

Tal y como resulta de la Exposición de Motivos, y de su articulado, el proyecto tiene por finalidad la modernización de la gestión fiscal mediante la estandarización y modernización de sistemas y programas informáticos o electrónicos que soportan los procesos contables, de facturación y de gestión de empresarios y profesionales, y además, establecer sistemas de facturación que permitan confiar en su inalterabilidad, mediante la interdicción del llamado software de supresión y manipulación de ventas. A lo anterior se añade una voluntad de asegurar la interconexión entre los sistemas informáticos de los administrados tributarios y la Administración, lo que dará lugar, continúa el proyecto, a permitir a medio plazo un significativo ahorro de los costes de cumplimiento de toda índole y, en particular, por lo que se refiere al presente proyecto, de los costes de cumplimiento tributario.

I

El proyecto expone que es desarrollo del art. 29.2.j) de la Ley 58/2003, de 17 de diciembre, General Tributaria (LGT), en la redacción añadida por la Ley 11/2021, de 9 de julio, que establece una obligación formal específica para productores, comercializadores y usuarios, de que los sistemas y programas informáticos o electrónicos que soporten los procesos contables, de facturación o de gestión de quienes desarrollen actividades económicas, garanticen la integridad, conservación, accesibilidad, legibilidad, trazabilidad e inalterabilidad de los registros, sin interpolaciones, omisiones o alteraciones de las que no quede la debida anotación en los sistemas mismos.

Se trata, en definitiva, del establecimiento de las características que ha de tener los sistemas de información de gestión tributaria y contable de empresarios o profesionales de manera que cumplan las características expresadas, lo que redundará en un beneficio para la gestión de la Hacienda Pública, y a su vez en un beneficio para dichos empresarios y profesionales en cuanto se simplifica la gestión tributaria.

Como tal, dichos sistemas tratan datos personales cuando se refieren a datos de personas físicas que resultan de las actividades de facturación (véanse art. 6 y 7 del Reglamento por el que se regulan las obligaciones de facturación, aprobado por Real Decreto 1619/2012, de 30 de noviembre): por ejemplo, DNI-NIF, nombre y apellidos, domicilio, o incluso la descripción de las operaciones (art. 6.1.f) del citado Reglamento), lo que puede incluso llegar a ser considerado datos de categorías especiales (por ejemplo, una factura de

una prestación de servicios médicos etc.). Dichos tratamientos de datos están incluidos en el ámbito de aplicación del RGPD, y de la LOPDGDD, y por lo tanto habrán de regirse igualmente por dicha normativa.

A este respecto, es preciso mencionar que el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS) establece expresamente (art. 3.1) que cuando un sistema de información trate datos personales le será de aplicación lo dispuesto en el RGPD y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, o, en su caso, 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, el resto de normativa de aplicación, así como los criterios que se establezcan por la Agencia Española de Protección de Datos o en su ámbito competencial, por las autoridades autonómicas de protección de datos, sin perjuicio de los requisitos establecidos en el presente real decreto. Añade expresamente (art. 3.2) en estos supuestos, el responsable o el encargado del tratamiento, asesorado por el delegado de protección de datos, realizarán un análisis de riesgos conforme al artículo 24 del Reglamento General de Protección de Datos y, en los supuestos de su artículo 35, una evaluación de impacto en la protección de datos.

En el proyecto presentado a informe no se contiene, en cambio, ninguna referencia ni a la protección de datos personales en dichos sistemas, ni a la necesidad de que el responsable, o encargado del tratamiento, realice, como establece el art. 3.2 citado del Real Decreto sobre el ENS un análisis de riesgos conforme al artículo 24 del Reglamento General de Protección de Datos y, en los supuestos de su artículo 35, una evaluación de impacto en la protección de datos. Y es de señalar igualmente que la Memoria de Análisis de Impacto Normativo (MAIN) tampoco contiene referencia alguna al impacto de estos sistemas de información en la protección de los datos personales de los interesados, ni establece medida alguna de seguridad o garantías para que esos tratamientos no interfieran más allá de lo estrictamente necesario en el derecho fundamental a la protección de datos de que disfrutaban las personas físicas.

