legitec
legislación y tecnología

Abril, 2020

INFORME JURÍDICO :
PRIVACIDAD VS APLICACIONES PARA FRENAR EL COVID-19

www.legitec.com

INTRODUCCIÓN

Se está debatiendo mucho sobre la utilización de aplicaciones para el control del COVID-19, y sus implicaciones para la privacidad y la intimidad. Estas aplicaciones de control de la pandemia del coronavirus se han utilizado con éxito en China y en Corea del Sur. En este sentido, China sería difícilmente asimilable a Europa, por ello el sistema más estudiado es el coreano, donde la aplicación realizaba seguimiento de aquellas personas afectadas y a las que habían tenido contacto con ellas, de forma identificada. Cuando hablamos de este tipo de aplicaciones, existen varias posibilidades que inciden de forma diferente en nuestra privacidad. En función de las implicaciones sobre esta, podríamos agruparlas en los siguientes grupos:

Aplicaciones que utilizan datos anonimizados, de movimientos de la población, para prever la evolución del coronavirus. Estos datos se obtienen a través de compañías telefónicas, y su uso está previsto en 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, que se publicó en el BOE del 28 de marzo.*

Aplicaciones así se están utilizando en Italia, donde permiten analizar de forma anónima los movimientos de la población. Las autoridades europeas de protección de datos han manifestado la posibilidad de usar estas aplicaciones, con las salvaguardas necesarias respecto al uso, acceso y almacenamiento de la información y periodos de retención. https://www.europarl.europa.eu/news/es/press-room/20200406IPR76604/respeto-a-proteccion-de-datos-al-recabar-informacion-de-moviles-contra-covid-19

Aplicaciones que utilizan datos identificativos, como la aplicación murciana #LlámaleyDile de realización de encuestas a enfermos de coronavirus y a las personas que se han puesto en contacto con ellas, para realizar después un seguimiento de las mismas, o la madrileña coronamadrid.com. Dentro de este grupo de aplicaciones se enmarcarían aquellas cuyos requisitos legales se estudiarán más adelante. Otro tipo de aplicaciones que utilizan datos identificativos, y que se proponen para controlar quien puede o no circular libremente

(de modo que se introduzcan los datos identificativos de las personas que se han realizado el test y posteriormente las Fuerzas y Cuerpos de Seguridad del Estado, por ejemplo, puedan controlar que estas personas son aptas para circular libremente). Aquí los datos ya no se introducirían voluntariamente por las personas sino por el personal sanitario que realiza el test

Algunas aplicaciones requieren el suministro de datos de salud personales y posibilitan rastrear la ubicación y los contactos del individuo, lo que permitiría controlar la ubicación de la persona y sus contactos anteriores para, por ejemplo, verificar el cumplimiento de la obligación de confinamiento. Dentro de las aplicaciones que utilizan datos identificativos se han valorado como instrumentos muy eficaces para interrumpir las cadenas de infección las aplicaciones de rastreo de contacto, que permitirán reducir el riesgo de una propagación significativa del virus. La Unión Europea se ha planteado el uso de estas aplicaciones como un instrumento que permita el levantamiento de las medidas de contención de la COVID-19. Las aplicaciones que se han analizado a nivel europeo son las que incorporan alguna de las siguientes funcionalidades:

- Facilitar información exacta a las personas sobre la pandemia de COVID-19 (funcionalidad informativa).
- Ofrecer cuestionarios de autoevaluación y orientación a los ciudadanos (funcionalidad de comprobación de síntomas).
- Alertar a las personas que hayan estado cerca de a una persona infectada durante un tiempo determinado, a fin de proporcionar información, por ejemplo, sobre la conveniencia de someterse a una “autocuarentena” y de hacerse las pruebas (funcionalidad de rastreo de contactos y de alerta).
- Proporcionar un foro de comunicación entre médicos y pacientes en autoaislamiento o en el que se brinden consejos adicionales en materia de diagnóstico y tratamiento (funcionalidad de telemedicina).

REQUISITOS LEGALES

El asunto no es, por lo tanto, si se van a utilizar o no estas aplicaciones, sino cómo lo podemos hacer garantizando al mismo tiempo los derechos de los interesados, especialmente el derecho a la protección de datos y a la intimidad y confidencialidad de las comunicaciones, y cuáles son los límites que deben imponerse a dichas aplicaciones.

