II

(Comunicaciones)

COMUNICACIONES PROCEDENTES DE LAS INSTITUCIONES, ÓRGANOS Y ORGANISMOS DE LA UNIÓN EUROPEA

COMISIÓN EUROPEA

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

(2020/C 124 I/01)

1. CONTEXTO

La pandemia de COVID-19 ha supuesto un desafío sin precedentes para la Unión y los Estados miembros, sus sistemas sanitarios, su modo de vida, su estabilidad económica y sus valores. Las tecnologías y los datos digitales tienen una valiosa función que desempeñar en la lucha contra la crisis de la COVID-19. Las aplicaciones para dispositivos móviles que suelen estar instaladas en teléfonos inteligentes («aplicaciones») pueden facilitar a las autoridades sanitarias públicas a nivel nacional y de la UE el seguimiento y contención de la pandemia de COVID-19 y son especialmente pertinentes de cara al levantamiento de las medidas de confinamiento. Esas aplicaciones pueden proporcionar orientaciones directas a los ciudadanos y facilitar la labor de rastreo de contactos. En algunos países, tanto dentro de la UE como en el resto del mundo, las autoridades nacionales o regionales o los desarrolladores han anunciado el lanzamiento de aplicaciones con diferentes funcionalidades destinadas a apoyar la lucha contra el virus.

El 8 de abril de 2020, la Comisión adoptó una Recomendación 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 lo sucesivo, «la Recomendación») ([1]). Lo que se pretende con esa Recomendación es, entre otras cosas, desarrollar un enfoque europeo común (el «conjunto de instrumentos») para el uso de aplicaciones móviles, coordinado a nivel de la Unión, con el fin de capacitar a los ciudadanos para adoptar medidas de distanciamiento social eficaces, así como con el fin de alertar, prevenir y rastrear contactos con miras a limitar la propagación de la enfermedad de la COVID-19. La Recomendación establece los principios generales que deberían guiar el desarrollo de ese conjunto de instrumentos e indica que la Comisión va a publicar orientaciones adicionales, especialmente en lo referente a las consecuencias del uso de las aplicaciones en este ámbito para la intimidad y la protección de los datos personales.

Con la hoja de ruta europea conjunta para el levantamiento de las medidas de confinamiento contra el COVID-19, la Comisión, en cooperación con el presidente del Consejo Europeo, estableció una serie de principios guía para el levantamiento gradual de las medidas de confinamiento impuestas como consecuencia de la pandemia de COVID-19. Las aplicaciones para dispositivos móviles, y en particular las funcionalidades de rastreo de contactos, pueden desempeñar un papel importante en este contexto. Dependiendo de sus características y de la medida en que la población las utilice, esas aplicaciones pueden tener un efecto significativo en el diagnóstico, el tratamiento y la gestión de la COVID-19 dentro y fuera del ámbito hospitalario. Serán especialmente pertinentes cuando se levanten las medidas de confinamiento y el riesgo de infección aumente a medida que más y más personas entren en contacto. Esas aplicaciones pueden ayudar a interrumpir las cadenas de infección con mayor rapidez y eficacia que las medidas generales de confinamiento, así como reducir el riesgo de una propagación significativa del virus. Por consiguiente, deberían ser un elemento importante de la estrategia de salida y servir de complemento a otras medidas, como las dirigidas a reforzar las capacidades para realizar pruebas ([2]). La confianza es un requisito previo fundamental para el desarrollo de esas aplicaciones y su aceptación y adopción por parte de los ciudadanos. Estos tienen que tener la certeza de que el respeto de los derechos fundamentales está garantizado, de que las aplicaciones van a utilizarse exclusivamente para los fines específicamente definidos, de que no se van a emplear para la vigilancia a gran escala y de que las personas van a seguir teniendo el control de sus datos. Esta es la base en la que

([1]) Recomendación C(2020) 2296 final, de 8 de abril de 2020: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32020H0518&qid=1586969392762&from=ES.

([2]) https://ec.europa.eu/info/sites/info/files/communication_-_a_european_roadmap_to_lifting_coronavirus_containment_measures_0.pdf

se sustentan la precisión y la eficacia de este tipo de aplicaciones a la hora de contener la propagación del virus. Es, pues, esencial encontrar soluciones que sean lo menos intrusivas posible y cumplan plenamente los requisitos en materia de protección de los datos personales y la intimidad establecidos en el Derecho de la UE. Por otra parte, las aplicaciones han de desactivarse a más tardar cuando se declare que la pandemia está controlada. Las aplicaciones deberían incluir también los mecanismos más avanzados de seguridad de la información.

