Centro de Estudios de Consumo

PUBLICACIONES JURÍDICAS
http://centrodeestudiosdeconsumo.com

Medidas que afectan a la protección de datos personales en tiempos del COVID-19*

Iuliana Raluca Stroie**
Centro de Estudios de Consumo
Universidad de Castilla-La Mancha

Fecha de publicación: 03 de abril de 2020

En un comunicado de 26 de marzo de 2020[1] la AEPD informaba que, en la actual situación de emergencia sanitaria, las autoridades competentes han desarrollado numerosas iniciativas que implican "un elevado volumen de tratamientos de datos personales y, especialmente, de datos sensibles como los de salud". Conforme señala la Agencia, la situación de emergencia "no puede suponer una suspensión del derecho fundamental a la protección de datos personales. Pero, al mismo tiempo, la normativa de protección de datos no puede utilizarse para obstaculizar o limitar la efectividad de las medidas que adopten las autoridades competentes, especialmente las sanitarias, en la lucha contra la epidemia".

* Trabajo realizado en el marco del contrato de investigación con referencia 2020-COB-9713 con cargo al Proyecto de Investigación PGC2018-098683-B-I00, del Ministerio de Ciencia, Innovación y Universidades (MCIU) y la Agencia Estatal de Investigación (AEI) cofinanciado por el Fondo Europeo de Desarrollo Regional (FEDER) titulado "Protección de consumidores y riesgo de exclusión social" dirigido por Ángel Carrasco Perera y Encarna Cordero Lobato y en el marco de la Ayuda para la financiación de actividades de investigación dirigidas a grupos de la UCLM Ref.: 2019-GRIN-27198, denominado "Grupo de Investigación del Profesor Ángel Carrasco" (GIPAC) y a la ayuda para la realización de proyectos de investigación científica y transferencia de tecnología, de la Junta de Comunidades de Castilla-La Mancha cofinanciadas por el Fondo Europeo de Desarrollo Regional (FEDER) para el Proyecto titulado "Protección de consumidores y riesgo de exclusión social en Castilla-La Mancha" (PCRECLM) con Ref.: SBPLY/19/180501/000333 dirigido por Ángel Carrasco Perera y Ana Isabel Mendoza Losana, en base a la Propuesta de Resolución Provisional de la Consejería de Educación, Cultura y Deportes, Dirección General de Universidades, Investigación e Innovación de la Junta de Comunidades de Castilla-La Mancha de 5 de diciembre de 2019.
** ORCID ID: https://orcid.org/0000-0003-1998-5412
[1] https://www.aepd.es/es/prensa-y-comunicacion/notas-de-prensa/aepd-apps-webs-autoevaluacion-coronavirus-privacidad

1. ¿Se suspende la obligación de notificar las brechas de seguridad como consecuencia de la suspensión de los plazos administrativos?

En este contexto, la primera norma que hace referencia al tratamiento de datos personales es el RD 463/2020 de 14 de marzo, por el que se declara el estado de alarma para la gestión de la situación de crisis sanitaria ocasionada por el COVID-19. Puesto que de conformidad a esta norma se suspenden los plazos administrativos para la tramitación de los procedimientos de las entidades del sector público, se ha generado la duda de si se vería afectada la obligación de comunicar las brechas de seguridad.

En su comunicado[2] del pasado 2 de abril, la AEPD aclara que la comunicación de brechas de seguridad no se vería afectada por esa suspensión, más cuando la situación de emergencia existente no puede suponer una suspensión del derecho fundamental a la protección de datos personales, por lo que persiste la obligación de los responsables de notificar ante la AEPD las quiebras de seguridad que afecten a datos personales.

Mas resulta todavía especialmente relevante que se conozca la existencia de dichas incidencias para que tanto autoridades de control como ciudadanos puedan adoptar las medidas de protección necesarias para su paliación. En consecuencia, los responsables de tratamientos están obligados a notificar a la autoridad de control cualquier brecha de seguridad a más tardar en el plazo de 72 horas, conforme se recoge en el art. 33 del RGDP[3]. Cometiendo en caso contrario una infracción grave, conforme a lo estipulado en el art. 73 r) de la LOPDPGDD[4]. La notificación se ha de realizar a través de la sede electrónica de AEPD y, además, si dicha brecha de seguridad supone un alto riesgo para los derechos y libertades de las personas físicas el responsable deberá comunicárselo también al interesado lo antes posible, "siendo especialmente relevante esta comunicación a los interesados en periodos de especial vulnerabilidad como en el que nos encontramos".

2. Aplicaciones y webs de autoevaluación del Coronavirus y medidas de geolocalización a través del teléfono móvil para las personas que han dado positivo en la prueba del COVID-19

El pasado 28 de marzo de 2020 se publico en el BOE la Orden SND/297/2020, de 27 de marzo, por la que se encomienda a la Secretaría de Estado de Digitalización e Inteligencia

[2] https://www.aepd.es/es/prensa-y-comunicacion/blog/notificacion-de-brechas-de-seguridad-de-los-datos-personales-durante-el

[3] 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 y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)

[4] Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

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.