El respeto a la normas fundamentales, en particular las normas de protección de datos y confidencialidad de las comunicaciones, y asegurar un uso de las aplicaciones que evite la estigmatización han sido las preocupaciones plasmadas en la Recomendación (UE) 2020/518 de la Comisión de 8 de abril de 2020 relativa a un conjunto de instrumentos comunes de la Unión para la utilización de la tecnología y los datos a fin de combatir y superar la crisis de la COVID-19, en particular por lo que respecta a las aplicaciones móviles y a la utilización de datos de movilidad anonimizados

En este punto se analiza el cumplimiento de los principios de tratamiento de datos personales que se regulan en el artículo 5 del 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 - RGPD), poniendo en foco en aquellas aplicaciones que Europa se ha planteado como probables para el control de la pandemia.

Licitud, lealtad y transparencia. Art. 5.1.a) RGPD

Los datos personales serán tratados de manera lícita, leal y transparente en relación con el interesado. Uno de los primeros aspectos que debemos determinar es quién deberá ser el **responsable del tratamiento**, teniendo en cuenta de que éste es quien decide los medios y los fines del tratamiento de datos.

Al estar hablando de aplicaciones de utilidad pública, con finalidades de control de epidemia, las Orientaciones de la Comisión publicadas en el DOUE núm. 124, de 17 de abril de 2020 (Comunicación de la Comisión orientaciones sobre las aplicaciones móviles de apoyo a la lucha contra la pandemia de covid-19 en lo referente a la protección de datos) considera que deberían estar bajo el control de las **autoridades sanitarias.**

"*Habida cuenta de la sensibilidad de los datos personales y la finalidad del tratamiento de los datos que se describe más abajo, la Comisión considera que las aplicaciones deberían estar diseñadas de tal manera que las autoridades sanitarias nacionales (o las entidades que realicen una misión que se lleva a cabo en favor del interés público en el ámbito de la salud) sean las responsables del tratamiento*"

"El control de la aplicación por las autoridades sanitarias contribuiría, además, a aumentar la confianza del ciudadano en las aplicaciones, ya que permite un adecuado control de los datos por parte de estos. Al analizar la licitud del tratamiento realizado por estas aplicaciones debemos considerar la necesidad de que estas cuenten con una **base jurídica adecuada.**

Distinguiremos aquí, por un lado, la legitimación de la instalación de las aplicaciones y almacenamiento de información en el dispositivo del usuario y, por otro, la base de legitimación del tratamiento efectuado por las autoridades sanitarias de los datos obtenidos. En un primer lugar, respecto a la legitimación de la instalación de las aplicaciones y almacenamiento de información en el dispositivo del usuario, hemos de tener en cuenta la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas) que, en su artículo 5, afirma que sólo es posible la utilización de aplicaciones que interfieran en la confidencialidad de las comunicaciones (y que supongan escucha, grabación, almacenamiento u otros tipos de intervención o vigilancia de las comunicaciones y los datos de tráfico asociados a ellas por personas distintas de los interesados) con el consentimiento de los usuarios o autorización legal (conforme al artículo 15.1, en virtud de una norma necesaria, adecuada y proporcionada), con la única excepción del almacenamiento técnico necesario para la conducción de la comunicación.

La carga de algunos de los datos exigidos para el funcionamiento de las aplicaciones objeto del análisis (como los datos de proximidad o los alias) no son necesarios para el funcionamiento de la misma, por lo que exigiría el consentimiento de los interesados, y que el mismo se otorgara de forma libre, específica, explícita e informado, manifestándose con una acción afirmativa de voluntad, tal y como exige el RGPD.