Las presentes orientaciones se han elaborado teniendo en cuenta la contribución del Comité Europeo de Protección de Datos (CEPD) ([3]) y los debates en el seno de la red de sanidad electrónica (eHealth). El CEPD tiene previsto publicar en los próximos días una serie de orientaciones sobre geolocalización y otras herramientas de rastreo en el contexto de la pandemia de COVID-19.

Ámbito cubierto por las orientaciones

Con objeto de garantizar un enfoque coherente en toda la UE y ofrecer orientaciones a los Estados miembros y los desarrolladores de aplicaciones, el presente documento determina las características y los requisitos que deberían reunir las aplicaciones para asegurar el cumplimiento de la legislación de la UE en materia de protección de la intimidad y los datos personales, en particular el Reglamento General de Protección de Datos ([4]) (RGPD) y la Directiva sobre la privacidad y las comunicaciones electrónicas ([5]). En las presentes orientaciones no se abordan otras condiciones, en particular las limitaciones que los Estados miembros pudieran haber incluido en su legislación nacional en lo que respecta al tratamiento de datos personales relativos a la salud.

Las presentes orientaciones no son jurídicamente vinculantes. Se entienden sin perjuicio del papel del Tribunal de Justicia de la UE, que es la única institución que puede interpretar de forma preceptiva el Derecho de la UE.

Las presentes orientaciones solo se refieren a aplicaciones de carácter voluntario para el apoyo a la lucha contra la pandemia de COVID-19 (aplicaciones descargadas, instaladas y utilizadas de forma voluntaria por los ciudadanos) que tengan una o varias de las funcionalidades siguientes:

— facilitar información exacta a las personas sobre la pandemia de COVID-19,

— ofrecer cuestionarios de autoevaluación y orientación a los ciudadanos (funcionalidad de comprobación de síntomas) ([6]),

— 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 (mayor recurso a la telemedicina).

En virtud de la Directiva sobre la privacidad y las comunicaciones electrónicas, la imposición del uso de una aplicación que interfiera con el derecho a la confidencialidad de las comunicaciones establecido en su artículo 5 solo es posible a través de una norma que sea necesaria, adecuada y proporcionada para proteger determinados objetivos específicos. Habida cuenta del alto grado de intrusión de un planteamiento de estas características y los desafíos que plantea, en particular por lo que respecta al establecimiento de salvaguardias adecuadas, la Comisión considera necesario proceder a un análisis riguroso antes de recurrir a esta opción. Por estas razones, la Comisión recomienda el uso de aplicaciones de carácter voluntario.

Las presentes orientaciones no contemplan las aplicaciones destinadas a controlar el cumplimiento de los requisitos de cuarentena (ni siquiera los obligatorios).

2. CONTRIBUCION DE LAS APLICACIONES A LA LUCHA CONTRA LA COVID-19

La función de comprobación de síntomas es una herramienta que permite a las autoridades sanitarias públicas proporcionar a los ciudadanos orientaciones sobre las pruebas de la COVID-19 e información sobre el autoaislamiento, la manera de evitar la transmisión a otras personas y el momento en que deben pedir asistencia sanitaria. Esa funcionalidad puede complementar también la vigilancia en el marco de la asistencia primaria y dar a conocer mejor el ritmo de transmisión de la COVID-19 entre la población.

([3]) https://edpb.europa.eu/sites/edpb/files/files/file1/edpbletterecadvisecodiv-appguidance_final.pdf

([4]) 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) (DO L 119 de 4.5.2016, p. 1).

([5]) 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) (DO L 201 de 31.7.2002, p. 37).

([6]) Si las aplicaciones proporcionan información relacionada con el diagnóstico, la prevención, el seguimiento, la predicción o el pronóstico, se debería determinar su posible calificación como productos sanitarios, de acuerdo con el marco regulador correspondiente. Por lo que se refiere al mencionado marco, véanse la Directiva 93/42/CEE del Consejo, de 14 de junio de 1993, relativa a los productos sanitarios (DO L 169 de 12.7.1993, p. 1) y el Reglamento (UE) 2017/745 del Parlamento Europeo y del Consejo, de 5 de abril de 2017, sobre los productos sanitarios (DO L 117 de 5.5.2017, p. 1).

Las funcionalidades de rastreo de contactos y alerta son herramientas que permiten identificar a las personas que han estado en contacto con alguien infectado por la COVID-19 e informarles de las medidas que conviene adoptar después, como someterse a autocuarentena o a pruebas, o proporcionar asesoramiento sobre qué hacer en caso de experimentar tal o cual síntoma. Esta funcionalidad es, pues, útil tanto para los ciudadanos como para las autoridades sanitarias públicas. También puede desempeñar un papel importante en la gestión de las medidas de confinamiento durante las posibles situaciones de desescalada. Su repercusión puede reforzarse mediante una estrategia que favorezca la ampliación de las pruebas a las personas que presenten síntomas leves.

