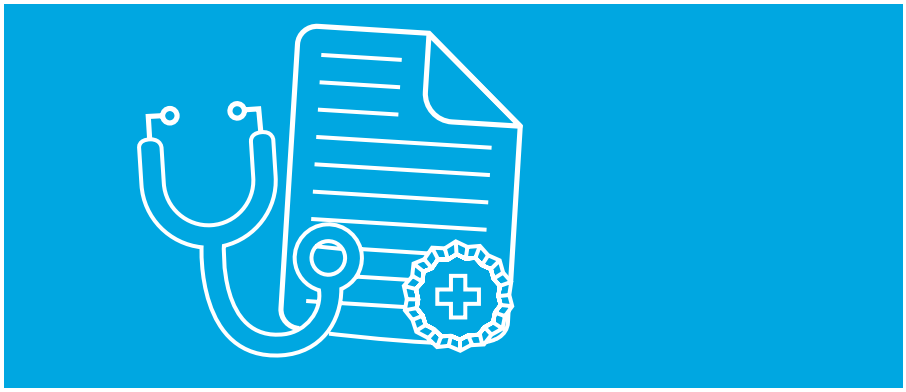
RSM Alert



LA PROTECCION DE DATOS Y EL USO DE LAS TECNOLOGÍAS EN LA LUCHA CONTRA EL COVID-19

Desde la declaración del estado de alarma por la crisis provocada por la propagación de la enfermedad COVID-19, la Agencia Española de Protección de Datos (en adelante la "AEPD") ha publicado a través de su página web determinados informes, notas de prensa, así como documentos consistentes en preguntas frecuentes sobre el tratamiento de datos de los particulares ante la pandemia.

En este entorno, en el mes de mayo, la AEPD ha publicado una guía práctica sobre el uso de determinados sistemas tecnológicos, mediante la cual, trata de analizar los beneficios, los costes y los riesgos que el uso de estas tecnologías puede suponer a la privacidad de los ciudadanos. No obstante, cabe precisar que el contenido de esta nota está sujeto a cambios puesto que como la Unión Europea está tratando esta materia a nivel global lo más probable es que tengamos comunicar cambios en los próximos días.

El documento elaborado por la AEPD se pronuncia acerca del uso de las siguientes herramientas tecnológicas:

1.- Geolocalización de los móviles por los operadores de telecomunicaciones:

Mediante este instrumento los operadores de telefonía móvil podrán proporcionar información anonimizada de la ubicación de sus usuarios. Este procedimiento ha sido utilizado recientemente tanto por nuestro Gobierno como por la Comisión Europea, para comprobar los movimientos de la población con el único fin de controlar la extensión de la pandemia.

A pesar de que este herramienta podría generar una inseguridad a los usuarios de estos terminales telefónicos, desde la AEPD aseguran que el acceso a dicha información de forma anónima no supone un mayor riesgo a la protección de la privacidad de los individuos que el que existía con anterioridad a la enfermedad, pues los ciudadanos siempre se encuentran expuestos a sufrir ciberataques, y a que no exista garantía ni certeza de su anonimización .

Por su parte, la AEPD, considera que este mecanismo puede suponer grandes ventajas para conocer los patrones de movilidad de la población y garantizar el control y la extensión de la pandemia desde el punto de vista sanitario. Una opinión que sin duda compartimos, pero a la que se deberá prestar especial atención en cuanto a su utilización para garantizar que la geolocalización no suponen una amenaza para la intimidad y la protección de datos de los usuarios.

2.- Geolocalización de los móviles a partir de las redes sociales:

Las direcciones IP desde las que se accede a estas plataformas, son utilizadas por los administradores de las páginas web para geolocalizar a los usuarios, normalmente con fines publicitarios.

Sin embargo, aunque los usuarios pueden verse amenazados por el uso de esta herramienta, lo cierto es que el riesgo de su localización a través de las redes sociales siempre ha generado una cierta inseguridad, que no se ve acentuada por la extensión de la pandemia. Este riesgo se incrementado en la medida en que los propios usuarios enriquecen sus perfiles sociales con información personal.

