

El proyecto sometido a consulta procede a integrar en una única norma jurídica, de forma clara y sistemática, la regulación aplicable a las aguas de consumo humano, hasta el momento dispersa en distintas normas jurídicas, al tiempo que se incorpora al ordenamiento jurídico interno las exigencias de la nueva Directiva (UE) 2020/2184 del Parlamento Europeo y del Consejo de 16 de diciembre de 2020 relativa a la calidad de las aguas destinadas al consumo humano.

De este modo, el proyecto de Real Decreto tiene una doble finalidad: por una parte, establece el marco jurídico para proteger la salud humana de los efectos adversos de cualquier contaminación del agua de consumo al garantizar que sea salubre y limpia y, por otra, facilita el acceso a la misma en el Reino de España

Asimismo, establece los requisitos de calidad del agua utilizada en la industria alimentaria para la fabricación de alimentos, o que entra en contacto con estos o con materiales y objetos destinados a entrar en contacto con alimentos. Asimismo, contempla posibles exenciones para los operadores de empresas alimentarias que dispongan de su propia fuente de agua y la utilicen para fines específicos de su actividad, siempre que se garantice la seguridad de los procesos y de los alimentos que fabrican, de acuerdo con los principios del análisis de peligros y puntos de control crítico establecidos en la legislación de seguridad alimentaria.

Del análisis del proyecto de Real Decreto, de un contenido eminentemente técnico, no se aprecia, en principio, que su aplicación vaya a implicar el tratamiento de datos de carácter personal, salvo en el supuesto del Sistema de Información Nacional de Agua de Consumo (SINAC) al que se refiere el Anexo IX, cuyo apartado 4, referido a la «Garantía de Seguridad», en su apartado b) señala que «Los datos de carácter personal se registrarán según lo dispuesto en Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales».

En, relación con dicho Sistema, sobre el que ya se pronunció esta Agencia, al amparo de la normativa entonces vigente, en sus informes de 2 de

febrero y 6 de junio de 2005, el Anexo IX contempla el alta de los «usuarios profesionales», así como el tratamiento de los datos correspondientes al nombre, apellidos y DNI, lo que va a implicar, en la forma en la que se señala en el apartado 3 del Anexo IX, tanto por parte de las entidades públicas y privadas que comuniquen los datos de los usuarios, los administradores autonómicos, así como por el Ministerio de Sanidad, el tratamiento de datos de carácter personal.

Todos estos tratamientos deben cumplir con la normativa sobre protección de datos de carácter personal que, en el momento actual, está constituida por el Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos, RGPD), que es directamente aplicable, así como por la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD) que lo complementa.

Por otro lado, tal y como viene señalando reiteradamente esta Agencia desde su informe 170/2018, es necesario deslindar los ámbitos de la seguridad de la información y de la protección de datos de carácter personal, al existir notables diferencias entre ambos:

«Consecuentemente, el derecho a la protección de datos de carácter personal de las personas físicas es un derecho fundamental y, por tanto, situado en el máximo nivel de protección jurídica, que actualmente se encuentra regulado directamente por la normativa comunitaria, estableciendo el citado RGPD un conjunto de principios, derechos, obligaciones y una estructura organizativa tendentes a garantizar dicho derecho fundamental. Dentro de los mismos, la seguridad de la información aparece como una obligación más de los responsables y encargados del tratamiento quienes deberán aplicar las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que incluirán, entre otros factores *“la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento”* y *“la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico”* (artículo 32.2. b) y c) del RGPD).

Por lo tanto, no cabe duda de que la garantía de la seguridad de los datos personales adquiere una especial trascendencia en cuanto a su protección, pero sin que ésta se limite exclusivamente al ámbito de la seguridad de dicha información, en cuanto que la protección de datos personales tiene un ámbito mucho más extenso que abarca, como

decíamos, a un conjunto de principios, derechos y obligaciones mucho más amplio.

Y todo ello bajo la garantía administrativa de las “autoridades de control”, funciones que en España asume, sin perjuicio de las competencias que corresponde a las autoridades de las Comunidades Autónomas en su ámbito competencial, la Agencia Española de Protección de Datos, que actúan con total independencia en el desempeño de sus funciones y en el ejercicio de sus poderes (Artículo 52 RGPD) y son las únicas competentes para *“asesorar sobre las medidas legislativas y administrativas relativas a la protección de los derechos y libertades de las personas físicas con respecto al tratamiento”* (artículo 57.1.c) RGPD)».

Por consiguiente, debe incluirse un apartado específico referido a la «Protección de datos personales» y modificarse la referencia a la normativa aplicable en los siguientes términos:

“Los tratamientos de datos de carácter personal de las personas físicas se realizarán con estricta sujeción a lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y el Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos y en Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales”.

Por otro lado, el mismo Anexo IX, contempla la información a facilitar a los consumidores tanto por parte de la Administración Local como por parte de la autoridad sanitaria, recogiendo en su PARTE D los requisitos de la solicitud de información, cuyo apartado 2 prevé la solicitud de datos al Ministerio de Sanidad cuando no sea posible obtenerlo de la Administración Local, del operador o de la Administración sanitaria autonómica en los términos que prevé su apartado 1. En este caso concreto de solicitud al Ministerio de Sanidad, se prevé específicamente que «c) Nunca sean datos personales».

Esta Agencia valora positivamente dicha exclusión, en la medida en que tampoco quedaría justificado, dada la finalidad pretendida con la información, referida a la calidad de agua de consumo, la comunicación de datos de carácter personal. No obstante, dicha exclusión, que implica para los órganos responsables la adopción de todas las medidas necesarias para garantizar que no se facilitan datos de carácter personal, debería contemplarse, igualmente, en el resto de supuestos de solicitudes de información contemplados en el apartado 1.

Por último, el apartado 3 prevé que la solicitud de información deberá contener el «nombre del solicitante y organismo al que pertenece», lo que implicará, a su vez, el tratamiento de datos de carácter personal, sometido a la normativa anteriormente citada.