Ambas funcionalidades pueden ser también una fuente pertinente de datos para las autoridades sanitarias públicas y facilitar la transmisión de ese tipo de datos a las autoridades epidemiológicas nacionales y al Centro Europeo para la Prevención y el Control de las Enfermedades (ECDC). Esto ayudaría a comprender los patrones de transmisión y, en combinación con los resultados de las pruebas, a estimar el valor predictivo positivo de los síntomas respiratorios en una comunidad dada y proporcionar información sobre el nivel de circulación del virus.

El grado de fiabilidad de las estimaciones depende directamente del número y fiabilidad de los datos transmitidos.

Por lo tanto, en combinación con las estrategias de pruebas adecuadas, tanto la funcionalidad de comprobación de síntomas como la de rastreo de contactos pueden proporcionar información sobre el nivel de circulación del virus y ayudar a determinar el efecto de las medidas de distanciamiento físico y de confinamiento. Tal como se establece en la Recomendación, para propiciar la colaboración transfronteriza y garantizar la detección de contactos entre los usuarios de distintas aplicaciones (lo cual es especialmente relevante en los movimientos transfronterizos de ciudadanos), debería garantizarse la interoperabilidad entre las soluciones informáticas de los distintos Estados miembros. Cuando una persona infectada entre en contacto con un usuario de una aplicación de otro Estado miembro, debería permitirse, en la medida de lo estrictamente necesario, la transmisión transfronteriza de datos personales de ese usuario a las autoridades sanitarias de su Estado miembro. La labor sobre esta cuestión se enmarcará en el conjunto de instrumentos anunciado en la Recomendación. La interoperabilidad debería garantizarse tanto mediante requisitos técnicos como mejorando la comunicación y la cooperación entre las autoridades sanitarias nacionales. También podría utilizarse un modelo de cooperación particular ([7]) como modelo de gobernanza para las aplicaciones de rastreo de contactos durante la pandemia de COVID-19.

3. ELEMENTOS PARA UN USO FIABLE Y RESPONSABLE DE LAS APLICACIONES

Las funcionalidades incluidas en las aplicaciones pueden tener distintas consecuencias en una amplia gama de derechos consagrados en la Carta de los Derechos Fundamentales de la UE, como la dignidad humana, el respeto de la vida privada y familiar, la protección de los datos personales, la libertad de circulación, la no discriminación, la libertad de empresa y la libertad de reunión y de asociación. La injerencia en la intimidad y el derecho a la protección de los datos personales pueden ser aspectos especialmente significativos, dado que algunas de las funcionalidades se basan en un modelo de uso intensivo de datos.

Los elementos que se exponen a continuación tienen por objeto servir de orientación sobre la manera de limitar la intrusión de las funcionalidades de las aplicaciones para garantizar el cumplimiento de la legislación de la UE en materia de protección de datos personales y de la intimidad.

3.1. Autoridades sanitarias nacionales (o entidades que realizan una misión que se lleva a cabo en favor del interés público en el ámbito de la salud) como responsables del tratamiento de datos

Determinar quién decide los medios y los fines del tratamiento de datos (el responsable del tratamiento) es crucial para establecer quién es responsable del cumplimiento de las normas de protección de datos personales de la UE, y en particular quién debería facilitar información a las personas que descargan la aplicación acerca del tratamiento de sus datos personales (ya existentes o que vayan a generarse a través del dispositivo, como un teléfono inteligente, en el que se instale la aplicación), cuáles van a ser sus derechos, quién va a ser responsable en caso de violación de la seguridad de los datos personales, etc.

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 ([8]). Esas autoridades o entidades son responsables del cumplimiento del RGPD (principio de responsabilidad proactiva). El alcance de ese acceso debería limitarse de acuerdo con los principios descritos en la sección 3.5.

([7]) Esa cooperación ya se ha establecido en relación con el proyecto MyHealth@EU para el intercambio de historiales resumidos de pacientes y recetas electrónicas. Véanse también el artículo 5, apartado 5, y el considerando 17 de la Decisión de Ejecución 2019/1765 de la Comisión.

([8]) Véase el considerando 45 del RGPD.

Esto también contribuirá a reforzar la confianza de los ciudadanos y, por ende, la aceptación de las aplicaciones (y de los sistemas subyacentes de información sobre cadenas de transmisión de infecciones), además de garantizar que estas cumplan el fin perseguido de protección de la salud pública. Las autoridades sanitarias nacionales responsables deberían armonizar y aplicar de una manera coordinada las políticas, requisitos y controles subyacentes.