2.1. Aplicaciones y webs de autoevaluación del Coronavirus

La norma habilita la creación de una aplicación informática para realizar al usuario la autoevaluación en base a los síntomas médicos que comunique, acerca de la probabilidad de que esté infectado por el coronavirus y, al mismo tiempo, debe ofrecer información, consejos prácticos y recomendaciones de acciones a seguir según la evaluación, sobre el COVID-19. No obstante, se advierte que dicha aplicación no sustituirá en ningún caso la consulta con un profesional médico debidamente cualificado, con lo cual no podrá sustituir el servicio de diagnóstico médico, de atención de urgencias o de prescripción de tratamientos farmacológicos.

Asimismo, se encomienda el desarrollo de un asistente conversacional/chatbot para ser utilizado vía WhatsApp y otras aplicaciones de mensajería instantánea para facilitar información oficial a la ciudadanía y responder a sus preguntas, basado en información oficial del Ministerio de Sanidad.

2.2. Geolocalizados por el COVID-19

Asimismo, la norma prevé dos posibilidades de geolocalización. Por un lado, se dispone que las aplicaciones de autoevaluación del coronavirus antes mencionadas, permitan la geolocalización del usuario solamente para verificar que se encuentra en la comunidad autónoma en la que declara estar, y pueden incluir dentro de sus contenidos enlaces con portales gestionados por terceros con el objeto de facilitar el acceso a información y servicios disponibles a través de Internet.

Por otro lado, se dispone la realización de estudios de movilidad a través del cruce de datos de los operadores móviles, de manera agregada y anonimizada, para el análisis de la movilidad de las personas en los días previos y durante el confinamiento.

Este método seguirá el modelo desarrollado por el Instituto Nacional de Estadística, siendo éste el responsable del tratamiento de datos mientras que los encargados serán los operadores de comunicaciones electrónicas móviles, con los que se llegue a un acuerdo.

3. Incidencia de las medidas con las normas de protección de protección de datos

Para empezar, debemos recordar la segunda parte del Considerando 46 del RGPD: *"[…Ciertos tipos de tratamiento pueden responder tanto a motivos importantes de interés*

público como a los intereses vitales del interesado, como por ejemplo cuando el tratamiento es necesario para fines humanitarios, incluido el control de epidemias y su propagación, o en situaciones de emergencia humanitaria, sobre todo en caso de catástrofes naturales o de origen humano]". Y también el Considerado 54 del mismo RGPD conforme al cual *"El tratamiento de categorías especiales de datos personales, sin el consentimiento del interesado, puede ser necesario por razones de interés público en el ámbito de la salud pública".*

Además, el artículo 6 del RGPD recoge una serie de supuestos en los que se legitima el tratamiento de datos personales como por ejemplo para el cumplimiento de una obligación legal aplicable al responsable del tratamiento (letra c), para proteger intereses vitales del interesado o de otra persona física (letra d), para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento (letra e). No obstante, el mismo Reglamento prohíbe, con carácter general en su art. 9, el tratamiento de datos sensibles, entre los cuales se encuentran los datos sobre la salud. Pero el mismo artículo, en su apartado 2 c) lo permite si "es necesario para proteger intereses vitales del interesado o de otra persona física".

Pero dentro de estas posibilidades ofrecidas por la normativa europea no se debe perder de vista que para salvaguardar intereses públicos, los responsables deben actuar de conformidad a la normativa establecida por un Estado miembro y en el caso de España, conforme señala el citado dictamen de la AEPD, la base jurídica se encuentra en la Ley Orgánica 3/1986, de 14 de abril, de Medidas Especiales en Materia de Salud Pública (modificada mediante Real Decreto-ley 6/2020, de 10 de marzo, por el que se adoptan determinadas medidas urgentes en el ámbito económico y para la protección de la salud pública, publicado en el Boletín Oficial del Estado de 11 de marzo de 2020) o la Ley 33/2011, de 4 de octubre, General de Salud Pública.

Por tanto, la legitimación de los tratamientos de datos antes mencionados podría encontrarse en el interés público o la garantía de los intereses vitales de los propios afectados o de terceras personas. No obstante, conforme señala la AEPD[5], el tratamiento no se puede realizar de cualquier manera, sino que se han de respetar los principios y las reglas contenidas en el Reglamento:

> 1º La finalidad para la que se pueden tratar los datos debe ser relacionada exclusivamente con el control de la epidemia, como por ejemplo ofrecer información sobre el uso de las aplicaciones de autoevaluación realizadas por las administraciones públicas o la obtención de estadísticas con datos de geolocalización agregados para ofrecer mapas que informen sobre áreas de mayor o menor riesgo.

[5] En su Comunicado de 26 de marzo de 2020.

2º Se ha de realizar el test de proporcionalidad por parte de las Autoridades Publicas y que se trate sólo de los datos necesarios para cumplir con el fin establecido.

3º Los datos podrán ser facilitado solo por mayores de 16 años requiriéndose autorización de los padres o representante legales para los menores de 16 años.

4º Los datos solo podrán ser tratados por las autoridades públicas competentes para actuar conforme a la declaración del estado de alarma, es decir, el Ministerio de Sanidad y las Consejerías de Sanidad de las Comunidades Autónomas, que podrán cederse datos entre ellas, y a los profesionales sanitarios que traten a los pacientes o que intervengan en el control de la epidemia.

5º Las entidades privadas que colaboren con dichas autoridades sólo podrán utilizar los datos conforme a las instrucciones de estas y, en ningún caso, para fines distintos de los autorizados.