Nº61 Abril de 2020

El interés público de los datos personales en tiempos del COVID-19

El COVID-19 nos recuerda que, entre los nuevos desafíos que nos muestra el siglo XXI, no es posible asumir que en el "estado del bienestar" las administraciones públicas serán las únicas con un papel clave para lograr una estabilidad en muchos aspectos, como el económico, el cultural o el social, sino que la colaboración público-privada es esencial, fundamentalmente en un ámbito como el tecnológico.

Los autores del artículo *"Big Tech Could Emerge From Coronavirus Crisis Stronger Than Ever"*, publicado en "*The New York Times*", explican con meridiana claridad cómo las grandes tecnológicas emergen frente al coronavirus más fuertes que nunca si cabe, frente a otros sectores de la economía a los que la pandemia sin lugar a dudas ha dejado en una cuarentena complicada de gestionar.

Y es que efectivamente la **tecnología se convierte en un arma estratégica para ganar la guerra al COVID-19,** por lo que no deja de ser en todo caso paradigmático que la tecnología a la que el COVID-19 hace emerger sea la mejor aliada de nuestras Administraciones Públicas para su freno.

A la necesidad de test, mascarillas, de respiradores, de personal sanitario, de ciencia e investigación, de buenos gestores y de mejores políticos, se le añade la necesidad de datos, de información, de tecnología, de infraestructura adecuada, de ética, de transparencia y de cumplimiento normativo.

En los últimos días hemos asistido a un importante **debate** en distintos medios de comunicación (al cual no hemos sido ajenos en este blog, véase **aquí**) sobre las bondades y los peligros de la recogida de datos personales en la lucha conta el COVID-19 en distintos ámbitos, como el laboral, el de la seguridad privada o el de la sanidad, al que se añade ahora el debate generado por la **Orden SND/297/2020**, de 27 de marzo, por la que se encomienda a la Secretaría de Estado de Digitalización e Inteligencia Artificial del Ministerio de Asuntos Económicos y Transformación Digital, el **desarrollo de diversas actuaciones para la gestión de la crisis sanitaria ocasionada por el COVID-19.**

Entre otras cuestiones, la Orden, en su norma segunda, sigue el modelo (también discutido en su día) emprendido por el Instituto Nacional de Estadística en su estudio de movilidad a través del **cruce de datos de los operadores móviles, de manera agregada y anonimizada**, para llevar a cabo el análisis de la movilidad de las personas en los días previos y durante el confinamiento.

La Orden deja clara una cuestión que será preciso explicar bien a la población: el responsable del tratamiento será el Instituto Nacional de Estadística (INE) y los operadores de comunicaciones electrónicas con quienes se llegue a un acuerdo de participación, los encargados del tratamiento.

La aclaración es a priori sencilla en un foro como el que entiendo lee este artículo: **los operadores llevarán a cabo el tratamiento de datos personales por encargo del INE**, quién por tanto, será el único que podrá decidir sobre el uso de los datos, debiendo someterse los operadores privados al Reglamento General de Protección de Datos (RGPD) y Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales (LOPDGDD) en el marco de un contrato u otro acto jurídico con el INE en el cual quedarán claramente reflejadas las obligaciones de cada parte y en el cual se limitará el tratamiento de los datos personales a dichos operadores privados en cuanto al objeto, la duración, la naturaleza y la finalidad del tratamiento y el tipo de datos objeto del tratamiento.

En su norma primera, la Orden encomienda a la Secretaría de Estado de Digitalización e Inteligencia Artificial, del Ministerio de Asuntos Económicos y Transformación Digital, el **desarrollo urgente y operación de una aplicación informática para el apoyo en la gestión de la crisis sanitaria** ocasionada por el COVID-19 que permitirá, al menos, realizar al usuario la autoevaluación en base a los síntomas médicos que comunique acerca de la probabilidad de que esté infectado, ofrecer información, consejos prácticos y recomendaciones a seguir y la

geolocalización del usuario a los solos efectos de verificar que se encuentra en la comunidad autónoma en que declara estar.