3.2. **Garantizar que la persona siga teniendo el control**

Un factor determinante para que las personas confíen en las aplicaciones es hacerles ver que siguen teniendo el control de sus datos personales. Al efecto, la Comisión considera que deberían cumplirse, en particular, las condiciones siguientes:

— La instalación de la aplicación en el dispositivo debería ser voluntaria, sin consecuencia negativa alguna para quien decida no descargar o no usar la aplicación.

— No deberían agruparse las distintas funcionalidades de la aplicación (por ejemplo, información, comprobación de síntomas, rastreo de contactos y alerta), de manera que la persona pueda dar su consentimiento específicamente para cada una de ellas. Sin embargo, el usuario debería tener la posibilidad de combinar distintas funcionalidades de la aplicación si el proveedor lo ofrece como opción.

— En caso de usarse datos de proximidad [datos generados mediante el intercambio de señales de Bluetooth de baja energía (BLE) entre dispositivos dentro de una distancia relevante desde el punto de vista epidemiológico y durante un tiempo relevante también desde el punto de vista epidemiológico], tales datos deberían almacenarse en el dispositivo de la persona. Si se prevé compartir estos datos con las autoridades sanitarias, debería hacerse únicamente cuando se haya confirmado que la persona en cuestión está infectada de COVID-19 y a condición de que la persona opte por que así se haga.

— Las autoridades sanitarias deberían proporcionar a la persona toda la información necesaria en relación con el tratamiento de sus datos personales (en consonancia con los artículos 12 y 13 del RGPD y el artículo 5 de la Directiva sobre la privacidad y las comunicaciones electrónicas).

— La persona debería poder ejercer sus derechos en virtud del RGPD (en particular, de acceso, rectificación y supresión). Toda restricción de los derechos que se derivan del RGPD y la Directiva sobre la privacidad y las comunicaciones electrónicas debería estar en sintonía con esos instrumentos, además de ser necesaria y proporcionada y estar prevista en la legislación.

— Las aplicaciones deberían desactivarse a más tardar cuando se declare que la pandemia está controlada. La desactivación no debería depender de la desinstalación por parte del usuario.

3.3. **Base jurídica para el tratamiento**

Instalación de las aplicaciones y almacenamiento de información en el dispositivo del usuario

Como se ha señalado anteriormente, en virtud de la Directiva sobre la privacidad y las comunicaciones electrónicas (artículo 5), el almacenamiento de información en el dispositivo del usuario o la obtención de acceso a la información ya almacenada se permite únicamente si: i) el usuario ha dado su consentimiento, o ii) el almacenamiento o el acceso son estrictamente necesarios para el servicio de la sociedad de la información (por ejemplo, la aplicación) que el usuario ha solicitado de manera expresa (esto es, mediante la instalación y activación).

Normalmente, para que funcione una aplicación, es necesario almacenar información y obtener acceso a la información ya almacenada en el dispositivo de la persona. La funcionalidad de rastreo de contactos y alerta exige, además, el almacenamiento de otro tipo de información en el dispositivo del usuario (como alias efímeros y que se vayan modificando periódicamente de identificación de los usuarios de esta funcionalidad que se encuentren próximos). Por otra parte, esta funcionalidad podría requerir que el usuario (infectado o posiblemente infectado) cargase datos de proximidad. La carga de tales datos no es necesaria para el funcionamiento de la aplicación en sí misma. Por lo tanto, al no cumplirse los requisitos de la opción ii) antes mencionada, el consentimiento [opción i)] sería la justificación más adecuada para las actividades pertinentes. El consentimiento debería ser libre, específico, explícito e informado en el sentido del RGPD, manifestándose mediante una clara acción afirmativa de la persona, lo que excluye las formas de consentimiento tácito (por ejemplo, el silencio o la inacción) ([9]).

([9]) Véanse las Directrices del Comité Europeo de Protección de Datos sobre el consentimiento: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051

Base jurídica para el tratamiento por parte de las autoridades sanitarias nacionales (Derecho de la Unión o de un Estado miembro)

Normalmente, el tratamiento de datos personales por parte de las autoridades sanitarias nacionales tiene lugar cuando el Derecho de la Unión o de un Estado miembro recoge una obligación jurídica que prevé que así se haga, cumpliendo las condiciones del artículo 6, apartado 1, letra c), y del artículo 9, apartado 2, letra i), del RGPD, o cuando dicho tratamiento es necesario para la realización de una misión que se lleva a cabo en favor del interés público en virtud del Derecho de la Unión o del Estado miembro en cuestión ([10]).

Todo instrumento legislativo nacional ha de prever medidas específicas y adecuadas para salvaguardar los derechos y las libertades de los titulares de los datos. Por norma general, cuanto mayor sea la repercusión de cara a las libertades de la persona, mayores deben ser las correspondientes salvaguardias previstas en la legislación pertinente.