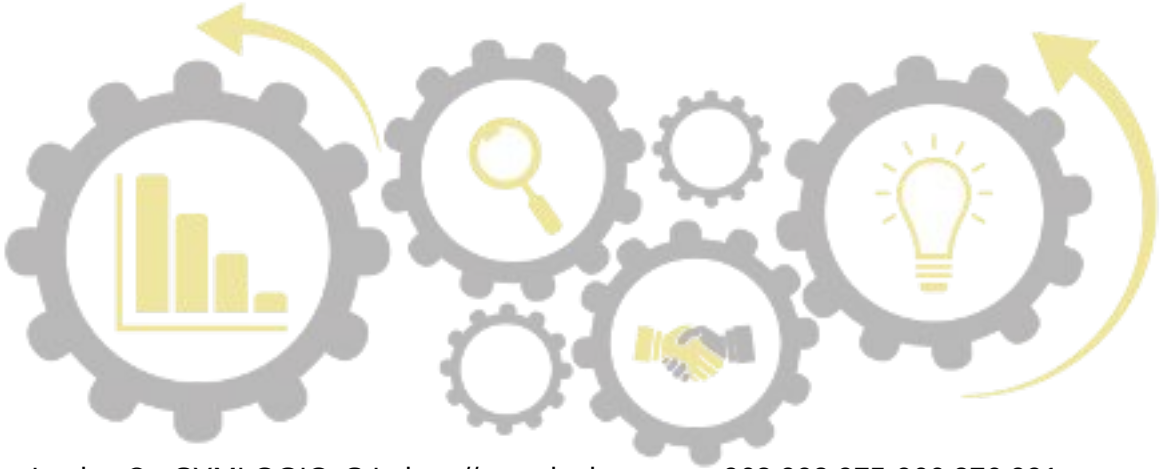
La Comisión, en las Orientaciones sobre las aplicaciones móviles de apoyo a la lucha contra la pandemia de COVID-19 en lo referente a la protección de datos, recomienda el uso de aplicaciones de carácter voluntario, "habida cuenta del alto grado de intrusión de una aplicación que se estableciera con carácter obligatorio. En este sentido, la no instalación de estas aplicaciones no deberá suponer ninguna consecuencia negativa para el ciudadano.

En segundo lugar, respecto a la base de legitimación del tratamiento efectuado por las autoridades sanitarias, el considerando 46 del RGPD afirma *que ciertos tipos de tratamiento pueden responder tanto a motivos importantes de interés público como a los intereses vitales del interesado,por ejemplo cuando el tratamiento es necesario para fines humanitarios, incluido el control de epidemias y su propagación.*

El tratamiento de los datos personales es licito cuando es necesario para proteger intereses vitales del interesado o de otra persona física y, también, cuando es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento (artículo 6 RGPD).
Puesto que en estas aplicaciones estamos tratando datos de categorías especiales (salud) debemos tener en cuenta el artículo 9 del RGPD que nos permite su tratamiento por razones de interés público esencial y por razones de interés público en el ámbito de la salud pública.

No debemos perder de vista que los diferentes Estados contaban ya con legislación que permitía la toma de medidas extraordinarias por razones de salud publica (articulo 4 Ley Orgánica 4/1981, de 1 de junio, de los estados de alarma, excepción y sitio, o el artículo 26 de la Ley 14/1986, de 25 de abril, General de Sanidad, por ejemplo). Además, la situación actual ha aumentado la actividad legislativa sobre el tema.
La Comisión aconseja apoyarse en la legislación como base jurídica que contribuye a la seguridad jurídica, al describir claramente los tratamientos y finalidades específicas, determinar de forma clara quién es el responsable del tratamiento y quién puede acceder a dichos datos, recoger garantías específicas y garantizar que los datos no pueden ser tratados para fines distintos de los recogidos legalmente.

Que la base de legitimación sea una ley no implica que la aplicación sea obligatoria, por las razones ya expuestas anteriormente. La decisión de no instalar o desinstalar una aplicación no debería tener consecuencias negativas para el individuo.



En caso de que las aplicaciones de rastreo de contactos y alerta emitan directamente la alerta, las Orientaciones de la Comisión nos recuerdan que está prohibido que una persona sea objeto de una decisión basada únicamente en un tratamiento automatizado que produzca efectos jurídicos para la persona o le afecte significativamente de modo similar (artículo 22 del RGPD).
Las aplicaciones deberán también garantizar la **transparencia** ofreciendo la información que se recoge en los artículos 12 y 13 del RGPD y 5 de la Directiva de comunicaciones y privacidad.

Limitación de la finalidad. Art. 5.1.b) RGPD

Los datos personales serán recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; de acuerdo con el artículo 89, apartado 1, el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales.

