Directrices

Directrices 04/2020 sobre el uso de datos de localización y herramientas de rastreo de contactos en el contexto de la pandemia de COVID-19

Adoptadas el 21 de abril de 2020

Translations proofread by EDPB Members.
This language version has not yet been proofread.

Historial de versiones

Versión 1.1	5 de mayo de 2020	Correcciones menores
Versión 1.0	21 de abril de 2020	Adopción de las Directrices

Índice

El Comité Europeo de Protección de Datos

Visto el artículo 70, apartado 1, letra e), 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 (en lo sucesivo, «RGPD»),

Visto el Acuerdo EEE, y en particular su anexo XI y su Protocolo 37, modificado por la Decisión n.º 154/2018 del Comité Mixto del EEE, de 6 de julio de 2018[1],

Vistos el artículo 12 y el artículo 22 de su Reglamento interno,

HA ADOPTADO LAS SIGUIENTES DIRECTRICES:

1. INTRODUCCIÓN Y CONTEXTO

1. Los gobiernos y el sector privado están dirigiendo su mirada hacia el uso de soluciones basadas en los datos como parte de la respuesta a la pandemia de COVID-19, lo que plantea muchos interrogantes desde el punto de vista de la privacidad.
2. El CEPD subraya que el marco jurídico de la protección de datos fue diseñado como un instrumento flexible que, por tanto, puede aportar una respuesta eficiente en la contención de la pandemia y, al mismo tiempo, proteger los derechos humanos y las libertades fundamentales.
3. El CEPD está firmemente convencido de que, en la medida en que el tratamiento de datos personales resulte necesario para la gestión de la pandemia de COVID-19, la protección de datos será imprescindible para generar confianza y sentar las condiciones para la aceptación social de cualquier solución y, así, garantizar la eficacia de las medidas adoptadas. Como el virus no conoce fronteras, parece preferible adoptar un enfoque europeo común en respuesta a la crisis actual o, por lo menos, establecer un marco interoperable.
4. Por lo general, el CEPD considera que los datos y la tecnología empleados para contribuir a la lucha contra la COVID-19 deben utilizarse para empoderar, más que para controlar, estigmatizar o reprimir a los ciudadanos. Además, aunque los datos y la tecnología pueden ser herramientas importantes, tienen limitaciones intrínsecas y tan solo pueden potenciar la eficacia de otras medidas de salud pública. Los principios generales de eficacia, necesidad y proporcionalidad deben dirigir cualquier medida adoptada por los Estados miembros o las instituciones de la UE que implique el tratamiento de datos personales para combatir la COVID-19.
5. Las presentes directrices precisan las condiciones y los principios que deben guiar el uso proporcionado de datos de localización y de herramientas de rastreo de contactos para dos fines específicos, a saber:
   - el uso de datos de localización para apoyar la respuesta a la pandemia mediante la modelización de la propagación del virus, a fin de evaluar la eficacia global de las medidas de confinamiento;

1 Las referencias a los «Estados miembros» en el presente documento se entenderán hechas a los «Estados miembros del EEE».

- el rastreo de contactos, cuyo objetivo es que las personas que hayan estado muy cerca de alguien que resulte ser un portador confirmado del virus sean informadas al respecto, a fin de romper las cadenas de transmisión lo antes posible.

6. La eficiencia de la contribución de una aplicación de rastreo de contactos a la gestión de la pandemia depende de muchos factores (p. ej., del porcentaje de personas que deban instalarla o de la definición de «contacto» en términos de proximidad y duración). Además, esas aplicaciones deben formar parte de una estrategia global de salud pública dirigida a combatir la pandemia que incluya, entre otras cosas, la realización de pruebas de detección y el subsiguiente rastreo manual de contactos para eliminar dudas. Su despliegue ha de completarse con una serie de medidas de apoyo que garanticen la contextualización de la información facilitada a los usuarios y la utilidad de las alertas para la sanidad pública. De no ser así, esas aplicaciones podrían no surtir todos los efectos deseados.

7. El CEPD hace hincapié en que tanto el RGPD como la Directiva 2002/58/CE (en lo sucesivo, «la Directiva») contienen normas específicas que permiten la utilización de datos anónimos o personales para apoyar a las autoridades públicas y otros agentes nacionales y de la UE en el seguimiento y la contención de la propagación del virus SARS-CoV-2[2].

8. A este respecto, el CEPD ya se ha pronunciado sobre el hecho de que el uso de aplicaciones de rastreo de contactos debe ser voluntario y no puede basarse en el rastreo de movimientos individuales, sino más bien en información sobre la proximidad de los usuarios[3].

[2] Véase la declaración previa del CEPD sobre el brote de COVID-19.
[3] https://edpb.europa.eu/sites/edpb/files/files/file1/edpbletterecadvisecodiv-appguidance_final.pdf

2. USO DE DATOS DE LOCALIZACIÓN

2.1. Fuentes de datos de localización

9. Hay dos fuentes principales de datos de localización disponibles para modelizar la propagación del virus y la eficacia global de las medidas de confinamiento:
   - los datos de localización recogidos por proveedores de servicios de comunicaciones electrónicas (como los operadores de comunicaciones móviles) en el contexto de la prestación de sus servicios; y
   - los datos de localización recogidos por las aplicaciones de los proveedores de servicios de la sociedad de la información cuya funcionalidad requiere el uso de dichos datos (aplicaciones de navegación, servicios de transporte, etc.).

10. El CEPD recuerda que el tratamiento de los datos de localización[4] obtenidos de los proveedores de servicios de comunicaciones electrónicas está sujeto a los límites de los artículos 6 y 9 de la Directiva. Esto significa que esos datos solo pueden transmitirse a las autoridades o a terceros si han sido anonimizados por el proveedor o, en el caso de los datos que indican la posición geográfica del equipo terminal de un usuario, que no son datos de tráfico, si se cuenta con el consentimiento previo de los usuarios[5].