En principio, tanto la legislación de la UE y de los Estados miembros anterior al brote de COVID-19 como aquella que los Estados miembros están promulgando específicamente para luchar contra la propagación de epidemias podrían usarse como base jurídica para el tratamiento de datos personales si, en dicha legislación, se prevén medidas que autoricen el seguimiento de epidemias y se cumplen los demás requisitos del artículo 6, apartado 3, del RGPD.

Dada la naturaleza de los datos personales en cuestión (a saber, datos relativos a la salud como categoría especial de los datos personales), así como las circunstancias de la actual pandemia de COVID-19, apoyarse en la legislación como base jurídica contribuiría a la seguridad jurídica, pues: i) se prescribiría con detalle el tratamiento de datos específicos relativos a la salud y se especificaría claramente la finalidad del tratamiento; ii) se determinaría de forma clara quién es el responsable del tratamiento, esto es, la entidad que trata los datos, y quién, además del responsable del tratamiento, puede acceder a ellos; iii) se excluiría la posibilidad de que dichos datos fueran tratados con fines distintos de los recogidos en la legislación, y iv) se preverían garantías específicas. A fin de no socavar la utilidad y la aceptación públicas de las aplicaciones, es conveniente que el legislador nacional preste especial atención a que la solución elegida sea, con respecto a los ciudadanos, lo más inclusiva posible.

Que las autoridades sanitarias traten los datos sobre la base de la legislación no cambia el hecho de que las personas siguen siendo libres para decidir si instalan la aplicación y si comparten sus datos con estas autoridades. Por lo tanto, cuandoquiera que se desinstale la aplicación, no debería haber ninguna consecuencia negativa para el usuario.

Las aplicaciones de rastreo de contactos y alerta permiten alertar a las personas. En caso de que la aplicación emita directamente la alerta, la Comisión recuerda 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).

3.4. **Minimización de datos**

Los datos generados a través de dispositivos y almacenados previamente en ellos gozan de la protección siguiente:

— En cuanto que «datos personales», esto es, toda información sobre una persona física identificada o identificable (artículo 4, apartado 1, del RGPD), están protegidos en virtud del RGPD. Los datos relativos a la salud gozan de protección adicional (artículo 9 del RGPD).

— En cuanto que «datos de localización», esto es, datos tratados en una red de comunicaciones electrónicas, o por un servicio de comunicaciones electrónicas, que indican la posición geográfica del equipo terminal del usuario, están protegidos en virtud de la Directiva sobre la privacidad y las comunicaciones electrónicas (artículo 5, apartado 1, y artículos 6 y 9) ([11]).

— Toda la información almacenada en el equipo terminal del usuario y a la que se acceda desde dicho equipo está protegida en virtud del artículo 5, apartado 3, de la Directiva sobre la privacidad y las comunicaciones electrónicas.

Los datos no personales (por ejemplo, los datos anonimizados de forma irreversible) no están protegidos en virtud del RGPD.

La Comisión recuerda que el principio de minimización de datos exige que únicamente se traten los datos personales que sean adecuados, pertinentes y estrictamente necesarios en relación con los fines por los que se lleva a cabo el tratamiento ([12]). En vista del fin o los fines perseguidos, debería llevarse a cabo una valoración de la necesidad de tratar los datos personales y la pertinencia de tales datos personales.

La Comisión señala que, por ejemplo, si la finalidad de la funcionalidad es la comprobación de síntomas o la telemedicina, no se requiere acceder a la lista de contactos del propietario del dispositivo.

([10]) Artículo 6, apartado 1, letra e), del RGPD.

([11]) El Código de las Comunicaciones Electrónicas establece que también están cubiertos los servicios funcionalmente equivalentes a los servicios de comunicaciones electrónicas.

([12]) Principio de la minimización de datos.

Generar y tratar menos datos restringe los riesgos para la seguridad. Por consiguiente, el cumplimiento de las medidas de minimización de datos también proporciona garantías de seguridad.

— Funcionalidad de información:

Una aplicación que solo tenga esta funcionalidad no requerirá el tratamiento de ningún dato personal relacionado con la salud. Simplemente proporcionará información a la persona. Para cumplir esta finalidad, el tratamiento de los datos almacenados en el equipo terminal o a los que se acceda desde este se limitaría a lo necesario para proporcionar la información.

— Funcionalidades de comprobación de síntomas y de telemedicina:

Si la aplicación comprende una de estas funcionalidades o ambas, sí se tratarán datos personales relativos a la salud. Así pues, la legislación de base aplicable a las autoridades sanitarias debería establecer específicamente una lista de los datos que podrían tratarse.

Por otra parte, es posible que las autoridades sanitarias necesiten el número de teléfono de quienes hayan usado la comprobación de síntomas y cargado los resultados. El tratamiento de la información almacenada en el equipo terminal y a la que se acceda desde este quedaría limitado a lo necesario para el cometido y el funcionamiento de la aplicación.