De nuevo se aclara que **el responsable del tratamiento será el Ministerio de Sanidad** y el encargado del tratamiento y titular de la aplicación será la Secretaría General de Administración Digital, quien además, autorizada por el Ministerio de Sanidad, podrá recurrir (esto es, contratar) a otros encargados (lo que incluirá seguramente otras terceras empresas privadas) para la ejecución de lo previsto.

En todo caso es preciso aclarar que el RGPD exige y condiciona al Ministerio a seleccionar únicamente para la colaboración a aquellos encargados del tratamiento que ofrezcan ***garantías suficientes para cumplir los requisitos de la normativa vigente*** y en los casos en que estos encargados del tratamiento sean empresas privadas hay que recordarles que quedarán sujetos a las exigencias del Real Decreto Ley 14/2019, de 31 de octubre, según el cual, entre otras cuestiones, por un lado, la empresa adjudicataria deberá presentar antes de la formalización del contrato una declaración en la que ponga de manifiesto dónde van a estar ubicados los servidores y desde dónde se van a prestar los servicios asociados a los mismos y por otro, se deberá advertir al contratista de que su obligación de someterse a la normativa nacional y de la Unión Europea en materia de protección de datos tiene el carácter de obligación contractual esencial, de conformidad con lo dispuesto en la letra f) del apartado 1 del artículo 211 y a los efectos de las causas de resolución del contrato. Aunque, de este Real Decreto mejor no hablar mucho porque su falta de técnica jurídica y pésima redacción pasará a la historia como una de las peores experiencias legislativas en materia de protección de datos personales.

En todo caso, si en base a lo establecido en la Orden ya se ha desencadenado un debate sobre las consecuencias de estas medidas para la privacidad y la protección de datos de la ciudadanía, parece predecible que cuando haya que ponerlas en práctica el escenario no va a ser distinto, aunque la Administración (*que es la responsable del tratamiento*), aún está a tiempo de cambiar esto.

Porque no es el “estado de alarma” lo que pone en riesgo la privacidad de las personas, sino la alarma que genera en la población la falta de información sobre la gestión del cumplimiento de la normativa de tratamiento de datos personales que de la Orden se deriva. No podemos olvidar que **la ciudadanía no tiene por qué ser experta en la norma, conocer su terminología ni confiar en las bondades del sistema,** menos aún en esta situación donde la acción del Gobierno está siendo tan censurable, a criterio de una mayoría de la población.

Aunque este Gobierno ya nos tenga acostumbrados a ello, no puede protegerse la privacidad y tratamiento de los datos personales de la ciudadanía a base de legislar con “reales decretos urgentes” y ”órdenes en situación de alarma”, con imprecisión, falta de claridad y ausencia informativa.

Hubiera sido deseable que la Orden SND/297/2020, de 27 de marzo, contase un informe preceptivo de la Agencia Española de Protección de Datos (AEPD) o en su caso, si contó con él, que así se hubiera indicado expresamente en el propio texto, puesto que, si bien es cierto que la Orden indica que velará por la exigencia de cumplimiento del RGPD, la LOPDGDD y los criterios interpretativos dados por la Agencia Española de Protección de Datos (AEPD), tanto lo uno como lo otro establecen amplios márgenes respecto de las modalidades de aplicación de las medidas de cumplimiento, por lo que en este punto queda esperar que el Ministerio de Sanidad acuda a los **recursos que el sistema establece para la salvaguarda de la seguridad jurídica en el cumplimiento de la norma**, como el de la consulta constante a la Autoridad de Control, la AEPD, lo que sin duda además ayudará a este organismo en relación con sus funciones de supervisión y ejecución de la normativa.

Parece que para ganar la confianza de la ciudadanía, al Ministerio de Sanidad solo le queda una opción: **cumplir la normativa y explicar cómo lo va a hacer.**

En este punto, vamos a destacar algunas de las obligaciones básicas del Ministerio de Sanidad en materia de protección de datos respecto del desarrollo de las soluciones tecnológicas contempladas en la norma primera de la Orden, llamando la atención sobre la posibilidad de

consultar además la extensa doctrina que la AEPD ha emitido para las Administraciones Públicas y ha publicado en su sitio web (véase por ejemplo la síntesis realizada en la infografía "Adaptación al RGPD de las Administraciones Públicas").

