ESTADO DE ALARMA POR COVID-19: ¿QUÉ IMPLICACIONES TIENE EN MATERIA DE PROTECCIÓN DE DATOS Y PRIVACIDAD?

16 de marzo de 2020

El pasado 11 de marzo de 2020, la Organización Mundial de la Salud (OMS) declaró a través de su director general, Tedros Adhanom Ghebreyesus la propagación del Coronavirus Covid-19 como una pandemia debido a la alta cantidad de personas infectadas y muertes que, hasta la fecha, ha causado el virus SARS-CoV-2.

Por lo que respecta a España, el pasado viernes 13 de marzo de 2020, es decir, dos días después de la declaración del Covid-19 como pandemia, el presidente del gobierno declaró el estado de emergencia ante la actual crisis sanitaria que está viviendo el país, que hasta la fecha de hoy reúne más de 9.000 contagios y 300 muertes.

La declaración del estado de emergencia supuso a su vez la aprobación en fecha 14 de marzo de 2020 del Real Decreto 464/2020, de 14 de marzo, por el que se declara el estado de alarmar para la gestión de la situación de crisis sanitaria ocasionada por el Covid-19 (en adelante, el "Real Decreto"). La entrada en vigor del Real Decreto ha supuesto, por aplicación de su artículo 10, la suspensión, como medida de contención de la pandemia, la apertura al público de una gran parte de los locales y establecimientos mercantiles de nuestra sociedad, lo cual se prevé que tenga un impacto altamente significativo en la economía española.

Adicionalmente, la entrada en vigor del Real Decreto ha supuesto, por un lado, la limitación de la libertad de circulación de las personas (artículo 7), quienes no obstante podrán seguir desplazándose al lugar de trabajo para efectuar sus prestaciones laborales y por el otro, ha reforzado el deber de colaboración con las autoridades competentes delegadas (artículo 5) otorgando a los agentes de la autoridad la facultad de comprobar que no se están llevando a cabo ninguna práctica suspendida por los anteriores artículos 7 y 10.

Pues bien, a pesar de que el Real Decreto carece de especificaciones en materia de protección de datos personales, el marco legislativo que dicha disposición implementará sobre España en, como mínimo, los próximos quince (15) días si es susceptible de contener diversas implicaciones en dicha materia que merecen ser analizadas en conjunto con la postura de la Agencia Española de Protección de Datos (en adelante, "AEPD").

En fecha 12 de marzo de 2020, el gabinete jurídico de la AEPD, en vista de la calificación del Covid-19 como pandemia, emitió un informe jurídico valorando la aplicabilidad de la normativa de protección de datos ante la inminente crisis sanitaria (en adelante, el "Informe"). Asimismo, y siguiendo la línea de otras autoridades de control como las agencias italianas y francesas de protección de datos, la AEPD también emitió una guía preguntas frecuentes que pretendía resolver las principales cuestiones con respecto al tratamiento de datos personales en el escenario del Covid-19.

En concreto, de los documentos anteriormente mencionados, se pueden derivar las siguientes conclusiones en relación con el Real Decreto en lo que respecta al marco de la protección de datos personales:

1. Aplicabilidad de la normativa de protección de datos a la situación actual.

En relación a la aplicabilidad de la normativa de protección de datos al escenario actual que ha implementado el Real Decreto, la AEPD recuerda que la normativa de protección de datos, cuyo objetivo es salvaguardar el derecho fundamental a la intimidad recogido en el artículo 18.4 de la Constitución, es aplicable en su integridad a la situación actual debido a que no existen razones ni se han adoptado medidas que puedan permitir determinar la suspensión de derechos fundamentales en este sentido.

Por tanto, el tratamiento de los datos personales que realicen las personas físicas o jurídicas dentro del ámbito de aplicación de la normativa deberá seguir efectuándose conforme las garantías que la misma prevé y en particular, en estricto cumplimiento de los principios de licitud, lealtad y transparencia, limitación de la finalidad, exactitud y minimización de los datos.