— Funcionalidad de rastreo de contactos y de alerta:

La mayoría de las infecciones de COVID-19 se producen a través de gotitas que apenas recorren una corta distancia. Identificar cuanto antes a quienes hayan estado próximos a una persona infectada es un factor clave para interrumpir la cadena de infección. La proximidad decisiva se determina en función de la distancia y la duración de un contacto, y esa determinación debería hacerse desde el punto de vista epidemiológico. Interrumpir la cadena de infección reviste especial importancia a fin de evitar que se reproduzcan las infecciones en la fase de salida de la crisis.

Para ello, podrían necesitarse datos de proximidad. A efectos de medir la proximidad y los contactos estrechos, la comunicación entre dispositivos por Bluetooth de baja energía (BLE) parece ser más precisa y, por tanto, más apropiada que la utilización de los datos de geolocalización (GNSS/GPS o datos de localización de dispositivos móviles). Además, el BLE no permite el rastreo (a diferencia de los datos de geolocalización). Por consiguiente, la Comisión recomienda el uso de los datos de las comunicaciones por BLE (o datos generados por una tecnología equivalente) para determinar la proximidad.

Los datos de localización no son necesarios para los fines de las funcionalidades de rastreo de contactos, ya que su objetivo no es ni seguir los movimientos de las personas ni controlar el cumplimiento de las prescripciones. Además, el tratamiento de los datos de localización en el marco del rastreo de contactos sería difícilmente justificable a la luz del principio de minimización de datos y podría plantear cuestiones relacionadas con la seguridad y la intimidad. Es por ello que, en este contexto, la Comisión aconseja no usar los datos de localización.

Con independencia de los medios técnicos empleados para determinar la proximidad, no parece que sea necesario almacenar ni el momento exacto ni el lugar del contacto (si se dispone de esta información). Sin embargo, sí podría ser útil almacenar el día del contacto para saber si se produjo cuando la persona experimentaba síntomas (o cuarenta y ocho horas antes ([13])) y definir con mayor precisión el mensaje de seguimiento en el que se ofrezcan consejos relacionados, por ejemplo, con la duración de la autocuarentena.

Únicamente deberían generarse y tratarse datos de proximidad si hay un riesgo real de infección (en función de la cercanía y la duración del contacto).

Es preciso señalar que la necesidad y la proporcionalidad de la recopilación de datos dependerán, por tanto, de factores como la medida en que se disponga de laboratorios de pruebas, en particular cuando ya se hubieran ordenado medidas como el confinamiento. Hay dos formas de alertar a las personas que hayan estado en contacto estrecho con una persona infectada:

Un primer enfoque consiste en emitir automáticamente una alerta a través de la aplicación dirigida a quienes hayan estado en contacto estrecho con una persona que notifique a la aplicación (previa aprobación o confirmación de la autoridad sanitaria, por ejemplo, a través de un código QR o TAN) que ha dado positivo en las pruebas (tratamiento descentralizado). Preferiblemente, la autoridad sanitaria debería determinar el contenido del mensaje de alerta. Un segundo enfoque consiste en almacenar los identificadores temporales arbitrarios en un servidor propiedad de la autoridad sanitaria («solución de servidor final»). Estos datos no permiten identificar directamente a los usuarios. Mediante los identificadores, aquellos usuarios que hayan estado en contacto estrecho con un usuario que ha dado positivo en las pruebas reciben una alerta en su dispositivo. Si las autoridades sanitarias desean comunicarse con los usuarios que han estado en contacto estrecho con una persona infectada también a través de una llamada o un SMS, necesitarán que estos usuarios consientan en facilitar sus números de teléfono.

([13]) La persona infectada ya es contagiosa cuarenta y ocho horas antes de la aparición de los síntomas.

3.5. **Limitar el acceso a los datos y su divulgación**

— Funcionalidad de información:

No se puede compartir con las autoridades sanitarias ninguna información almacenada en el equipo terminal y a la que se acceda desde dicho equipo, aparte de la necesaria para disponer de esta funcionalidad. Dado que esta funcionalidad constituye únicamente el medio de comunicación, las autoridades sanitarias no tendrán acceso a ningún otro dato.

— Funcionalidades de comprobación de síntomas y de telemedicina:

La funcionalidad de comprobación de síntomas puede ser útil para que los Estados miembros orienten a los ciudadanos sobre la conveniencia de que se sometan a pruebas o les proporcionen información sobre el aislamiento y sobre cuándo y cómo obtener asistencia sanitaria, en particular a los grupos de riesgo. Esta funcionalidad también puede complementar la vigilancia de la asistencia primaria y contribuir a que se comprenda cuáles son los índices de infección de la COVID-19 en la población. Por consiguiente, puede decidirse que las autoridades sanitarias competentes y las autoridades epidemiológicas nacionales tengan acceso a la información facilitada por el paciente. El ECDC podría recibir datos agregados de las autoridades nacionales a efectos de vigilancia epidemiológica.