En primer lugar, y aunque parezca de Perogrullo, el proyecto requiere la presencia constante del **delegado de protección de datos** del Ministerio de Sanidad, velando por el cumplimiento de la normativa de protección de datos y ejerciendo, entre otras, sus funciones consistentes en: **(i)** inspección y supervisión del tratamiento que realice el Ministerio y emisión de las recomendaciones que considere necesarias, todo ello con imparcialidad, profesionalidad y garantizando su independencia sin incurrir en conflicto de intereses; **(ii)** documentación de cualquier vulneración relevante de la normativa que además, deberá comunicar inmediatamente a los órganos de administración y dirección.

Como la AEPD indica expresamente en su blog, el delegado de protección de datos es una **figura clave** para cumplir con el RPGD, además de ser el interlocutor con los ciudadanos en todas las cuestiones relacionadas con la protección de datos, incluyendo las reclamaciones. En la misma línea, la propia Agencia en su Guía para pacientes y usuarios de la Sanidad explica que la "*figura del delegado de protección de datos es importante para los ciudadanos, que pueden dirigirse a él para que atienda las reclamaciones que planteen sobre el tratamiento de sus datos y el ejercicio de sus derechos".*

Pero la ciudadanía no quiere solo un delegado sobre el papel, quiere un delegado ejecutivo, con recursos, y garantizando los derechos y libertades de las personas. En definitiva, un delegado "que se haga notar".

En segundo lugar, es obligación del Ministerio de Sanidad desarrollar las soluciones tecnológicas bajo el **principio de privacidad desde el diseño y por defecto,** lo que supone la adopción de medidas que pueden consistir en reducir al máximo el tratamiento de datos personales, seudonimizar lo antes posible los datos personales y dar transparencia a las funciones y el tratamiento permitiendo a las personas interesadas titulares de los datos supervisar el tratamiento.

- Si como la norma indica, "*la aplicación permitirá la geolocalización del usuario a los solos efectos de verificar que se encuentra en la comunidad autónoma en que declara estar*" será preciso que quede bien justificado técnica y organizativamente las medidas establecidas para impedir el uso de los datos con otros fines, o en otro caso, qué otros fines derivados de esta geolocalización se aplicarán además de verificar que una persona "está donde está".

- Si como la norma indica *"la aplicación no constituirá, en ningún caso, un servicio de diagnóstico médico, de atención de urgencias o de prescripción de tratamientos farmacológicos y su uso no sustituirá en ningún caso la consulta con un profesional médico debidamente cualificado*" pero sin embargo *"permitirá, al menos, realizar al usuario la autoevaluación en base a los síntomas médicos que comunique, acerca de la probabilidad de que esté infectado por el COVID-19, ofrecerle información sobre el COVID-19 y proporcionarle consejos prácticos y recomendaciones de acciones a seguir según la evaluación"*. será preciso valorar muy bien qué datos se van a pedir y durante cuánto tiempo se van a conservar por la Administración porque, tras ofrecer la información al usuario y proporcionarle los consejos parece que el tratamiento debería llegar a su fin, y con este fin a un proceso de bloqueo consistente en la identificación y reserva de los datos, adoptando medidas técnicas y organizativas, para impedir su tratamiento, incluyendo su visualización, excepto para la puesta a disposición de los datos a los jueces y tribunales, el Ministerio Fiscal o las Administraciones Públicas competentes, en particular de las autoridades de protección de datos, para la exigencia de posibles responsabilidades derivadas del tratamiento y solo por el plazo de prescripción de las mismas. Y transcurrido este plazo procederse a la destrucción de los datos.

No obstante, según nuestra normativa local de protección de datos, la AEPD puede fijar excepciones a la obligación de bloqueo pero, para ello se debería trasladar la consulta.

Suena raro en todo caso las limitadas finalidades explicadas en la Orden, teniendo en cuenta que la normativa permite el tratamiento ulterior de los datos personales con fines de archivo en

interés público, fines de investigación científica e histórica o fines estadísticos, por no ser incompatibles con el principio de «limitación de la finalidad», pero deben ser informados.

