

I

El art. 1 del proyecto de Real Decreto presentado establece que *“el presente real decreto tiene por objeto desarrollar la organización y el funcionamiento del Registro de Contratos Alimentarios, creado por el artículo 11 bis de la Ley 12/2013, de 2 de agosto, de medidas para la mejora del funcionamiento de la cadena alimentaria”*.

El proyecto expone que la Ley 16/2021, de 14 de diciembre, por la que se modifica la Ley 12/2013, de 2 de agosto, de medidas para mejorar el funcionamiento de la cadena alimentaria, ha introducido en dicho cuerpo legal el artículo 11 bis, por el que se dispone que el Ministerio de Agricultura, Pesca y Alimentación dispondrá de un registro digital en el que se inscribirán, con carácter obligatorio, los contratos alimentarios que se suscriban con los productores primarios y las agrupaciones de éstos, y sus modificaciones, antes de la entrega del producto objeto del contrato. Asimismo, se dispone que la Agencia de Información y Control Alimentarios, O.A. y las restantes autoridades competentes tendrán la potestad de acceder a dicho registro para realizar las comprobaciones pertinentes en el ámbito de sus competencias, con sujeción a la normativa en materia de protección de datos de carácter personal y de competencia. A su vez, la disposición final sexta de la Ley 16/2021, de 14 de diciembre, habilita expresamente al Ministro de Agricultura, Pesca y Alimentación a dictar cuantas disposiciones sean precisas para el desarrollo normativo y puesta en marcha del registro de contratos alimentarios previsto en el artículo 11 bis de la ley.

Se trata, en definitiva, del establecimiento de un sistema de información por el cual se contribuirá *“a incrementar la protección del productor primario y sus agrupaciones, al poner a disposición de las Autoridades de Ejecución encargadas de control del cumplimiento de las obligaciones impuestas en materia de cadena alimentaria un instrumento que facilitará las tareas de inspección y de control que tengan atribuidas y la tramitación de los posibles procedimientos sancionadores por las Administraciones competentes que se deriven los incumplimientos a lo dispuesto en la Ley 12/2013, de 2 de agosto, lo que, a su vez, redundará en una mayor seguridad jurídica en dichas relaciones comerciales y una estructuración más eficiente de la cadena”*.

Dicho sistema, como expresa la citada Exposición de Motivos, *“tendrá la finalidad de suministrar a la Agencia de Información y Control Alimentarios, O.A. (AICA, O.A.) y al resto de Autoridades de Ejecución designadas por las comunidades autónomas, la información necesaria para la comprobación del cumplimiento de la obligación de inscribir los contratos alimentarios y sus modificaciones, anexos y documentación complementaria, de conformidad con*

lo establecido en el artículo 11 bis de la Ley 12/2013, de 2 de agosto. Con tal finalidad, el real decreto regula los sujetos obligados a la inscripción y el contenido de la misma, y detalla la aplicación electrónica del Registro, (...)”

Como tal, dicho sistema trata datos personales -cuando se refieren a datos de personas físicas que resultan de las actividades reguladas en el registro- (véase Anexo I y Anexo II del Proyecto sometido a informe: por ejemplo, DNI-NIF, nombre y apellidos, direcciones de establecimientos, correo electrónico, 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 mencionado real decreto. Añade expresamente (art. 3.2) que, 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 RGPD y, en los supuestos de su artículo 35, una evaluación de impacto en la protección de datos (EIPD).

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 RGPD 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 este sistema 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 disfrutaran 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. 11 bis de la ley 12/2013, de 2 de agosto, de medidas para mejorar el funcionamiento de la cadena alimentaria, en la redacción dada por la ley 16/2021, de 14 de diciembre, 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.) quien realice 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 (MAIN). 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, o cuando menos, no se ha aportado a esta AEPD. Su realización permitiría que los responsables o encargados del tratamiento, una vez promulgada la norma, 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

El art. 10.4 del proyecto, al referirse al Inventario de Compradores, señala que *“los datos mínimos para dar de alta al sujeto obligado en el Inventario de Compradores serán los recogidos en el anexo I”*. E igualmente el art. 12.1 del Proyecto, al referirse esta vez al procedimiento de inscripción de contratos alimentarios en el Registro de Contratos Alimentarios, establece que *“el sujeto obligado (...) deberá inscribir los contratos alimentarios y sus modificaciones, anexos y documentación complementaria conforme a lo establecido en el artículo 4, de acuerdo con el procedimiento de inscripción regulado en este capítulo y que se detallará en la aplicación informática. Como mínimo, los datos a cumplimentar serán los establecidos en el anexo II”*. En ambos casos, el proyecto de Real Decreto hace referencia a que los datos regulados en el mismo son sólo “como mínimo”, esto es, que deja al desarrollo posterior por Orden Ministerial (véase Disposición Final Segunda) la posibilidad de modificar los Anexos, de modo que se permita ampliar los datos que “como mínimo” ha establecido el RD como de obligatoria inscripción en el registro.

Esta Agencia no comparte dicha posibilidad, desde la perspectiva de la normativa de protección de datos personales y siempre que se refiera a este tipo de datos, de que sea delegado en una Orden Ministerial, cuáles son -repetimos, siempre que se incluyan datos personales- en concreto la información que ha de ser tratada en el tratamiento de datos que la norma establece, 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. 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, que dicha regulación debería venir establecida directamente en la ley (ni siquiera en el proyecto de Real Decreto sometido a informe) 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).

Esta AEPD considera por tanto que es la norma con rango de ley que autoriza dicha intromisión en el derecho fundamental a la protección de datos personales de los afectados (esto es, la inscripción de determinados datos personales en un Registro) la que ha de determinar, como regulación básica, los datos personales que habrán de constar en dicho Registro, sin poder deferir dicha circunstancia a un reglamento, ni siquiera bajo la fórmula (utilizada aquí no en la ley, art. 11 bis, sino en el art. 1 del proyecto de Real Decreto informado) de que este desarrolla la “organización y funcionamiento” del Registro de Contratos Alimentarios, pues una cosa, desde la perspectiva de la normativa de protección de datos personales, es la “organización y funcionamiento del Registro” y otra es que sea el propio reglamento el que determine qué datos personales han de hacerse constar en el Registro, circunstancia esta que sería contraria al art. 18.4 de la Constitución, como ha resaltado la jurisprudencia que, de manera extensa, hemos citado.

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. En este último aspecto citado, se recuerda que, aunque el Proyecto restringe el acceso a la información a las autoridades que cita en el art. 16.2 y a los sujetos obligados en el art. 16.1, ello no es obstáculo para que los interesados cuyos datos personales son tratados (véase definición de “interesados” a estos efectos de protección de datos en el art. 4.1 RGPD) tengan en dichos tratamientos los derechos que les otorga en el RGPD y la LOPDGDD, que no se han visto limitados en modio alguno.

Por ello, se sugiere que se incluya un apartado en el proyecto en virtud del cual los tratamientos que se realicen sobre la base de esta norma estarán sujetos al RGPD y a la LOPDGDD.