11. En cuanto a la información, incluidos los datos de localización, obtenida directamente de los equipos terminales, es de aplicación el artículo 5, apartado 3, de la Directiva. Así, el almacenamiento de información en el dispositivo del usuario o la obtención de acceso a la información ya almacenada solo se permite cuando i) el usuario haya dado su consentimiento[6], o cuando ii) el almacenamiento y/o acceso sea estrictamente necesario para la prestación del servicio de la sociedad de la información expresamente solicitado por el usuario.

12. No obstante, cabe establecer excepciones a los derechos y obligaciones contemplados en la Directiva en virtud de su artículo 15, cuando constituyan una medida necesaria, adecuada y proporcionada en una sociedad democrática para cumplir determinados objetivos[7].

13. La reutilización de datos de localización recogidos por un proveedor de servicios de la sociedad de la información a efectos de modelización (por ejemplo, a través del sistema operativo o de alguna aplicación previamente instalada) exige el cumplimiento de condiciones adicionales. En efecto, cuando los datos se han recogido de conformidad con el artículo 5, apartado 3, de la Directiva, solo pueden someterse a tratamiento ulterior con el consentimiento adicional del interesado o sobre la base de una disposición de la Unión o del Estado miembro que constituya una medida necesaria y proporcionada en una sociedad democrática para proteger los objetivos a que se refiere el artículo 23, apartado 1, del RGPD[8].

2.2. Prioridad al uso de datos de localización anonimizados

14. El CEPD señala que, a la hora de utilizar datos de localización, debe darse siempre preferencia al tratamiento de datos anonimizados, en lugar de datos personales.

15. Por anonimización se entiende el uso de un conjunto de técnicas destinadas a suprimir la capacidad de asociar los datos a una persona física identificada o identificable mediante un esfuerzo «razonable». Esta «prueba de razonabilidad» debe tener en cuenta tanto los aspectos

---

[4] Véase el artículo 2, letra c), de la Directiva.
[5] Véanse los artículos 6 y 9 de la Directiva.
[6] El concepto de consentimiento recogido en la Directiva se corresponde con el recogido en el RGPD y está sujeto al cumplimiento de todos los requisitos del consentimiento previstos en el artículo 4, punto 11, y en el artículo 7 de este Reglamento.
[7] En relación con la interpretación del artículo 15 de la Directiva, véase también la sentencia del TJUE de 29 de enero de 2008 en el asunto C-275/06, Productores de Música de España (Promusicae) / Telefónica de España SAU.
[8] Véase la sección 1.5.3 de las Directrices 1/2020 sobre el tratamiento de datos personales en el contexto de los vehículos conectados.

objetivos (tiempo, medios técnicos) como los elementos contextuales, que pueden variar de un caso a otro (carácter excepcional de un fenómeno teniendo en cuenta, por ejemplo, la densidad de la población y la naturaleza y volumen de los datos). Si los datos no superan esta prueba, no se han anonimizado y, por tanto, se mantienen dentro del ámbito de aplicación del RGPD.

16. La evaluación de la consistencia de la anonimización depende de tres criterios: i) singularización (identificación de una persona dentro de un grupo mayor sobre la base de los datos); ii) vinculación (vinculación de dos registros de datos sobre la misma persona); y iii) inferencia (deducción, con una probabilidad significativa, de información desconocida sobre una persona).

17. El concepto de anonimización tiende a ser malinterpretado y suele confundirse con la seudonimización. La anonimización permite utilizar los datos sin ninguna restricción, mientras que los datos seudonimizados siguen entrando en el ámbito de aplicación del RGPD.

18. Existen muchas opciones para una anonimización eficaz[9], pero con una salvedad. No se pueden anonimizar datos aislados, es decir, solo se pueden anonimizar (o no) series de datos completas. En este sentido, toda intervención en un patrón de datos único (mediante cifrado o cualquier otra transformación matemática) puede calificarse como máximo de seudonimización.

19. Los procesos de anonimización y los ataques de reidentificación son ámbitos de investigación dinámicos. Es crucial que todo responsable del tratamiento que aplique soluciones de anonimización se mantenga al corriente de las últimas novedades en este campo, especialmente en lo relativo a los datos de localización (procedentes de operadores de telecomunicaciones o de servicios de la sociedad de la información), cuya especial dificultad de anonimización es bien conocida.

20. De hecho, un amplio corpus de investigación revela[10] la existencia de *datos que se creían anonimizados* y que en la práctica podrían no estarlo. Los rastros de los movimientos de las personas están de forma intrínseca muy relacionados entre sí y son únicos. Por tanto, en determinadas circunstancias pueden ser vulnerables a los intentos de reidentificación.

21. Un patrón de datos único que rastree la localización de una persona durante un período de tiempo significativo no puede ser anonimizado por completo. Esta consideración posiblemente siga siendo válida si la precisión de las coordenadas geográficas registradas no se reduce en una medida suficiente, o si se suprimen los pormenores del itinerario, e incluso si solo se retiene la localización de los lugares en los que el interesado permanece durante cantidades importantes de tiempo. Lo mismo sucede con los datos de localización mal agregados.

22. Para conseguir la anonimización, el tratamiento de los datos de localización ha de ser cuidadoso para superar la prueba de razonabilidad. Se trata, en este sentido, de considerar series de datos de localización en su conjunto, así como de tratar datos de un conjunto de personas razonablemente amplio utilizando técnicas de anonimización disponibles que sean consistentes, siempre y cuando se apliquen de forma adecuada y efectiva.

23. Por último, dada la complejidad de los procesos de anonimización, se recomienda encarecidamente la transparencia en lo que respecta a la metodología de anonimización.

---

[9] De Montjoye y otros (2018) «On the privacy-conscientious use of mobile phone data».
[10] De Montjoye y otros (2013) «Unique in the Crowd: The privacy bounds of human mobility», y Pyrgelis y otros (2017) «Knock, Who's There? Membership Inference on Aggregate Location Data».