Esta Agencia viene recomendando repetidamente en sus informes que el prelegislador, en aquellos casos, como el presente, en que los tratamientos tienen 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 art. 29.2.j) LGT, y desarrollados por el proyecto sometido a informe, haga uso de la posibilidad que establece el art. 35.10 RGPD de modo que sea el propio órgano

proponente de la disposición general, en el curso del procedimiento de creación de la disposición de la norma (ley, real decreto etc.) realice una evaluación de impacto relativa a la protección de datos como parte de una evaluación de impacto general en el contexto de la adopción de dicha base jurídica. 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***

Dicha EIPD no se ha llevado a cabo por el órgano proponente de la disposición general. Su realización permitiría que los responsables o encargados del tratamiento no tendrían la obligación de realizar dicha evaluación de impacto de datos personales (EIPD) prescrita en el art. 35 RGPD (y que el Real Decreto del ENS ha considerado asimismo obligatoria) precisamente por haberse llevado ya a cabo en el seno del proceso de gestación de la norma de carácter general.

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 RGPD) y la evaluación de impacto relativa a la protección de datos (art. 35 RGPD), 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 (ver art. 35.7.d) RGPD). Al no haber una EIPD no se conocen cuáles son esos riesgos que derivan del tratamiento generalizado y mecanizado, masivo, de datos personales que establece la norma, por lo que a esta Agencia no se le han ofrecido ni los riesgos ni en consecuencia 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 presente Reglamento, 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.

II

En la Disposición final primera del proyecto se modifica el Reglamento por el que se regulan las obligaciones de facturación, aprobado por el Real Decreto 1619/2012, de 30 de noviembre, en concreto se añade un apartado 5 al art. 6, en el cual se establece que en las facturas que se expidan mediante los sistemas informáticos regulados en el proyecto se incluirán “la representación gráfica de *ciertos* datos de la factura mediante un código «QR», y ello de acuerdo con las especificaciones técnicas y funcionales que se establezcan mediante Orden Ministerial. Igualmente, en la Disposición final tercera del proyecto, en la letras b) y c), se dice que mediante Orden Ministerial se “detallarán” determinados aspectos recogidos en el proyecto de Real Decreto, entre los que se incluyen: c) “*la estructura, contenido, detalle, formato, diseño y características de la información a que se refiere el artículo 10 del Reglamento anexo a este Real Decreto que deberá incorporarse al registro de facturación de alta*”, y “d) *la estructura, contenido, detalle, formato, diseño y características de la información a que se refiere el apartado 2 del artículo 11 del Reglamento anexo a este Real Decreto que deberá contener el registro de facturación de anulación*”. Lo mismo cabe decir respecto de la letra i) de la citada DF 3ª: i) *el contenido, formato, diseño, plazos de remisión y características de la información a que se refiere la disposición adicional tercera de este Real Decreto que podrá añadirse a la del registro de facturación de alta a efectos de completar el contenido y estructura del libro de facturas expedidas (...).*

Esta Agencia no comparte la consideración de que sea un mero “detalle”, susceptible de ser delegado en una Orden Ministerial, cuál es en concreto la Información que ha de ser tratada en el tratamiento de datos que la

norma establece (siempre que dicha “información” haga referencia a “datos personales”), lo que dejaría en una disposición de ínfimo rango la posibilidad de determinar qué datos personales (o cómo esos datos personales) habrán de reflejarse en el sistema. Así, por ejemplo, podría una mera OM establecer cómo habrían de reflejarse los datos personales en que consiste un acto médico en una factura, yendo más allá de lo establecido en el propio RD de facturación o en el proyecto. Esta AEPD considera que, por lo que se refiere a los datos personales que pudieran tratarse en los sistemas de información regulados en el proyecto, dicha regulación debería venir establecida directamente en la ley que ha establecido la necesidad del tratamiento (véase art. 6.3 in fine RGPD o art. 8 LOPDGDD).

El derecho a la protección de datos personales es un derecho fundamental, cuyo contenido consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso» (STC76/2019, de 22 de mayo, y STC 292/2000, de 30 de noviembre). Pero, además, estas sentencias señalaron igualmente la necesidad de que la injerencia esté prevista en una ley o norma de la Unión Europea, con respeto, en todo caso, al principio de proporcionalidad.