La AEPD advierte que las redes sociales no contienen una base jurídica adecuada que asegure que el uso y las políticas de privacidad se adapten al correcto tratamiento de los datos, pero apunta a que, si las autoridades sanitarias definen con exactitud el propósito de la utilización de esta información, esta herramienta podría ayudar a controlar la extensión de la pandemia. De modo que, una vez más se pone el foco de atención sobre las autoridades sanitarias, a las que se pide definición de propósitos y estrategias para ponderar los derechos y libertades de los ciudadanos respecto a la expansión de la pandemia.

3. Utilización de Apps, webs y chatbots para auto test o cita previa:

Con la aparición del COVID-19, son muchas las aplicaciones móviles, las webs y las chatbots que han implementado consultas de información, citas previas en servicios sanitarios o incluso test de preguntas y respuestas para comprobar la existencia de síntomas de esta enfermedad en los ciudadanos.

Aunque a priori la utilización de estas aplicaciones puede suponer grandes ventajas a la población, puesto que conlleva la relajación de otros canales de comunicación como el telefónico, lo cierto es que también pueden constituir una grave amenaza para los derechos y libertades de los ciudadanos. Hay que tener en cuenta que los datos que se incorporan a esta aplicación son datos relacionados con la salud, que requieren de la máxima protección por parte de quién lleva a cabo el tratamiento de estos datos.

De hecho, la AEPD ha podido constatar que algunas páginas web y apps no aportan una información suficientemente detallada que resulta exigible para identificar a los responsables, ni incluyen finalidades para las que podrían tratarse tales datos, por lo que, desde nuestro punto de vista, recomendamos que los ciudadanos extremen las precauciones con la utilización de estas aplicaciones.

4.- Apps de información voluntaria de contagios (Covapps).

Estas aplicaciones consisten en la elaboración de mapas y estadísticas de la propagación y extensión de la enfermedad del COVID-19, a través de la aportación de información proporcionada por los propios ciudadanos de forma completamente voluntaria. Una herramienta que contribuirá a conocer cuáles son las regiones o los puntos geográficos más afectados.

Sin embargo, tal y como venimos exponiendo, la utilización de estas herramientas sin la certeza de que cumplen con la normativa referente a la protección de datos podría suponer una grave amenaza para quienes facilitan esta información. Además, su uso es francamente controvertido, pues al monitorizar datos únicamente proporcionados por los ciudadanos, podría provocar una alteración de las estadísticas

si la información suministrada no es veraz. Desde nuestro punto de vista, no parece que sea aconsejable que los usuarios asuman los riesgos por el uso de estas aplicaciones frente a las eventuales ventajas que proporcionaría su uso.

5.- Apps de seguimiento de contactos por bluetooth (contact trace apps).

Estas aplicaciones utilizan la tecnología bluetooth de cualquier dispositivo electrónico para enviar una supuesta "tarjeta" a los usuarios de otros dispositivos. La tarjeta no tiene una identificación real del usuario, sino un apodo de su identidad. Este mecanismo permite que cada móvil pueda coleccionar de forma anónima tarjetas de las personas con las que ha estado en contacto los últimos días. De esta manera, aquel ciudadano que haya sido diagnosticado con el COVID-19 podrá informar a las personas con las que ha estado en contacto para que adopten las medidas que resulten necesarias.

La principal amenaza que contiene dicha aplicación es la construcción de las tarjetas anónimas, que aseguren la no identificación de los contagiados. Una tarea especialmente difícil, pues el uso de la tarjeta afecta a todos aquellos terceros con los que el usuario hubiera estado en contacto.

Por este motivo, a pesar de que esta herramienta pueda constituir una medida de prevención de contagios, desde la AEPD aseguran que en los protocolos de criptografía y anonimización de datos existen brechas que podrían provocar la identificación de las tarjetas con números de teléfonos y personas concretas, vulnerando sus derechos.