3. APLICACIONES DE RASTREO DE CONTACTOS

3.1. Análisis jurídico general

24. El seguimiento sistemático y masivo de la localización o los contactos de las personas físicas es una grave injerencia en su privacidad. Esta práctica solo puede legitimarse sobre la base de su adopción voluntaria por parte de los usuarios para cada uno de los fines respectivos, lo que implica, entre otras cosas, que las personas que decidan no utilizar esas aplicaciones, o no sepan hacerlo, no deben sufrir ninguna desventaja.

25. Para garantizar la rendición de cuentas, debe definirse con claridad quiénes son los responsables del tratamiento de datos en este tipo de aplicaciones. En opinión del CEPD, podrían serlo[11] las autoridades sanitarias nacionales, aunque cabe prever también otras fórmulas. En todo caso, si el despliegue de aplicaciones de rastreo de contactos implica a diferentes agentes, es importante que sus funciones y responsabilidades estén claramente delimitadas desde el principio y que se expliquen a los usuarios.

26. Además, en relación con el principio de limitación de la finalidad, las finalidades deben ser lo suficientemente específicas como para excluir un tratamiento ulterior con fines ajenos a la gestión de la crisis sanitaria de la COVID-19 (p. ej., para fines comerciales o coercitivos). Una vez definido con claridad el objetivo, será necesario velar por que el uso de datos personales sea adecuado, necesario y proporcionado.

27. En estas aplicaciones conviene prestar especial atención al principio de minimización de datos y a la protección de datos desde el diseño y por defecto:
    - las aplicaciones de rastreo de contactos no requieren un seguimiento de la ubicación de los usuarios a título individual; en su lugar, deben utilizarse datos de proximidad;
    - como se trata de aplicaciones que pueden funcionar sin la identificación directa de personas, conviene establecer medidas adecuadas para prevenir la reidentificación;
    - la información recogida debe alojarse en el equipo terminal del usuario y solo debe recogerse la información pertinente cuando sea absolutamente necesario.

28. En cuanto a la legalidad del tratamiento, el CEPD señala que las aplicaciones de rastreo de contactos implican el almacenamiento de información y/o el acceso a datos ya almacenados en el equipo terminal, que están sujetos al artículo 5, apartado 3, de la Directiva. Si tales operaciones son estrictamente necesarias para que el proveedor de la aplicación preste el servicio solicitado explícitamente por el usuario, el tratamiento no requerirá su consentimiento. En el caso de las operaciones que no sean estrictamente necesarias, el proveedor deberá pedir el consentimiento del usuario.

29. Además, el CEPD considera que el mero hecho de que el uso de tales aplicaciones tenga carácter voluntario no significa que el tratamiento de datos personales se base necesariamente en el consentimiento. Cuando las autoridades públicas prestan un servicio basado en un mandato atribuido por la legislación y acorde con los requisitos legales vigentes, la base jurídica más adecuada para el tratamiento de datos es la necesidad de cumplir una misión de interés público, es decir, el artículo 6, apartado 1, letra e), del RGPD.

30. El artículo 6, apartado 3, del RGPD precisa que la base del tratamiento indicado en el artículo 6, apartado 1, letra e), debe ser establecida por el Derecho de la Unión o el Derecho de los Estados miembros que se aplique al responsable del tratamiento. La finalidad del tratamiento debe estar fijada en dicha base jurídica o, en lo relativo al tratamiento a que se refiere el apartado 1, letra e), debe ser necesaria para el cumplimiento de una misión realizada

[11] Véase también el documento de la Comisión Europea «Orientaciones sobre las aplicaciones móviles de apoyo a la lucha contra la pandemia de COVID-19 en lo referente a la protección de datos», Bruselas, 16 de abril de 2020, C(2020) 2523 final.

en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento[12].

31. Ahora bien, la base jurídica o medida legislativa que proporcione la base legítima para el uso de aplicaciones de rastreo de contactos debe incorporar salvaguardias significativas, incluida una referencia al carácter voluntario de la aplicación. Procede incluir una especificación clara de la finalidad y limitaciones explícitas respecto a la utilización ulterior de datos personales, y debe identificarse con claridad al responsable o los responsables del tratamiento. También deben definirse las categorías de datos y las entidades a las que pueden transmitirse los datos personales, y para qué fines. En función del nivel de interferencia, conviene incorporar salvaguardias adicionales, teniendo en cuenta la naturaleza, el alcance y los fines del tratamiento. Por último, el CEPD recomienda que, en la medida de lo posible, se incluyan los criterios que determinen cuándo se desmantelará la aplicación y qué entidad será responsable de esa determinación y rendirá cuentas al respecto.

32. No obstante, si el tratamiento de datos se apoya en un fundamento jurídico distinto, como, por ejemplo, el consentimiento [artículo 6, apartado 1, letra a)][13], el responsable del tratamiento tendrá la obligación de velar por que se cumplan los estrictos requisitos necesarios para dotar de validez a ese fundamento jurídico.

33. Además, el uso de una aplicación para combatir la pandemia de COVID-19 podría llevar a la recogida de datos sanitarios (por ejemplo, sobre el estado de una persona infectada). El tratamiento de estos datos está permitido cuando es necesario por razones de interés público en el ámbito de la salud pública y, por tanto, se cumplen las condiciones del artículo 9, apartado 2, letra i), del RGPD[14], o para los fines de asistencia sanitaria descritos en su artículo 9, apartado 2, letra h)[15]. Dependiendo de la base jurídica, el tratamiento podría fundamentarse también en el consentimiento explícito [artículo 9, apartado 2, letra a), del RGPD].

34. De conformidad con la finalidad inicial, el artículo 9, apartado 2, letra j), del RGPD también permite el tratamiento de datos sanitarios cuando resulte necesario para fines de investigación científica o fines estadísticos.