Las distintas funcionalidades de la aplicación no deben agruparse. De esta manera la persona puede dar el consentimiento específicamente para cada una de ellas, o bien combinar distintas funcionalidades. En cualquier caso, la persona debería siempre poder escoger entre las que persigan un fin distinto.
No se deben utilizar los datos recogidos para fines distintos a los específicos de lucha contra el COVID-19. Si se desean utilizar también para investigación científica y estadística, se deberían incluir en la lista original de fines y comunicarse claramente a los usuarios (transparencia).

En la Comunicación de la Comisión se aclara como definir las finalidades de forma determinada, explícita y legítima en las aplicaciones para las funcionalidades estudiadas, de forma que se huya de finalidades genéricas o abstractas. Aclara así, por ejemplo, que la mera indicación como finalidad de “prevención de nuevas infecciones de COVID-19” no es suficientemente específica.

Minimización de datos. Art. 5.1.c) RGPD

Los datos personales serán adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados

Minimización de datos recogidos

Las aplicaciones analizadas en este artículo recogen, generan y almacenan diferentes tipos de datos:

- Datos personales (información de personas físicas identificadas o identificables), protegidos por el RGPD, algunos de ellos con protección especial por ser datos sensibles como los datos de salud.
- Datos almacenados en la terminal del usuario, y los que se acceda desde dicho equipo, así como datos de localización, que indican la posición del equipo terminal del usuario, tratados por una red de comunicaciones o servicio de comunicaciones electrónicas, protegidos por la Directiva sobre la privacidad y las comunicaciones electrónicas.
- Datos no personales (por ejemplo, datos anonimizados de forma irreversible) que no gozan de protección.

En aplicación del principio de **minimización de datos** (art. 5), está claro que tendremos que utilizar para dicho control de la pandemia solo los datos adecuados, pertinentes y estrictamente necesarios, control que se debe realizar en aplicación del artículo 25 Protección de datos desde el diseño y por defecto) mediante un análisis realizado con carácter previo, que debe incluir, en algunas ocasiones, (y esta sería sin duda una de ellas) una evaluación del impacto de dicho tratamiento en los derechos y libertades de los interesados que analice, entre otras cosas, la proporcionalidad de dicho tratamiento de datos para el cumplimiento de los fines propuestos.

Esto implica que estas aplicaciones deben haber realizado, con carácter previo, un análisis de riesgos y evaluación de impacto para valorar las medidas de seguridad utilizadas, los datos tratados y la proporcionalidad del tratamiento en sí.
Las Orientaciones de la comisión dan indicaciones sobre los datos que se consideran adecuados en función de las funcionalidades que incorpora la aplicación. Por ejemplo, una aplicación cuya funcionalidad sea ofrecer información al afectado no requerirá el acceso a datos de salud, ni a los contactos del interesado.

En este sentido resultan muy interesantes las orientaciones para las aplicaciones de rastreo de contactos y alerta, en las que pueden necesitarse datos de proximidad. Por ejemplo, para la detección de los dispositivos próximos la Comisión recomienda el uso de los datos de comunicaciones por Bluetooth de baja energía (BLE), por ser más precisa y no permitir el rastreo (a diferencia de los datos de geolocalización o datos GNSS/GPS).

La Comisión establece, por ejemplo, que en las aplicaciones anteriormente citadas de información, dado que constituyen únicamente el medio de comunicación, las autoridades sanitarias no tendrán acceso a ningún otro dato. En las aplicaciones de rastreo y alerta, las más discutibles desde el punto de vista de la protección de datos, se tratan datos de la persona infectada y datos de las personas que han estado en contacto con la misma.

Con base en el principio de minimización de datos se debería optar por una solución descentralizada, almacenando los datos de la persona infectada en el dispositivo del usuario y no en el servidor final, de forma que el dato que llega a las autoridades sanitarias es el de las personas que han estado en contacto con aquella (datos de proximidad). Los datos de la persona infectada tampoco deberían llegar a sus contactos.
En otro sentido, tal y como establece la Comisión, los datos sobre el momento y el lugar de tales contactos no deberían almacenarse, por lo que no es necesario ni posible comunicar dichos datos.
Estas y otras indicaciones sobre la minimización de datos aparecen reflejadas en la comunicación de la Comisión de 17 de abril.