2. Bases de legitimación de las que disponen los Responsables del Tratamiento para legitimar el tratamiento de los datos personales en la situación actual.

La AEPD a su vez indica en su Informe a los Responsables del Tratamiento del deber del empresario de proteger y garantizar la seguridad y la salud de los trabajadores en aplicación del artículo 14 de la Ley 31/1995, de 8 de noviembre, de prevención de Riesgos Laborales (en adelante, "LPRL"). En este sentido, la AEPD recuerda que el cumplimiento de las obligaciones legales es una base de legitimación válida conforme al artículo 6.1.c) del Reglamento (UE) 2016/679 (en adelante, "RGPD"), no siendo necesario el consentimiento del afectado en lo que respecta al tratamiento de sus datos personales para garantizar el cumplimiento con la LPRL.

Sin embargo, la AEPD también reconoce la existencia de bases de legitimación alternativas que igualmente permitirían tratar datos personales de los afectados sin requerir de un consentimiento expreso. En particular, la AEPD, en alusión del Considerando 46 del RGPD indica que las bases de legitimación contempladas en los artículos 6.1.d) (Protección de los intereses vitales del interesado u otras personas físicas) y 6.1.e) (Misión realizada en interés público) podrán emplearse para el tratamiento de datos personales con la finalidad de controlar tanto epidemias como su programación.

Pues bien, en lo que respecta a las bases de legitimación resumidas en los artículos 6.1.c) y 6.1.e RGPD, la Agencia indica, en aplicación del artículo 6.3 RGPD, que la base del tratamiento ha de ser establecida por el Derecho de la Unión o el Derecho de los Estados Miembros, como por ejemplo, por medio de la normativa de prevención de riesgos laborales.

Sin embargo, y en lo que respecta a la base de legitimación del artículo 6.1.d) RGPD, la AEPD confirma que la justificación de intereses vitales no requiere de la obligación anterior, pudiendo a tales efectos emplearse sin necesidad de establecerse por el Derecho de la Unión o de los Estados Miembros. Adicionalmente, conviene indicar que tal base de legitimación puede ser empleada no solo para proteger los intereses vitales del interesado, sino además los de

terceros, pudiéndose ampararse en esta base medidas aplicables a una persona física que vayan encaminadas a consolidar y garantizar la protección de otras personas físicas, por tanto.

3. Principales implicaciones del tratamiento de datos de carácter personal de salud y otras categorías de datos sensibles.

De conformidad con el artículo 9 del RGPD, el tratamiento de datos personales de salud constituyen datos de categoría especial. El artículo 9.1 RGPD indica que el tratamiento de cualquier dato constitutivo de "categoría especial" está expresamente prohibido salvo que medie alguna de las excepciones que se indican en el artículo 9.2 RGPD. Por tanto, para justificar el tratamiento de datos de salud, el Responsable del Tratamiento necesitará de: (i) una base de legitimación válida conforme al artículo 6 RGPD; y (ii) la aplicación de una de las excepciones resumidas en el artículo 9.2 RGPD.

Pues bien, la AEPD en su Informe señala la posibilidad de aplicar a la situación actual una de las siguientes excepciones a la norma general de prohibición del artículo 9.1 RGPD:

i. Necesidad de tratar los datos para el cumplimiento de obligaciones en el ámbito del derecho laboral y de la seguridad y protección social (Artículo 9.2.b RGPD);

ii. Necesidad de tratar los datos para proteger intereses vitales del interesado o de otra persona física en caso de que el interesado no esté capacitado para dar su consentimiento (artículo 9.2.c RGPD);

iii. El tratamiento es necesario por razones de un interés público esencial, sobre la base del derecho de la Unión o de los Estados Miembros que debe ser proporcional y establecer medidas adecuadas para proteger los intereses y derechos fundamentales (artículo 9.2.g RGPD);

iv. Necesidad de tratar los datos con fines de medicina preventiva o laboral o diagnóstico médico (artículo 9.2.h RGPD); o

v. Necesidad de tratar los datos por razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud (artículo 9.2.i RGPD).