35. La crisis sanitaria actual no ha de servir de oportunidad para establecer mandatos desproporcionados de conservación de datos. En la limitación del almacenamiento han de considerarse las necesidades reales y la importancia médica (que puede incluir consideraciones epidemiológicas como el período de incubación, etc.), y los datos personales solo deben conservarse durante la crisis de la COVID-19. Después, como regla general, todos los datos personales deberían borrarse o anonimizarse.

36. El CEPD entiende que esas aplicaciones no pueden sustituir, sino meramente apoyar, el rastreo manual de contactos realizado por personal sanitario cualificado, que puede determinar si los contactos estrechos pueden o no dar lugar a una transmisión del virus (p. ej., cuando se interactúa con una persona protegida —o no— por un equipo adecuado, como puede ser el cajero de un establecimiento comercial). El CEPD subraya que los procedimientos y procesos ejecutados por las aplicaciones de rastreo de contactos, incluidos sus respectivos algoritmos, han de estar sujetos a una estricta supervisión por parte de personal cualificado, a fin de limitar la aparición de falsos positivos y negativos. En concreto, la labor de facilitar asesoramiento sobre los pasos que han de darse a continuación no puede depender exclusivamente de un tratamiento automatizado.

---

[12] Véase el considerando 41.

[13] Los responsables del tratamiento (especialmente, las autoridades públicas) han de prestar especial atención al hecho de que no debe considerarse que el consentimiento se ha dado libremente si el interesado no tiene la posibilidad real de denegar o retirar su consentimiento sin verse perjudicado.

[14] El tratamiento debe basarse en el Derecho de la Unión o de los Estados miembros que establezca medidas adecuadas y específicas para proteger los derechos y libertades del interesado, en particular, el secreto profesional.

[15] Véase el artículo 9, apartado 2, letra h), del RGPD.

37. Para asegurar su equidad, la rendición de cuentas y, más en general, su consonancia con la ley, los algoritmos deben ser auditables y han ser revisados periódicamente por expertos independientes. El código fuente de la aplicación debe hacerse público con miras a un control lo más amplio posible.

38. Hasta cierto punto, siempre aparecerán falsos positivos. Teniendo en cuenta que, probablemente, la identificación de un riesgo de infección tendrá repercusiones significativas para la persona afectada, como la de mantenerse aislada hasta dar negativo en una prueba de detección, la capacidad de corregir datos y/o de realizar los consiguientes análisis es necesaria. Lógicamente, esto solo debe aplicarse a los escenarios y usos en los cuales los datos se tratan y/o almacenan de tal manera que este tipo de corrección es técnicamente viable y en los que es probable que se produzcan los efectos adversos arriba mencionados.

39. Por último, el CEPD considera que ha de llevarse a cabo una evaluación de impacto relativa a la protección de datos (EIPD) antes de empezar a utilizar una aplicación de este tipo por cuanto se considera que el tratamiento puede entrañar un alto riesgo (datos sanitarios, adopción previa a gran escala, seguimiento sistemático, utilización de una nueva solución tecnológica)[16]. El CEPD recomienda encarecidamente la publicación de las EIPD.

3.2. Recomendaciones y requisitos funcionales

40. De acuerdo con el principio de minimización de datos, además de cumplir otras medidas de la protección de datos desde el diseño y por defecto[17], los datos objeto de tratamiento deben reducirse a los mínimos estrictamente necesarios. La aplicación no debe recoger información que no tenga relación con el objeto específico o no sea necesaria — por ejemplo, estado civil, identificadores de las comunicaciones, elementos del directorio del equipo, mensajes, registros de llamadas, datos de localización, identificadores de dispositivos, etc.—.

41. Los datos difundidos por las aplicaciones solo deben incluir algunos identificadores únicos y seudónimos, generados por la aplicación y específicos de esta. Esos identificadores deben renovarse periódicamente, con una frecuencia compatible con el propósito de contener la propagación del virus y suficiente para limitar el riesgo de identificación y de rastreo físico de personas.

42. Las aplicaciones de rastreo de contactos pueden seguir un enfoque centralizado o descentralizado[18]. Ambos deben considerarse opciones válidas, siempre que se establezcan medidas de seguridad adecuadas, pues los dos presentan una serie de ventajas y desventajas. Así, la fase conceptual del desarrollo de aplicaciones debe incluir en todos los casos una consideración exhaustiva de ambos modelos que pondere cuidadosamente sus respectivos efectos en la protección de datos y la privacidad y sus posibles repercusiones en los derechos individuales.

43. Todo servidor que participe en el sistema de rastreo de contactos debe limitarse a recoger el historial de contactos o los identificadores seudónimos de un usuario que haya sido diagnosticado como infectado como resultado de una evaluación adecuada realizada por las autoridades sanitarias y de una acción voluntaria del usuario. Como alternativa, el servidor debe conservar una lista de identificadores seudónimos de usuarios infectados o su historial de contactos únicamente durante el tiempo necesario para informar de su exposición a los usuarios que puedan haber sido infectados, sin tratar de identificarles.

44. La implantación de una metodología global de rastreo de contactos que incluya tanto estas aplicaciones como el rastreo manual podría requerir en algunos casos el tratamiento de

[16] Véanse las Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento «entraña probablemente un alto riesgo» a efectos del Reglamento (UE) 2016/679, Grupo de Trabajo del Artículo 29.
[17] Véanse las Directrices 4/2019 del CEPD sobre la protección de datos desde el diseño y por defecto.
[18] En general, la solución descentralizada está más en consonancia con el principio de minimización.

información adicional. En este contexto, esa información adicional debe permanecer en el equipo terminal del usuario y solo puede ser objeto de tratamiento cuando resulte estrictamente necesario y con su consentimiento previo y específico.

45. Deben aplicarse las técnicas criptográficas más avanzadas para garantizar la seguridad de los datos almacenados en los servidores y aplicaciones y los intercambios entre las aplicaciones y el servidor remoto. También conviene proceder a la autenticación mutua entre la aplicación y el servidor.