Exactitud. Art 5.1. d) RGPD

Los datos personales serán exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan.

A la hora de evaluar el cumplimiento del principio de exactitud de los datos, uno de los aspectos que puede resultar más problemático es el uso de datos de proximidad en aplicaciones de rastreo y seguimiento, ya que pueden generar falsos positivos.
El uso de datos de localización basado en redes de telefonía móvil no garantiza la precisión suficiente, por lo que la Comisión aconseja el uso de tecnologías como el Bluetooth que permiten una evaluación más precisa.

Limitación del plazo de conservación. Art. 5.1.e) RGPD

Los datos personales serán mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento.

Los plazos de tiempo establecidos para la conservación de los datos deben fijarse teniendo en cuenta datos médicos (por ejemplo, el plazo de incubación) y el plazo necesario para tomar las medidas administrativas necesarias.

En sus orientaciones la Comisión establece, por ejemplo, que no hay justificación para la conservación de datos en aplicaciones con funcionalidad de información, mientras que en las aplicaciones de comprobación de síntomas y telemedicina se deberían suprimir los datos tras un período máximo de un mes (período de incubación más el margen) o después de que la persona haya sido sometida a una prueba con resultado negativo, dando el mismo plazo para aplicaciones de rastreo y seguimiento.
La conservación más allá de estos plazos se debería realizar con datos anonimizados.

Integridad y confidencialidad. Art. 5.1.f) RGPD

Los datos serán tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas. Es importante que se garantice la seguridad de los datos personales almacenados, tanto en el dispositivo como en el servidor central.
En este sentido, es aconsejable que los datos se almacenen en el dispositivo del usuario, pasando solo al servidor central en el momento en que sean necesarios para el cumplimiento de la finalidad.
También resulta necesario el cifrado de dicha información y el control de accesos, incluido el acceso administrativo a los datos del servidor central.

En cuanto a los identificadores de usuario creados para las aplicaciones de proximidad, se aconseja la utilización de identificadores temporales que garanticen la confidencialidad.

Las Orientaciones incluyen otras medidas que pueden revisarse, además de aconsejar, en consonancia con los solicitado por numerosos expertos, que el código fuente de la aplicación se haga público y esté disponible para su revisión.

CONCLUSIONES

Algunas de las dudas que se planteaban en origen han sido abordadas por la Comisión. El último punto de las Orientaciones nombradas afirma que "Las autoridades de protección de datos deberían participar y ser consultadas plenamente en el contexto del desarrollo de la aplicación y seguir atentamente su despliegue". Este era uno de los requisitos más demandados para asegurar el respeto a los derechos fundamentales y garantizar la confianza de la ciudadanía en estas aplicaciones.

El hecho de que la instalación de dichas aplicaciones precise de nuestro consentimiento elimina las reticencias lógicas que una aplicación de uso obligatorio generaría. Sin embargo, en relación al tratamiento efectivo de los datos, descartar ese mismo consentimiento como base de legitimación del tratamiento, fundamentando el mismo en una norma, refuerza la seguridad jurídica y aumenta la confianza en dichas aplicaciones.

En cualquier caso, es necesario que se realicen los análisis de riesgos y las evaluaciones de impacto correspondientes al tratarse de tratamiento a gran escala de categorías especiales de datos.

Y, por último, pero no menos importante, concluimos que la transparencia en estos temas es fundamental, por lo que el ciudadano debería poder informarse de forma clara del tratamiento que se está realizando de sus datos personales, así como mantener el control de los mismos y poder ejercitar de manera fácil los derechos reconocidos por la legislación de protección de datos sin consecuencias negativas.

Escrito por:
María Herrera de Orduña
Consultora jurídica y auditora. Delegada de Protección de Datos.

Avenida de los Rectores 2, bajo, 30100, MURCIA
info@legitec.com
Murcia: +34 968902975 – murcia@legitec.com
Alicante: +34 966276991 – alicante@legitec.com
Córdoba:+34 957492510 – cordoba@legitec.com
Madrid: +34 911124085 – madrid@legitec.com
Sevilla:+34 954640434 – sevilla@legitec.com

@legitec

legitec
legislación y tecnología