Sin embargo, la existencia las anteriores excepciones no implica que la totalidad de empresas y/u organismos puedan hacer uso de las anteriores excepciones para legitimar el tratamiento de datos personales de salud. En particular, la AEPD hace referencia a la normativa general de salud pública, compuestas principalmente por la Ley Orgánica 3/1986 de Medidas Especiales en materia de Salud Pública, así como la Ley 33/2011 General de Salud Pública para indicar que es la autoridad sanitaria quien, ante casos de epidemia adoptarán las medidas convenientes, correspondiéndoles a tal autoridad la protección de los intereses de las personas físicas. De esta manera, la AEPD destaca que serán las autoridades sanitarias quienes adoptarán las decisiones en aplicación de los intereses de las personas físicas y los responsables del tratamiento quienes seguirán tales instrucciones incluso en casos en los que pueda suponer un tratamiento de datos de categorías especiales.

Por otro lado, y en lo que respecta a la legitimación indicada en el artículo 9.2.b) RGPD, serán los empleadores, como sujetos obligados por la normativa de prevención de riesgos laborales quienes, en aplicación en todo momento de lo dispuesto en la misma podrán establecer las garantías necesarias para cumplir con su deber de garantizar la salud y seguridad de sus empleados, inclusive la prevención de contagios del Covid-19 en el centro de trabajo.

4. Otras cuestiones de relevancia: Aplicación de la Disposición Adicional 3ª del Real Decreto a las actividades de la AEPD.

El Real Decreto contiene a su vez una disposición adicional tercera que anuncia la suspensión de términos e interrupción de plazos para la tramitación de los procedimientos de las entidades del sector público, procediendo a tales efectos a reanudarse los mismos en el momento en que pierda vigencia el Real Decreto o en su caso, las prórrogas del mismo.

En vista de lo anterior, los procedimientos ante la AEPD quedarían a tales efectos cubiertos por lo

anterior, suspendiéndose a tales efectos hasta la efectiva pérdida de vigencia del Real Decreto.

Sin perjuicio de lo anterior, el apartado 3 de la Disposición Adicional tercera otorga la facultad al órgano competente de acordar, mediante resolución motivada, las medidas de ordenación e instrucción estrictamente necesarias para evitar perjuicios graves en los derechos e intereses del interesado en el procedimiento en dos casos específicos: (i) siempre que el interesado manifieste su conformidad; o (ii) cuando manifieste su conformidad con que no se suspenda el plazo. En este sentido, se deberá estar a la espera de la interpretación que realiza la AEPD de dicha facultad, pudiendo a tales efectos contemplarse la adopción de tales medidas en casos de violaciones de seguridad y/o ejercicio de derechos de interesados que sea significativamente perjudiciales para los derechos y libertades del interesado,, entre otros.

5. Conclusiones: Aplicación conjunta de las normas del Real Decreto y la postura de la AEPD.

Expuesta la postura de la AEPD en esta materia, y en vista de los artículos 5 y 7 del Real Decreto, se deben tener en cuenta las siguientes implicaciones:

i. Con independencia de la declaración del estado de emergencia el pasado 13 de marzo de 2020, la normativa de protección de datos personales seguirá resultando de aplicación;

ii. Asimismo, la normativa también contempla bases de legitimación alternativas al consentimiento, como el cumplimiento de una misión en interés público o la protección de los intereses vitales del interesado u otras personas físicas. En particular, la AEPD ha puesto de manifiesto que la legitimación de tratamientos basada en estas bases de legitimación es posible en estados de emergencia sanitaria como el actual;