46. La notificación de los usuarios infectados de SARS-CoV-2 en la aplicación debe someterse a una autorización adecuada, por ejemplo, mediante un código de un solo uso unido a una identidad seudónima de la persona infectada y vinculado con un laboratorio de pruebas de detección o con un profesional de atención sanitaria. Si no se puede obtener confirmación de forma segura, no debe tener lugar ningún tratamiento de datos que presuponga la validez del estado del usuario.

47. El responsable del tratamiento, en colaboración con las autoridades públicas, tiene que facilitar información clara y explícita sobre el enlace que permita descargar la aplicación oficial nacional de rastreo de contactos, con el fin de mitigar el riesgo de que se utilicen aplicaciones de terceros.

4. CONCLUSIÓN

48. El mundo se enfrenta a una grave crisis de salud pública que exige respuestas contundentes cuyo impacto trascenderá a esta emergencia. El tratamiento automatizado de datos y las tecnologías digitales pueden ser componentes esenciales de la lucha contra la COVID-19. No obstante, debemos ser cautelosos con el carácter irreversible de ciertas medidas. Es nuestra responsabilidad garantizar que cada una de las medidas adoptadas en estas circunstancias extraordinarias sea necesaria, limitada en el tiempo y de alcance mínimo, y que se someta a una verdadera revisión periódica y a evaluación científica.

49. El CEPD insiste en que nadie debe verse obligado a elegir entre una respuesta eficaz a la crisis actual y la protección de nuestros derechos fundamentales, puesto que podemos conseguir ambas cosas; es más, los principios de la protección de datos pueden desempeñar un papel muy importante en la lucha contra el virus. La legislación europea en materia de protección de datos permite el uso responsable de datos personales para fines de gestión sanitaria, al tiempo que garantiza que en ese proceso no se erosionen los derechos y libertades individuales.

Por el Comité Europeo de Protección de Datos

La Presidenta

(Andrea Jelinek)

ANEXO: APLICACIONES DE RASTREO DE CONTACTOS GUÍA DE ANÁLISIS

0. Cláusula de exención de responsabilidad

La presente guía no es prescriptiva ni exhaustiva y tiene como único objetivo proporcionar orientaciones generales a los responsables del diseño y la implementación de aplicaciones de rastreo de contactos. Puede optarse por soluciones distintas de las descritas aquí, que pueden ser lícitas siempre y cuando se ajusten al marco jurídico pertinente (es decir, al RGPD y a la Directiva).

Conviene señalar, asimismo, que la presente guía es de carácter general. Por tanto, las recomendaciones y obligaciones contenidas en el presente documento no deben considerarse exhaustivas. Toda evaluación debe realizarse caso por caso, y determinadas aplicaciones podrían requerir la adopción de medidas adicionales no incluidas en la presente guía.

1. Resumen

En muchos Estados miembros, las partes interesadas están considerando la posibilidad de utilizar aplicaciones *de rastreo de contactos* que ayuden a los ciudadanos a descubrir si han estado en contacto con una persona infectada por el SARS-CoV-2.

Aún no se han determinado las condiciones en las que esas aplicaciones contribuirían de manera eficaz a la gestión de la pandemia. Y esas condiciones tendrían que estar fijadas antes de que se ponga en funcionamiento cualquier aplicación de este tipo. Con todo, conviene proporcionar directrices que aporten información temprana útil a los equipos de desarrollo de estas aplicaciones, de tal modo que quede garantizada la protección de datos personales desde la fase inicial de diseño.

Es importante señalar que la presente guía reviste un carácter general. Por tanto, las recomendaciones y obligaciones contenidas en el presente documento no deben considerarse exhaustivas. Toda evaluación debe realizarse caso por caso, y determinadas aplicaciones podrían requerir la adopción de medidas adicionales no incluidas en la presente guía. El objetivo de la presente guía es proporcionar orientaciones generales a los responsables del diseño y la implementación de aplicaciones de rastreo de contactos.

Algunos criterios podrían ir más allá de los estrictos requisitos que se derivan del marco de protección de datos. Su finalidad es asegurar el mayor nivel de transparencia y, por ende, favorecer la aceptación social de esas aplicaciones.

A tal fin, los editores de aplicaciones de rastreo de contactos deben tener en cuenta los siguientes criterios:

- El uso de una aplicación de este tipo ha de ser estrictamente voluntario. No puede condicionar el acceso a ningún derecho garantizado por ley. Las personas deben ejercer en todo momento el pleno control sobre sus datos y deben poder decidir libremente si desean usar la aplicación.
- Las aplicaciones de rastreo de contactos pueden entrañar un alto riesgo para los derechos y libertades de las personas físicas, por lo que probablemente se deba llevar a cabo una evaluación de impacto relativa a la protección de datos antes de su despliegue.

- Se puede obtener información sobre la proximidad entre los usuarios de la aplicación sin proceder a su localización. Este tipo de aplicación no necesita ni, por tanto, debe implicar el uso de datos de localización.
- El hecho de que un usuario sea diagnosticado de infección por el SARS-CoV-2 únicamente se debe comunicar a las personas con las que el usuario haya estado en estrecho contacto dentro del período de conservación de datos que, desde el punto de vista epidemiológico, resulte pertinente a efectos del rastreo de contactos.
- El funcionamiento de este tipo de aplicación podría requerir, dependiendo de la arquitectura elegida, el uso de un servidor centralizado. En ese caso, y de conformidad con los principios de minimización de datos y de protección de datos desde el diseño y por defecto, los datos tratados por el servidor centralizado deberían limitarse al mínimo estrictamente necesario:
    - Cuando un usuario reciba un diagnóstico de infección, solo puede recogerse información sobre sus contactos estrechos anteriores o los identificadores difundidos por la aplicación del usuario con el consentimiento del usuario. Es preciso establecer un método de verificación que permita afirmar que la persona está efectivamente infectada sin que ello implique identificar al usuario. Desde el punto de vista técnico, esto podría conseguirse no alertando a los contactos hasta que haya intervenido un profesional sanitario, por ejemplo, utilizando un código especial de un solo uso.
    - La información almacenada en el servidor central no debe permitir al responsable del tratamiento identificar a usuarios diagnosticados de infección o que hayan estado en estrecho contacto con esos usuarios, ni debe permitir la inferencia de patrones de contacto no necesarios para determinar los contactos pertinentes.
- El funcionamiento de este tipo de aplicaciones requiere la difusión de datos y su lectura por los dispositivos de otros usuarios, así como la escucha de estas difusiones:
    - Es suficiente con que se intercambien identificadores seudónimos entre los equipos móviles de los usuarios (ordenadores, tabletas, relojes de pulsera conectados, etc.), en particular, mediante su difusión (por ejemplo, a través de la tecnología Bluetooth de baja energía).
    - Los identificadores deben generarse utilizando los procesos criptográficos más avanzados.
    - Los identificadores deben renovarse periódicamente para reducir el riesgo de rastreo físico y ataques de enlace.
- Las aplicaciones deben dotarse de medidas de seguridad que garanticen unos procesos técnicos seguros. En concreto:
    - no deben transmitir a los usuarios información que les permita inferir la identidad o el diagnóstico de otras personas. El servidor central no debe identificar a los usuarios ni inferir información sobre ellos.