Asimismo, de acuerdo con el RGPD, si 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 (*en este caso el Ministerio de Sanidad*) será preciso que la finalidad del tratamiento dicha base jurídica podrá contener disposiciones específicas para adaptar la aplicación de normas del RGPD, entre otras: las condiciones generales que rigen la licitud del tratamiento; los tipos de datos objeto de tratamiento; los interesados afectados; las entidades a las que se pueden comunicar datos personales y los fines de tal comunicación; la limitación de la finalidad; los plazos de conservación de los datos, así como las operaciones y los procedimientos del tratamiento incluidas las medidas para garantizar un tratamiento lícito y equitativo, como las relativas a otras situaciones específicas de tratamiento.

Sobra decir que la Orden no llega a este nivel de detalle.

Asimismo, los tratamientos de datos deben ser sometidos a una **evaluación de impacto en la protección de datos "con carácter previo a su puesta en funcionamiento",** lo que exige que el responsable del tratamiento (esto es, el Ministerio de Sanidad) realice, antes del tratamiento:

- Una descripción sistemática de las operaciones de tratamiento previstas;
- Una descripción de los fines del tratamiento.
- Una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad.
- Una evaluación de los riesgos para los derechos y libertades de las personas interesadas.
- La descripción de las medidas previstas para afrontar los riesgos.
- La descripción de las garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales y que demuestren la conformidad con el RGPD.
- Y cuando proceda, recabar la opinión de los interesados o de sus representantes en relación con el tratamiento previsto, sin perjuicio de la protección de intereses públicos o de la seguridad de las operaciones de tratamiento.

En este proceso se exige la **participación del delegado de protección de datos** en relación con su función de asesoramiento, debiendo responder a las consultas que surjan y monitorizar el proceso.

Sin perjuicio de lo anterior, el Ministerio de Sanidad deberá activar el procedimiento de "***consulta previa***" ante la AEPD antes de poner en marcha el tratamiento de los datos si el resultado de la evaluación de impacto muestra que el tratamiento entrañaría un alto riesgo para los derechos y libertades de las personas y el Ministerio de Sanidad no ha identificado o mitigado suficientemente el riesgo. En estos casos, la autoridad de control deberá, en un plazo de ocho semanas -desde la solicitud de la consulta-, asesorar por escrito al Ministerio de Sanidad.

En tercer lugar, es obligación del Ministerio de Sanidad **proporcionar información detallada a la ciudadanía sobre el tratamiento de sus datos y los protocolos para ejercitar y garantizar sus derechos**.

El principio de transparencia exige que la información para la ciudadanía relativa al tratamiento de sus datos personales sea "fácilmente accesible y fácil de entender", esto es, en un lenguaje sencillo y claro, dando respuesta a cuestiones cómo la identidad del responsable del tratamiento, la del delegado de protección de datos, los datos objeto de tratamiento, su origen, los fines y base legítima, los destinatarios, el plazo de conservación, la necesidad de su tratamiento, los riesgos, las normas, las salvaguardias y los derechos relativos al tratamiento de datos personales así como del modo de hacer valer sus derechos en relación con el tratamiento reclamando la tutela de la AEPD.

En este punto, reiteramos **lo crucial de que los fines de tratamiento sean absolutamente informados** en su integridad y sin oscurantismos, con un lenguaje sencillo y con suficiente detalle **así como si los hay, los destinatarios de los datos**.

Es importante que se facilite a la ciudadanía **la forma de ejercicio de sus derechos,** puesto que a pesar de que el RGPD ha reforzado las garantías y derechos de las personas en relación con el tratamiento de sus datos, **es arduo y complejo para el ciudadano medio entender el objeto y alcance de cada derecho, su aplicación, las condiciones y requisitos para su ejercicio y la forma en que deben ejercitarse,** por lo que se deberían implantar protocolos fácilmente accesibles por las personas interesadas teniendo en cuenta los distintos segmentos poblacionales de quienes se tratarán los datos personales.