Sobre esta herramienta, la AEPD, considera que la colaboración ciudadana en el uso de este sistema es imprescindible para su utilidad, pues efectivamente solo será eficaz si al menos un 60 % de la población se da alta en la plataforma, por lo que, actualmente parece difícil su puesta en marcha.

6.- Pasaportes de inmunidad

Algunos países se están planteando la posibilidad de utilizar pasaportes de inmunidad. El mecanismo de estas aplicaciones es idéntico al que se utiliza con una tarjeta de embarque en los aeropuertos. Concretamente, a través de esta aplicación un responsable de control de acceso podría comprobar si una persona está inmunizada o ha padecido la enfermedad a través de la exhibición de un código QR en la pantalla de un dispositivo móvil.

Aunque esta aplicación puede suponer un plus de seguridad en los desplazamientos, y la existencia de un nuevo documento de identidad en un dispositivo móvil, que puede constituir una adecuada forma de controlar la pandemia, también expone al individuo a grandes riesgos como es el ciberataque que podría tener acceso a datos tan sensibles como el historial clínico.

La propia AEPD establece que actualmente la forma correcta de comprobar si una persona está contagiada o ha padecido la enfermedad, es a través de la realización de pruebas sanitarias realizadas presencialmente por un profesional especializado, pudiendo conceder en esos casos un certificado

que acredite dicha situación, constituyendo a su vez un salvoconducto para poder viajar, para ello, es imprescindible que estas apps se generalicen y se acepten por los distintos operadores implicados.

En definitiva, en nuestra opinión, el uso bien gestionado de estos registros electrónicos puede ser de gran utilidad, siempre y cuando dicha información sea realizada por un personal autorizado y vinculado al cumplimiento del control de la pandemia.

7.- Cámaras de infrarrojos para lecturas masivas de temperatura y toma de temperatura en centros de trabajo y comercios.

La utilización de termómetros como mecanismo para permitir el acceso a centros de trabajo o establecimientos comerciales y a estos fines el uso de cámaras que permiten el reconocimiento facial y la medición de la temperatura de los individuos, son sin duda las medidas de la que más se ha hablado durante los últimos días.

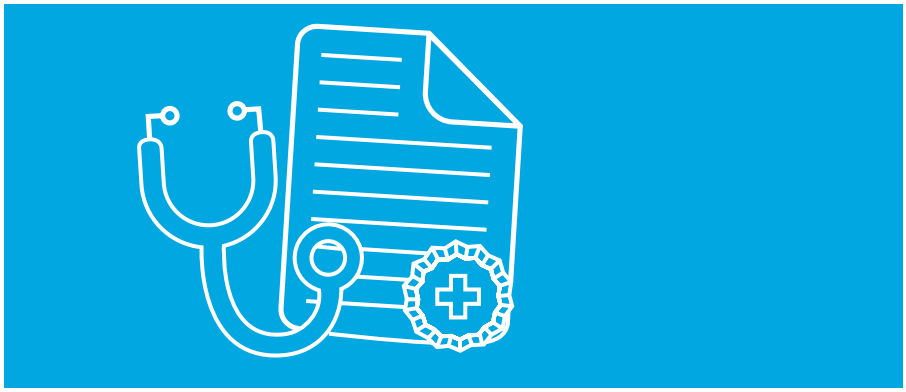
Ahora bien, en estos supuestos existen muchos interrogantes acerca de quien se encontraría legitimado para llevarla a cabo, en qué condiciones debería realizarse, y por supuesto, cuál es el tratamiento que se debe dar a estos datos.

La AEPD subraya que habrá que analizar caso por caso, y aclara que la toma de temperatura en centros de trabajo no es equiparable a la toma de temperatura en establecimientos comerciales. Así, el empresario que realice una toma de temperatura a sus empleados en un centro de trabajo se encontraría legitimado para realizarla ante la necesidad de cumplir con lo dispuesto en la Ley de prevención de Riesgos Laborales, quedando obligado en todo caso a preservar la proporcionalidad y la garantía del tratamiento de los datos de sus empleados. En cambio, la legitimación de la toma de temperatura en establecimientos comerciales es mucho más dudosa, pues si una persona se niega a que le tomen la temperatura antes de acceder al establecimiento, la consecuencia es que no le permitan el acceso. Por lo tanto, dicho condicionante implica que su consentimiento no sea del todo libre.