Si se opta por permitir el contacto con los agentes sanitarios, y no un mero contacto a través de la propia aplicación, entonces también será necesario revelar a las autoridades sanitarias nacionales el número de teléfono de los usuarios de la aplicación.

— Funcionalidad de rastreo de contactos y de alerta:

— Datos de la persona infectada

Las aplicaciones generan, de manera pseudoaleatoria, identificadores efímeros y que cambian periódicamente de los teléfonos que están en contacto con el usuario. Una opción es que los identificadores se almacenen en el dispositivo del usuario (el denominado «tratamiento descentralizado»). Otra opción puede ser que esos identificadores arbitrarios se almacenen en un servidor al que tengan acceso las autoridades sanitarias (la denominada «solución de servidor final»). La solución descentralizada está más en consonancia con el principio de minimización. Las autoridades sanitarias únicamente deberían tener acceso a los datos de proximidad procedentes del dispositivo de la persona infectada de manera que puedan ponerse en contacto con las personas que hayan corrido el riesgo de infectarse.

Tales datos solo estarían a disposición de las autoridades sanitarias después de que la persona infectada (tras haber sido sometida a pruebas) los hubiera compartido de manera proactiva con ellas.

La persona infectada no debería ser informada de la identidad de las personas con las que haya podido tener un contacto epidemiológicamente relevante y que serán alertadas.

— Datos de las personas que han estado en contacto (epidemiológico) con la persona infectada

La identidad de la persona infectada no debería revelarse a las personas con las que haya estado en contacto epidemiológico. Es suficiente que se les comunique que han estado en contacto epidemiológico con una persona infectada en los últimos dieciséis días. Como se ha señalado anteriormente, los datos sobre el momento y el lugar de tales contactos no deberían almacenarse. Por consiguiente, no es necesario ni posible comunicar dichos datos.

Para rastrear los contactos epidemiológicos del usuario de la aplicación cuyo estado infeccioso se haya constatado, las autoridades sanitarias nacionales únicamente deberían ser informadas del identificador de las personas con las que el infectado haya estado en contacto epidemiológico desde cuarenta y ocho horas antes de la aparición de los síntomas hasta catorce días después de su aparición, sobre la base de la proximidad y la duración del contacto.

El ECDC podría recibir datos agregados de rastreo de contactos de las autoridades nacionales a efectos de vigilancia epidemiológica atendiendo a una serie de indicadores definidos en colaboración con los Estados miembros.

3.6. **Tratamiento de los datos con fines precisos**

La base jurídica (legislación de la Unión prever la finalidad del tratamiento. El fin debería ser explícito y específico, de modo que no quepa duda sobre la clase de datos personales que se han de tratar a fin de alcanzar el objetivo deseado.

El fin o los fines exactos dependerán de las funcionalidades de la aplicación. Cada una de las distintas funcionalidades de una aplicación puede obedecer a varios fines. Para que las personas tengan pleno control sobre sus datos, la Comisión recomienda no agrupar diferentes funcionalidades. En cualquier caso, la persona debería tener la posibilidad de elegir entre diferentes funcionalidades que persigan individualmente un fin distinto.

La Comisión aconseja que no se utilicen los datos recogidos en las condiciones mencionadas para fines distintos a los de la lucha contra la COVID-19. Cuando sea necesario atender a fines como los de la investigación científica y las estadísticas, deberían incluirse en la lista original de fines y comunicarse claramente a los usuarios.

— Funcionalidad de información:

El fin de esta funcionalidad es proporcionar la información que sea pertinente desde el punto de vista de las autoridades sanitarias en el contexto de la crisis.

— Funcionalidades de comprobación de síntomas y de telemedicina:

La función de comprobación de síntomas puede ofrecer una indicación de qué proporción de las personas que presentan síntomas compatibles con la COVID-19 está realmente infectada (por ejemplo, sometiendo a todos a frotis y pruebas o en función de un número aleatorio de personas con tales síntomas, si hay capacidad para proceder así). La especificación de la finalidad debería dejar claro que los datos sanitarios personales serán procesados para: i) ofrecer a la persona la posibilidad de valorar por sí misma, basándose en una serie de preguntas, si ha desarrollado los síntomas de la COVID-19, o ii) recibir asesoramiento médico si se han desarrollado los síntomas de la COVID-19.