La transparencia o información a la ciudadanía sobre el alcance del tratamiento, según lo explicado y la garantía de sus derechos, son **elementos verdaderamente cardinales en la protección de datos,** por lo que un mal paso en las condiciones de regulación de estos aspectos supondrá un aldabonazo importante para una ciudadanía que ya mira con recelo las medidas adoptadas para controlar el contagio del COVID-19 en relación con su privacidad, sin perjuicio de la responsabilidad en que la Administración pueda incurrir.

Añadido a ello hay que hacer hincapié en que **no solo quedaría menoscabada la confianza de la sociedad en las instituciones, sino que, en términos de daño reputacional, las entidades privadas participantes en el proyecto podrían quedar seriamente dañadas**, con el agravante de que estas, en su condición de "meras encargadas del tratamiento" no son las responsables del tratamiento de los datos ni de las decisiones sobre el mismo, sino que son meras ejecutoras de las instrucciones que el Ministerio de Sanidad les comunique, lo cual, en todo caso, no les dejaría indemnes, dado que el RGPD les atribuye un **"deber in vigilando"** de que ninguna de las instrucciones infringe la normativa o, en su caso, si lo hiciera, informar de ello de inmediato al Ministerio.

Asimismo, el RGPD exige que el Ministerio de Sanidad cumpla con su responsabilidad proactiva y haga frente a la "***rendición de cuentas***" conforme a la cual debe construir la formulación específica y detallada de las medidas que para la observancia de la normativa de protección de datos adoptará y sería deseable que con el fin de evitar bulos y ganar la confianza de la población publique a través de su portal de transparencia, a modo de memoria, aquella información en relación con las medidas que ha adoptado, que no pongan en riesgo ni la privacidad de las personas ni las políticas públicas ni los secretos empresariales de las entidades privadas que participen.

Porque **la sociedad no solo demanda la observancia de la normativa, sino también una mayor transparencia en términos de privacidad** -según todo lo ya explicado- en relación con el funcionamiento de las soluciones tecnológicas y aplicaciones que se utilizarán para la batalla contra el COVID-19, algunas de ellas -como dijimos al inicio- en manos de entidades privadas a las que el coronavirus incluso ha hecho más fuertes.

Pero, a priori, aquí el problema no son las empresas privadas, las cuales, por norma general, disponen de exhaustivos planes de cumplimiento normativo y responsabilidad social empresarial para demostrar su "buen hacer", sino la incertidumbre provocada por la Administración al no establecer un marco claro de actuación. Porque de nuevo hay que mencionar que **en este caso, las entidades privadas tratarán los datos actuando "por Orden" y "por encargo" de Administración y no decidirán sobre el tratamiento de los datos de los ciudadanos**.

Eso sí, la falta de definición del marco claro de actuación por parte de la Administración (en términos de privacidad), además del perjuicio a los ciudadanos, redundará en perjuicio de la imagen y reputación de las empresas privadas colaboradoras, pese a sus muchos programas de cumplimiento normativo, sistemas de calidad y planes de responsabilidad social corporativa.

Solo si la responsabilidad de la Administración funciona en términos de transparencia y es capaz de explicar a la población cuál es el marco de actuación del tratamiento de los datos personales, se podrá desarrollar en la práctica la confianza suficiente de la ciudadanía y

también una crítica más constructiva por parte de los estudiosos o expertos de la privacidad. Ello desde luego, con la permanente supervisión de la Autoridad de Control, que es quien, en última instancia, tiene en su mano la aplicación efectiva de la normativa vigente en protección de datos.

De otra forma aumentará la sensibilización de la ciudadanía en contra de medidas que en otros países se han puesto en práctica y han sido efectivas y que, como hemos analizado, tienen cabida en el marco de nuestro Ordenamiento Jurídico y que además fomentan una colaboración público-privada en el marco del interés público, con un claro reparto de riesgos, funciones y capacidades, siempre en beneficio de la ciudadanía y en la única batalla posible, que es la batalla contra el COVID-19.

Ana Marzo Portera. Abogada
Publicado en el blog Hay Derecho
(https://hayderecho.expansion.com/2020/04/10/el-interes-publico-de-los-datos-personales-en-tiempos-del-covid-19/)