En concreto, el Tribunal Constitucional, en la STC 76/2019, de 22 de mayo, tras citar, entre otras, a su anterior STC 292/2000, de 30 de noviembre, señala:

- En segundo lugar, 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 (art. 81.1 CE), ora limite o condicione su ejercicio (art. 53.1 CE), precisa una habilitación legal (por todas, STC 49/1999, de 5 de abril, FJ 4). En la STC 49/1999, FJ 4, definimos la función constitucional de esa reserva de ley en los siguientes términos:

Esa reserva de ley a que, con carácter general, somete la Constitución española la regulación de los derechos fundamentales y libertades públicas reconocidos en su Título I, desempeña una doble función, a saber: de una parte, asegura que los derechos que la Constitución atribuye a los ciudadanos no se vean afectados por ninguna injerencia estatal no autorizada por sus representantes; y, de otra, en un Ordenamiento jurídico como el nuestro en el que los Jueces y Magistrados se hallan sometidos “únicamente al imperio de la Ley” y no existe, en puridad, la vinculación al precedente (SSTC 8/1981, 34/1995, 47/1995 y 96/1996) constituye, en definitiva, el único modo efectivo de garantizar las exigencias de seguridad jurídica en el ámbito de los derechos fundamentales y las libertades públicas. Por eso, en lo que a

nuestro Ordenamiento se refiere, hemos caracterizado la seguridad jurídica como una suma de legalidad y certeza del Derecho (STC 27/1981, fundamento jurídico 10)."

*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).*

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

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

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

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, Schrems 2, se añade (y se reitera posteriormente en las citadas sentencias de 6 de octubre de 2020):

176 Finalmente, para cumplir el requisito de proporcionalidad según el cual las excepciones a la protección de los datos personales y las limitaciones de esa protección no deben exceder de lo estrictamente

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

Como ya mencionamos más arriba en este informe, la STC 76/2019, tan reiterada, dispone:

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).

En definitiva, esas características del tratamiento de datos personales no deberían ser deferidas a una norma administrativa de inferior rango, como la Orden Ministerial.

III

En el art. 17 se establece la posibilidad, que no obligación, para los receptores de las facturas, de proporcionar a la AEAT voluntariamente “determinada” información, facilitando los datos contenidos en el código QR, cuyo contenido exacto se deja al arbitrio de una OM (nuevo art. 6.5 del Reglamento de facturación), siendo esta OM por tanto la que determinaría el tratamiento de datos. A esto ya se ha hecho referencia en el epígrafe anterior de esta Informe.

Igualmente, en este apartado, se recuerda que la remisión voluntaria de las facturas por los receptores a la AEAT, al igual que lo sería la remisión de la información por los emisores de las facturas a la AEAT, constituye una cesión

de datos (esto es, una “comunicación por transmisión”, es decir, un tratamiento de datos -art. 4.2 RGPD), por lo que los cedentes estarían sujetos a las obligaciones de información frente a los interesados que se recogen el RGPD, como sería, por ejemplo, la información contenida en el art. 13 RGPD. Ello es una mera consecuencia de los tratamientos de datos que se originan por la norma, al estar dichos tratamientos de datos sometidos en todo caso al RGPD.

En definitiva, y, por último, el proyecto no contiene referencia alguna a la normativa de protección de datos. Como es obvio, al no estar incluida la materia regulada en el proyecto en ninguna de las excepciones del art. 2.2 RGPD, o 2.2 LOPDGDD, será de aplicación el RGPD y la LOPDGDD, y ello debería reflejarse así en el texto de la norma, pues aun no siendo estrictamente necesaria (ya que la sujeción de los tratamientos de datos que se realicen sobre la base de esta norma a la normativa de protección de datos personales se producirá igual, con independencia de que se recoja así en la norma) sí que establece una certeza a los operadores jurídicos acerca de la normativa aplicable a dichos tratamientos, y, sobre todo, a los derechos de los interesados. Por ello, se sugiere que se incluya un apartado en el Reglamento que se aprueba en el Anexo en virtud del cual los tratamientos que se realicen sobre la base de esta norma estarán sujetos al RGPD y a la LOPDGDD.