ha publicado (abril 2023) su **Guía** denominada **“Orientaciones para la realización de una evaluación de impacto para la protección de datos en el desarrollo normativo”**¹, que tienen como objeto servir de guía para la realización de una evaluación de impacto para la protección de datos (EIPD) en el marco de la elaboración de la Memoria de Análisis de Impacto Normativo (MAIN), cuando las iniciativas legislativas de las Administraciones Públicas implican el tratamiento de datos personales. Este documento está orientado a los organismos de las Administraciones Públicas que promuevan proyectos normativos que impliquen tratamientos de datos personales a los que sea de aplicación el RGPD, así como la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales (L.O. 7/2021). Asimismo, está dirigido a los Delegados de Protección de Datos (DPD) de los citados organismos con el fin de contribuir al desempeño de sus funciones de asesoramiento en relación con dichos proyectos normativos.

En esta “Guía” se contienen, con profundidad y rigor, los pasos o el método a seguir para determinar la necesidad y el contenido de la Evaluación de Impacto, y entre ellos esta AEPD desea resaltar en este momento el apartado D del epígrafe II del mismo, relativo a las características de la norma que ampara el tratamiento:

Toda medida legislativa que habilite un tratamiento debe cumplir con la premisa de “previsto en la ley”. Esto implica que debe ser clara y precisa, y su aplicación accesible y previsible para sus destinatarios, de conformidad con el TEDH, el TJUE y el Tribunal Constitucional (TC). Por lo tanto, en la norma han de estar claramente definidos, con precisión y apropiadamente:

1.- La finalidad o finalidades del tratamiento.

2.- La legitimidad del tratamiento.

3.- La descripción de la implementación del tratamiento en sus aspectos relevantes, como pueden las operaciones y los procedimientos determinantes del tratamiento (por ejemplo, recogida, almacenamiento, acceso, transmisión, difusión,...), las tecnologías planteadas para implementar las operaciones (inteligencia artificial, almacenamiento en

¹ <https://www.aepd.es/es/documento/orientaciones-evaluacion-impacto-desarrollo-normativo.pdf>

Nube, biometría, IoT, móviles, videovigilancia,...), la existencia de decisiones automatizadas, así como la participación o posible participación de encargados y/o subencargados en distintas operaciones del tratamiento, entre otros.

4.- El ámbito y extensión del tratamiento con relación a las categorías de datos personales tratados (especialmente si son categorías especiales), las categorías de interesados afectados, las circunstancias en las que se utiliza la información personal (por ejemplo: de forma sistemática, solo en determinados casos, durante un periodo de tiempo limitado, etc.), los plazos de conservación de los datos, la frecuencia de recogida de datos, la granularidad de los datos y otros factores que definan el alcance del tratamiento.

5.- Los responsables/corresponsables o categorías de responsables y, en su caso, los encargados o categorías de encargos y/o de subencargados.

6.- Las entidades que acceden y a las que se pueden comunicar datos personales, así como los fines de tal comunicación, en particular, las condiciones de la comunicación de datos entre autoridades públicas en virtud de una obligación legal para el ejercicio de una misión oficial según las condiciones del RGPD (Cons. 31):

- En el marco de una investigación concreta.*
- De interés general.*
- De conformidad con el Derecho de la Unión o de los Estados miembros.*
- Por escrito y de forma motivada.*
- Con carácter ocasional.*
- No deben referirse a la totalidad de un fichero.*
- No deben dar lugar a la interconexión de varios ficheros.*

7.- La justificación de la solución adoptada para el acceso a datos personales, teniendo en cuenta que supone la utilización de datos de conformidad con unos requisitos específicos de carácter técnico, jurídico u organizativo, sin que ello implique necesariamente la transmisión o la descarga de los datos.

*8.- Las **medidas para garantizar un tratamiento lícito y equitativo, habida cuenta de la naturaleza, alcance (especialmente con relación a las categorías especiales de datos), contexto y finalidades del tratamiento** o de las categorías de tratamientos, los mecanismos de información y transparencia, así como las relativas a otras situaciones específicas de tratamiento a tenor del capítulo IX del*

RGPD, en particular, aquella orientadas a evitar los accesos o las transferencias de datos ilícitos o abusivos.

9.- En el caso de limitación por ley de derechos u obligaciones al amparo de los arts. 23 del RGPD o 24 de la L.O. 7/2021, debe estar muy clara su determinación, las condiciones específicas de limitación de las obligaciones y derechos (Cons. 19 del RGPD), y los perjuicios concretos a la consecución de los fines que justifican la falta de información a los interesados sobre la limitación. La lista anterior no es exhaustiva, sino que cualquier otra disposición pertinente, para cada caso concreto, debería incluirse en la descripción del tratamiento.

En cuanto a las características esenciales de los tratamientos que la norma habría de recoger, esta Agencia sugiere que el Proyecto que se realice tenga en consideración normas ya aprobadas que regulan tratamientos y que recogen este y las cautelas y garantías de estos, como puedan ser las siguientes:

- Ley Orgánica 11/2021, de 28 de diciembre, de lucha contra el dopaje en el deporte, ver Disposición Adicional (DA) cuarta;
- Ley 20/2022, de 19 de octubre, de Memoria Democrática, DA décima;
- Ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción, Título VI, arts. 30 y 32.
- Ley 3/2023, de 28 de febrero, de Empleo, art. 16.
- Ley 7/2023, de 28 de marzo, de protección de los derechos y el bienestar de los animales, art. 10, apartados 2, 4, 5, 6, 7, y art. 12.