— Funcionalidades de rastreo de contactos y de alerta:

La mera indicación de la finalidad de «prevención de nuevas infecciones de COVID-19» no es suficientemente específica. En este caso, la Comisión recomienda especificar en mayor medida los fines en consonancia con lo siguiente: «mantener los contactos de las personas que utilizan la aplicación y que pueden haber estado expuestas a la infección de la COVID-19 con el fin de alertar a aquellas que podrían haber sido infectadas».

3.7. **Establecimiento de límites estrictos al almacenamiento de datos**

El principio de limitación del almacenamiento exige que los datos personales no se conserven durante más tiempo del necesario. Los plazos deberían basarse en la importancia médica (dependiendo de la finalidad de la aplicación: el período de incubación, etc.) y en lapsos realistas para las medidas administrativas que si acaso deban tomarse.

— Funcionalidad de información:

Cualquier dato que se recoja al instalar esta funcionalidad debe suprimirse inmediatamente. No hay justificación para mantener esos datos.

— Funcionalidades de comprobación de síntomas y de telemedicina:

Las autoridades sanitarias deberían suprimir estos 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. Las autoridades sanitarias podrán conservar los datos durante períodos más largos a efectos de información sobre la vigilancia e investigación, siempre que se conserve en un formato anonimizado.

— Funcionalidades de rastreo de contactos y de alerta:

Los datos de proximidad deberían suprimirse tan pronto como dejen de ser necesarios para alertar a las personas. Deberían suprimirse 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. Las autoridades sanitarias podrán conservar los datos de proximidad durante períodos más largos a efectos de información sobre la vigilancia e investigación, siempre que se conserve en un formato anonimizado.

Los datos deberían almacenarse en el dispositivo del usuario, y solo aquellos que hayan sido comunicados por los usuarios y que sean necesarios para cumplir la finalidad deberían cargarse en el servidor a disposición de las autoridades sanitarias cuando se haya elegido tal opción (es decir, solo se cargarían los datos en el servidor de «contactos estrechos» de una persona que hubiera dado positivo a la infección de COVID-19).

3.8. **Garantizar la seguridad de los datos**

La Comisión recomienda que los datos se almacenen en el dispositivo terminal de la persona de forma cifrada utilizando las técnicas criptográficas más avanzadas. En caso de que los datos se almacenen en un servidor central, el acceso a dicho servidor, incluido el acceso administrativo, debería estar sujeto a registro previo.

Los datos de proximidad solo deberían generarse y almacenarse en el dispositivo terminal de la persona en un formato cifrado y pseudonimizado. Para garantizar que se excluya el rastreo por terceros, la activación de Bluetooth debería ser posible sin tener que activar otros servicios de localización.

Durante la recogida de datos de proximidad mediante BLE es preferible ir creando y almacenando identificadores temporales del usuario que vayan cambiando periódicamente, en lugar de almacenar el identificador real del dispositivo. Este proceder brinda una mayor protección contra las escuchas y el rastreo por parte de piratas informáticos, por lo que dificulta la identificación de las personas.

La Comisión recomienda que el código fuente de la aplicación se haga público y esté disponible para su revisión.

Cabe contemplar medidas adicionales para garantizar la seguridad de los datos objeto de tratamiento, en particular su anonimización o supresión automática transcurrido un plazo determinado. En general, el grado de seguridad debería estar en consonancia con el volumen y la sensibilidad de los datos personales tratados.

Todas las transmisiones desde el dispositivo personal a las autoridades sanitarias nacionales deberían cifrarse.

Cuando la legislación nacional establezca que los datos personales recogidos también pueden tratarse con fines de investigación científica, se debería utilizar, en principio, la pseudonimización.

3.9. **Garantizar la exactitud de los datos**

Garantizar la exactitud de los datos personales tratados no es solo un requisito previo para la eficiencia de la aplicación, sino también una obligación en virtud de la legislación en materia de protección de datos personales.

En este contexto, es esencial garantizar la exactitud de la información sobre si se ha producido efectivamente un contacto con una persona infectada (distancia y duración epidemiológicas), a fin de minimizar el riesgo de que se generen falsos positivos. Aquí se deberían contemplar las situaciones en las que dos usuarios de la aplicación estén en contacto en la calle, en el transporte público o en un edificio. Es poco probable que el uso de datos de localización basados en las redes de telefonía móvil sea lo suficientemente preciso a tal efecto.

Por lo tanto, es aconsejable basarse en tecnologías que permitan una evaluación más precisa del contacto (por ejemplo, Bluetooth).

3.10. **Involucrar a las autoridades de protección de datos**

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. Dado que el tratamiento de datos en el contexto de la aplicación se considerará un tratamiento a gran escala de categorías especiales de datos (datos relativos a la salud), la Comisión remite al artículo 35 del RGPD, sobre la evaluación de impacto relativa a la protección de datos.