Cláusula de exención de responsabilidad: los principios enunciados se refieren con carácter exclusivo a la finalidad declarada de las aplicaciones de *rastreo de contactos*, a saber, la de informar de manera automática a las personas que podrían estar expuestas al virus (sin tener que identificarlas). Los operadores de estas aplicaciones y su infraestructura pueden ser objeto de control por parte de la autoridad supervisora competente. El seguimiento del conjunto de las presentes directrices, o de una

parte de ellas, no es necesariamente suficiente para garantizar el pleno cumplimiento del marco de protección de datos.

2. Definiciones

Contacto	En el contexto de una aplicación de rastreo de contactos, un contacto es un usuario que ha participado, con un usuario confirmado como portador del virus, en una interacción que, por su duración y distancia, conlleva un riesgo de exposición significativa a la infección por el virus. Las autoridades sanitarias deben ponderar los parámetros relativos a la duración de la exposición y la distancia entre personas, que pueden incorporarse a la aplicación.
Datos de localización	Este término alude a todos los datos tratados en una red de comunicaciones electrónicas o por un servicio de comunicaciones electrónicas que indican la posición geográfica del equipo terminal de un usuario de un servicio de comunicaciones electrónicas disponible para el público (según la definición de la Directiva), así como a los datos de otras posibles fuentes, relativos a: • la latitud, longitud o altitud del equipo terminal, • la dirección del desplazamiento del usuario, o • el momento en el que se registró la información sobre la localización.
Interacción	En el contexto de una aplicación de rastreo de contactos, una interacción se define como el intercambio de información entre dos dispositivos que están muy próximos entre sí (en tiempo y espacio), dentro del rango de la tecnología de comunicación utilizada (por ejemplo, Bluetooth). Esta definición excluye la localización de los dos usuarios de la interacción.
Portador del virus	En el presente documento, consideramos que son portadores del virus los usuarios que han dado positivo en una prueba de detección del virus y que han obtenido un diagnóstico oficial de facultativos o centros sanitarios.
Rastreo de contactos	Las personas que han estado en estrecho contacto (según los criterios que definan los epidemiólogos) con una persona infectada por el virus corren un riesgo significativo de infectarse también y, a su vez, de infectar a otras personas. El rastreo de contactos es una metodología de control de enfermedades que registra a todas las personas que han estado muy cerca de un portador del virus, con el fin de comprobar si están expuestas al riesgo de infección y aplicarles las medidas sanitarias adecuadas.

3. Consideraciones generales

GEN-1	La aplicación debe ser una herramienta complementaria de las técnicas tradicionales de rastreo de contactos (en particular, de las entrevistas con personas infectadas), es decir, debe formar parte de un programa de salud pública de mayor alcance. Ha de utilizarse exclusivamente hasta el momento en que las técnicas de localización manual de contactos puedan gestionar por sí solas el volumen de nuevas infecciones.
GEN-2	A más tardar cuando las autoridades públicas competentes decidan «volver a la normalidad», debe establecerse un procedimiento para detener la recogida de identificadores (desactivación global de la aplicación, instrucciones para desinstalarla, desinstalación automática, etc.) y para activar la eliminación de todos los datos recogidos de todas las bases de datos (aplicaciones móviles y servidores).
GEN-3	El código fuente de la aplicación y de su servidor final debe ser abierto, y las especificaciones técnicas han de hacerse públicas, de modo que cualquier parte interesada pueda auditar el código y, cuando proceda, contribuir a mejorarlo, corrigiendo posibles errores y asegurando la transparencia en el tratamiento de datos personales.
GEN-4	Las fases de despliegue de la aplicación deben permitir validar progresivamente su eficacia desde el punto de vista de la salud pública. A tal fin, conviene definir previamente un protocolo de evaluación que especifique los indicadores que permitirán medir la eficacia de la aplicación.

4. Finalidad

PUR-1	La aplicación debe tener la finalidad exclusiva de rastrear contactos, de tal modo que las personas que puedan estar expuestas al SARS-CoV-2 puedan ser alertadas y recibir asistencia. No debe utilizarse para ninguna otra finalidad.
PUR-2	La aplicación no puede desviarse de su finalidad primordial para controlar el cumplimiento de medidas de cuarentena o de confinamiento y/o de distanciamiento social.
PUR-3	La aplicación no puede utilizarse para extraer conclusiones sobre la ubicación de los usuarios basadas en su interacción ni por cualquier otro medio.

5. Consideraciones funcionales

FUNC-1	La aplicación debe proporcionar una funcionalidad que permita informar a los usuarios de que posiblemente han estado expuestos al virus; esa información ha de basarse en la proximidad a un usuario infectado en un intervalo de X días antes de la prueba de detección que haya dado positivo (corresponde a las autoridades sanitarias definir el valor X).