iii. De igual forma, la normativa de protección de datos también contempla como base de legitimación el cumplimiento de obligaciones legales (artículo 6.1.c RGPD). A tales efectos, la facultad de inspección que el Real Decreto otorga a las autoridades competentes por virtud del artículo 5.2 y el posible tratamiento de datos personales que se origine a través del acceso a datos personales por parte de dicha autoridad competente encontraría debida justificación en tal precepto. Por tanto, no se requerirá el consentimiento por parte de las personas físicas para el desempeño de las funciones contempladas en la normativa por parte de las autoridades competentes;

iv. De igual manera, la solicitud al interesado de una autorización para acreditar que circula con motivos laborales no se recoge expresamente en el Real Decreto, por lo que podría contemplar un tratamiento no amparable en el artículo 6.1.c) RGPD. No obstante, actualmente existen varios organismos autonómicos que han recurrido a dicha obligación en alusión de las disposiciones del Real Decreto, por lo que es posible que en los próximos días la monitorización de los desplazamientos en este sentido pueda ser añadido como disposición legal, pudiendo a tales efectos ampararse el tratamiento de datos en este precepto. En cualquier caso, existen otras bases de legitimación alternativas mediante las cuales se podría justificar el tratamiento de datos personales en tal sentido, como por ejemplo, el consentimiento por parte del empleado e incluso la protección de intereses vitales del interesado (en permitirle desplazarse sin mayor inconveniente por parte de la autoridad competente) como de terceros (en garantizar que el autorizado en cuestión se desplaza por una cuestión debidamente contemplada en el Real Decreto);

v. El tratamiento de datos de categorías especiales como por ejemplo, los datos de salud, requerirán a su vez de una segunda legitimación con el fin de derogar la prohibición general que impide el tratamiento de dichas categorías de datos sensibles;

vi. Asimismo, y en lo que respecta al tratamiento de datos personales de salud en el ámbito de la relación empleador-empleado, la normativa de protección de

datos y la LPRL permiten el tratamiento por parte del empleador de los datos personales de sus empleados que sean necesarios para garantizar su salud y evitar así los contagios en el seno de la empresa y/o centro de trabajo.

vii. Lo anterior también aplicaría a la posibilidad de que, en el desempeño de garantizar la salud y seguridad de los empleados, el empleador pudiese llegar a tratar datos personales de visitantes con los que no mantiene ninguna relación laboral. En este sentido no obstante, la AEPD recomienda aplicar el principio de proporcionalidad, limitándose en todo caso la cantidad de información personal que se recabará sobre el visitante y evitando en cualquier caso toda aquella información que no esté relacionada con la enfermedad en cuestión.

viii. Sin perjuicio de lo anterior, y en cualquier caso, con independencia de que las categorías de interesados sean empleados o visitantes, los responsables del tratamiento deberán aplicar las garantías previstas en la normativa, así como la proporcionalidad en los tratamientos a desempeñar, debiendo seguir en cualquier caso las recomendaciones establecidas por las autoridades sanitarias, en particular, en lo que respecte al tratamiento de datos de categorías especiales de datos;

ix. La disposición adicional tercera del Real Decreto conlleva la suspensión e interrupción de plazos a todo el sector público, incluyendo a tales efectos los procedimientos ante la AEPD. Sin perjuicio de lo anterior, el apartado 2 de dicha disposición contempla la posibilidad de acordar mediante resolución motivada las medidas de ordenación e instrucción necesarias para evitar perjuicios graves en los derechos del interesado en el procedimiento. A tales efectos, será la AEPD quien, en el transcurso de las próximas semanas tan vitales para el estado español, deje entrever qué asuntos concretos se acordarán mediante resolución y qué medidas de ordenación e instrucción se dictarán para evitar dichos perjuicios.

ONTIER

Departamento: Propiedad Intelectual y Nuevas Tecnologías
Contactos:
Joaquín Muñoz: jmunoz@ontier.net
Álvaro Vidal: avidal@ontier.net