Ante la inseguridad que está provocando tanto a empresarios como propietarios de comercios la utilización de esta herramienta, la AEPD ha consultado al Ministerio de Sanidad la proporcionalidad de la utilización de las cámaras de infrarrojos y la toma de temperatura. Sin embargo, desde el Ministerio de Sanidad se ha recibido una respuesta muy poco concluyente, pues apuntan que dicha herramienta a día de hoy no es un mecanismo fiable para conocer si una persona se encuentra infectada por COVID-19.

Sin duda, la legitimación para el tratamiento de un dato de salud como es la toma de temperatura está sujeta a fuertes restricciones puesto que estos datos no podrán ser cedidos a terceros en ningún caso. Por este motivo, la AEPD exige al Ministerio de Sanidad que se pronuncie con rigor sobre las condiciones en las que se debe llevar a cabo esta medida, y que determine quienes son sujetos legitimados para ello y con qué garantías.

RSM Alert



En cuanto a la utilización de cámaras cabe señalar que es una cuestión controvertida, -de ahí la preocupación de la AEPD y la necesidad de recibir respuestas por parte del Ministerio de Sanidad-, pues hasta ahora la herramienta utilizada y permitida en nuestro país son las cámaras de video vigilancia desde el punto de vista del control empresarial y laboral [1]. De modo que su uso respondía hasta ahora a dos finalidades distintas, una relacionada al control laboral, en la que se requiere informar previamente a los trabajadores de forma expresa, y otra a la seguridad de las instalaciones y oficinas, en las que se requiere la colocación visible de un cartel informativo[2].

Es claro que el uso de cámaras de reconocimiento facial a través de las cuales se permita tomar la temperatura a los ciudadanos implica una nueva actividad que persigue una finalidad distinta de la que actualmente se encuentra permitida, y que requiere, sin lugar a dudas, de unas indicaciones y precisiones tanto por parte de las autoridades sanitarias como en materia de protección de datos.

En definitiva, podemos concluir que LA UTILIZACIÓN DE CUALQUIER HERRAMIENTA PARA COMBATIR LA PROPAGACIÓN DEL COVID-19, DEBE SER PROPORCIONAL A LA EFICIENCIA Y RECURSOS ORGANIZATIVOS, RESPETANDO LOS PRINCIPIOS ESTABLECIDOS EN EL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS, Y LAS FINALIDADES FIJADAS POR EL MINISTERIO DE SANIDAD, EXIGIENDO UNA PONDERACIÓN ENTRE LOS DERECHOS Y LIBERTADES DE CADA CIUDADANO Y LOS INTERESES POR EL CONTROL Y EXPANSIÓN DE LA PANDEMIA. ESTO SUPONE QUE, EN LA ACTUALIDAD, NO EXISTE UNA SOLUCIÓN FIABLE A LOS PROBLEMAS QUE PLANTEA EL USO DE LA TECNOLOGÍA PARA HACER FRENTE AL COVID-19.

1 Cuya regulación se encuentra amparada por el artículo 20.3 del Real Decreto Legislativo 2/2015, de 23 de octubre, por el que, se aprueba el texto de los Estatuto de los Trabajadores, y por el artículo 89.1 de la Ley Orgánica de Protección y garantía de los derechos digitales

2 Contemplado en el artículo 22.4 de la LOPDGDD.

TELEFONO ATENCIÓN CONSULTAS
LEGALES, LABORALES, FISCALES Y FINANCIERAS **CRISIS COVID-19**

Madrid T +34 91 457 02 39
Barcelona T +34 93 418 47 47

DIRECCIÓN EMAIL ATENCIÓN CONSULTAS
LEGALES, LABORALES, FISCALES Y FINANCIERAS **CRISIS COVID-19**

ready@rsm.es