FUNC-2	La aplicación debe facilitar recomendaciones a los usuarios identificados por su posible exposición al virus. Debe transmitirles instrucciones acerca de las medidas que han de tomar y permitirles pedir asesoramiento. En esos casos, sería obligatoria una intervención humana.
FUNC-3	El algoritmo que mida el riesgo de infección teniendo en cuenta factores de distancia y tiempo y, así, determine cuándo debe incluirse a un contacto en la lista de rastreo de contactos debe poder sintonizarse de manera segura, teniendo en cuenta los conocimientos más recientes sobre la propagación del virus.
FUNC-4	**Los usuarios han de ser informados en caso de que hayan estado expuestos al virus**, o deben recibir periódicamente información sobre si han estado o no expuestos al virus, dentro del período de incubación de este.
FUNC-5	La aplicación debe ser interoperable con otras aplicaciones desarrolladas en los Estados miembros, de tal modo que los usuarios que se desplacen por otros Estados miembros puedan recibir notificaciones de forma eficaz.

6. Datos

DATA-1	La aplicación debe poder difundir y recibir datos a través de tecnologías de comunicación de proximidad, como Bluetooth de baja energía, para que pueda llevarse a cabo el rastreo de contactos.
DATA-2	Esos datos difundidos deben incluir identificadores seudoaleatorios fuertes desde el punto de vista criptográfico, generados por la aplicación y específicos de esta.
DATA-3	El riesgo de colisión de identificadores seudoaleatorios debe ser lo suficientemente bajo.
DATA-4	Los identificadores seudoaleatorios deben renovarse periódicamente y con una frecuencia suficiente para limitar cualquier riesgo de reidentificación, rastreo físico o vinculación de personas por parte de operadores de servidores centrales, otros usuarios de la aplicación o terceros malintencionados, etc. Esos identificadores deben ser generados por la aplicación del usuario, posiblemente sobre la base de una semilla proporcionada por el servidor central.
DATA-5	Según el principio de minimización de datos, la aplicación no debe recoger datos distintos de los estrictamente necesarios a efectos del rastreo de contactos.
DATA-6	La aplicación no debe recoger datos de localización a efectos del rastreo de contactos. Los datos de localización solo pueden tratarse con el propósito exclusivo de permitir que la aplicación interactúe con aplicaciones similares de otros países, y deben limitarse en cuanto a la precisión a lo estrictamente necesario para ese único propósito.

DATA-7	La aplicación no debe recoger otros datos sanitarios además de los estrictamente necesarios para los fines de la aplicación, excepto con carácter opcional y con el único propósito de ayudar en el proceso de toma de la decisión de informar al usuario.
DATA-8	Debe informarse al usuario de todos los datos personales que se recojan. Esos datos deben recogerse únicamente con la autorización del usuario.

7. Características técnicas

TECH-1	La aplicación debe utilizar tecnologías disponibles, como las tecnologías de comunicación de proximidad (p. ej., Bluetooth de baja energía), para detectar la presencia de usuarios cerca del dispositivo que está usando la aplicación.
TECH-2	La aplicación solo puede conservar el historial de los contactos del usuario en el equipo durante un período de tiempo limitado determinado previamente.
TECH-3	La aplicación puede recurrir a un servidor central para implementar algunas de sus funcionalidades.
TECH-4	La arquitectura de la aplicación debe basarse en la medida de lo posible en los dispositivos de los usuarios.
TECH-5	A iniciativa de los usuarios que han notificado su infección por el virus, y tras la confirmación de su estado por parte de un profesional sanitario debidamente certificado, el historial de sus contactos o sus propios identificadores deben transmitirse al servidor central.

8. Seguridad

SEC-1	Un mecanismo debe verificar el estado de los usuarios que notifican en la aplicación su condición de positivos en infección por SARS-CoV-2, por ejemplo, facilitando un código de un solo uso vinculado con un laboratorio de pruebas o a un profesional de atención sanitaria. Si no se puede obtener confirmación de forma segura, no debe procederse al tratamiento de datos.
SEC-2	Los datos enviados al servidor central han de transmitirse a través de un canal seguro. El uso de servicios de notificación prestados por proveedores de plataformas de sistema operativo debe evaluarse cuidadosamente y no debe dar lugar a la divulgación de ningún dato a terceros.
SEC-3	Las solicitudes no deben ser vulnerables a la manipulación por parte de un usuario malintencionado.
SEC-4	Deben aplicarse las técnicas criptográficas más avanzadas para asegurar los intercambios entre la aplicación y el servidor, y entre aplicaciones, y, como regla general, para proteger la información almacenada en las aplicaciones y en el servidor. Entre las técnicas que pueden utilizarse figuran, por ejemplo, las siguientes: cifrado simétrico y asimétrico, funciones *hash*, prueba privada de pertenencia (*private membership test*, PMT), intersección privada de conjuntos

	(*private set intersection*, PSI), filtros Bloom, recuperación de información privada, cifrado homomórfico, etc.
SEC-5	El servidor central no debe conservar los identificadores de conexión a la red (p. ej., las direcciones IP) de ningún usuario, incluidos los que han sido diagnosticados positivamente y que han transmitido su historial de contactos o sus propios identificadores.
SEC-6	Para evitar la suplantación o la creación de falsos usuarios, el servidor debe autenticar la aplicación.
SEC-7	La aplicación debe autenticar el servidor central.
SEC-8	Las funcionalidades del servidor deben estar protegidas frente a ataques de repetición.
SEC-9	La información transmitida por el servidor central debe estar firmada para autenticar su origen e integridad.
SEC-10	El acceso a todos los datos almacenados en el servidor central y que no estén a disposición del público debe circunscribirse a las personas autorizadas.
SEC-11	El gestor de permisos del dispositivo en el nivel del sistema operativo solo debe solicitar los permisos necesarios para acceder a los módulos de comunicación y utilizarlos cuando resulte necesario, para almacenar los datos en el equipo terminal y para intercambiar información con el servidor central.

9. Protección de datos personales y privacidad de las personas físicas

Recordatorio: las directrices que figuran a continuación se refieren a las aplicaciones cuya única finalidad es el rastreo de contactos.

PRIV-1	Los intercambios de datos deben respetar la privacidad de los usuarios (y, en particular, el principio de minimización de datos).
PRIV-2	La aplicación no puede permitir identificar directamente a los usuarios al utilizar la aplicación.
PRIV-3	La aplicación no ha de permitir que se rastreen los movimientos de los usuarios.
PRIV-4	El uso de la aplicación no debe permitir que los usuarios obtengan información de otros usuarios (y, en particular, que sepan si son o no portadores del virus).
PRIV-5	La confianza en el servidor central debe ser limitada. La gestión del servidor central debe seguir normas de gobernanza claramente definidas e incluir todas las medidas necesarias para garantizar su seguridad. La ubicación del servidor central debe permitir una supervisión eficaz por parte de la autoridad supervisora competente.
PRIV-6	Ha de llevarse a cabo una evaluación de impacto relativa a la protección de datos, que debería ponerse a disposición del público.
PRIV-7	La aplicación solo debe revelar al usuario si ha estado expuesto al virus y, en la medida de lo posible, sin facilitar información sobre otros usuarios, el número de veces y las fechas de la exposición.
PRIV-8	La información transmitida por la aplicación no debe permitir a los usuarios identificar a los usuarios portadores del virus ni conocer sus movimientos.
PRIV-9	La información transmitida por la aplicación no debe permitir a las autoridades sanitarias identificar a los usuarios que pueden estar expuestos sin el consentimiento de estos.
PRIV-10	Las solicitudes cursadas por la aplicación al servidor central no deben revelar ninguna información sobre el portador del virus.
PRIV-11	Las solicitudes cursadas por la aplicación al servidor central no deben revelar ninguna información innecesaria sobre el usuario, excepto, posiblemente —y solo cuando resulte necesario—, sus identificadores seudónimos y su lista de contactos.
PRIV-12	Han de impedirse los ataques de enlace.
PRIV-13	Los usuarios han de poder ejercer sus derechos a través de la aplicación.
PRIV-14	La supresión de la aplicación debe entrañar la eliminación de todos los datos recogidos a nivel local.
PRIV-15	La aplicación solo puede recoger datos transmitidos por instancias de la aplicación o de aplicaciones interoperables equivalentes. No pueden recogerse datos sobre otras aplicaciones ni otros dispositivos de comunicación de proximidad.

PRIV-16	Para evitar la reidentificación por parte del servidor central, deben implementarse servidores proxy. La finalidad de estos *servidores no colusores es* combinar los identificadores de varios usuarios (tanto los de los portadores del virus como los enviados por los solicitantes) antes de compartirlos con el servidor central, para evitar que este conozca los identificadores de los usuarios (como las direcciones IP).
PRIV-17	La aplicación y el servidor deben desarrollarse y configurarse cuidadosamente con el fin de que no recojan datos innecesarios (p. ej., no debe incluirse ningún identificador en los registros del servidor, etc.) y de evitar el uso de SDK de terceros que recojan datos para otros fines.

La mayoría de las aplicaciones de rastreo de contactos que están siendo objeto de debate actualmente siguen básicamente dos enfoques para abordar la situación en la que un usuario se declara infectado: o bien pueden enviar a un servidor el historial de los contactos de proximidad que han obtenido mediante escaneo, o bien pueden enviar la lista de sus propios identificadores difundidos. Estos dos enfoques están sujetos a los principios que figuran a continuación. El hecho de que estos enfoques se analicen en el presente documento no significa que no haya otros posibles, incluso preferibles —por ejemplo, enfoques que implementan alguna forma de cifrado E2E o aplican otras tecnologías de refuerzo de la seguridad o privacidad—.

9.1. Principios que se aplican únicamente **cuando la aplicación envía al servidor una lista de contactos:**

CON-1	El servidor central debe recoger el historial de contactos de los usuarios declarados positivos por SARS-CoV-2 como resultado de una acción voluntaria por parte de estos.
CON-2	El servidor central no debe mantener ni difundir una lista de los identificadores seudónimos de usuarios portadores del virus.
CON-3	El historial de contactos almacenado en el servidor central debe eliminarse una vez se haya notificado a los usuarios su proximidad a una persona con diagnóstico positivo.
CON-4	Excepto si un usuario detectado como positivo comparte su historial de contactos con el servidor central o si un usuario solicita al servidor que investigue su posible exposición al virus, ningún dato debe salir del equipo del usuario.
CON-5	Cualquier identificador incluido en el historial local debe eliminarse a los X días de su recogida (corresponde a las autoridades sanitarias definir el valor X).
CON-6	Los historiales de contactos enviados por distintos usuarios no deben someterse a tratamiento adicional; por ejemplo, no debe examinarse su correlación cruzada para elaborar mapas globales de proximidad.
CON-7	Los datos contenidos en los registros del servidor han de minimizarse y deben cumplir los requisitos de protección de datos.

9.2. Principios que se aplican únicamente cuando la aplicación envía al servidor una lista de sus propios identificadores:

ID-1	El servidor central debe recoger los identificadores de los usuarios declarados positivos por SARS-CoV-2, difundidos por la aplicación, como resultado de una acción voluntaria por parte de estos.
ID-2	El servidor central no debe mantener ni difundir el historial de contactos de usuarios portadores del virus.
ID-3	Los identificadores almacenados en el servidor central deben eliminarse una vez distribuidos a las demás aplicaciones.
ID-4	Excepto si un usuario detectado como positivo comparte sus identificadores con el servidor central o si un usuario solicita al servidor que investigue su posible exposición al virus, ningún dato debe salir del equipo del usuario.
ID-5	Los datos contenidos en los registros del servidor han de minimizarse y deben cumplir los requisitos de protección de datos.