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

Olivier Micol

Bruselas, 14 de abril de 2020

Jefe de Unidad. Comisión Europea
DG Justicia y Consumidores
Unidad C.3. Protección de Datos
Bélgica

Ref.: OUT2020-0028

Estimado señor Micol:

Le agradecemos mucho que haya ejercido de contacto con el Comité Europeo de Protección de Datos (CEPD) para recabar asesoramiento acerca del proyecto de Directrices sobre las aplicaciones de apoyo a la lucha contra la pandemia de COVID-19. En efecto, el CEPD ha querido ponerse a trabajar rápidamente en esta cuestión; el 19 de marzo publicó una declaración y para la próxima semana tiene previsto publicar directrices adicionales sobre rastreo, investigación científica y teletrabajo. Algunas autoridades nacionales de control están elaborando también directrices nacionales para asesorar a sus gobiernos y a sus operadores de telecomunicaciones acerca de la mejor manera de cumplir la normativa de protección de datos. El CEPD acoge con satisfacción la iniciativa de la Comisión de desarrollar una respuesta paneuropea y coordinada en virtud de la cual las aplicaciones para dispositivos móviles podrían figurar entre las medidas propuestas para empoderar a los ciudadanos en la lucha contra la pandemia. El CEPD ha declarado en repetidas ocasiones que la aplicación de los principios de protección de datos y el respeto de los derechos y libertades fundamentales no solo constituyen una obligación legal, sino también un requisito para reforzar la eficacia de cualquier iniciativa basada en datos para luchar contra la propagación del virus causante de la COVID-19 y para guiar las estrategias de desescalada.

El CEPD es consciente de que, en esta materia, no existe una solución uniforme que sea válida para todos los casos y de que las opciones disponibles exigen que se tengan en cuenta muchos factores, incluido el hecho de que puede verse afectada la salud de las personas. Ese es el motivo por el que las soluciones técnicas contempladas deben examinarse detalladamente, caso por caso. Además, el CEPD considera que poner de relieve la necesidad esencial de consultar a las autoridades de protección de datos para garantizar que los datos personales se traten con arreglo a la legalidad y respetando los

Andrea Jelinek
Chair of the European Data Protection Board
rue Wiertz, 60
1047 Brussels

derechos de las personas, de conformidad con la legislación en materia de protección de datos, es un paso en la dirección correcta.

El desarrollo de las aplicaciones debe hacerse con plena asunción de responsabilidades, documentando con una evaluación del impacto relativa a la protección de datos todos los mecanismos de privacidad desde el diseño y de privacidad por defecto aplicados, y el código fuente ha de hacerse público con miras a un control lo más amplio posible por parte de la comunidad científica.

En la fase actual, y sobre la base de la información facilitada por la Comisión, el CEPD solo puede centrarse en el objetivo general de las aplicaciones previstas, para comprobar si estas se ajustan a los principios de la protección de datos, y en los mecanismos previstos para el ejercicio de los derechos y las libertades de la población. El CEPD entiende que, de esta manera, la Comisión obtendrá elementos de análisis que permitan proseguir la reflexión para ajustar las opciones que se exponen en el documento, cuando resulte necesario, o para explorar nuevas opciones técnicas. En cualquier caso, el CEPD investigará más a fondo esta cuestión en sus próximas directrices.

En la presente respuesta, el CEPD desea referirse específicamente al uso de aplicaciones para el rastreo de contactos y a la función de alerta, aspectos que son los que merecen una mayor atención si se pretende minimizar las interferencias con la vida privada y, al mismo tiempo, permitir el tratamiento de datos para proteger la salud pública.

En caso de que esas aplicaciones resulten útiles para la ejecución de alguna política de salud pública, solo podrán alcanzar su máxima eficiencia si son utilizadas por la mayor proporción posible de la población, en un esfuerzo colectivo de lucha contra el virus. Cualquier heterogeneidad funcional, falta de interoperabilidad o incluso diferencia individual en el uso de la aplicación puede tener repercusiones externas negativas que afecten a otras personas, lo que reduciría su efecto sanitario. El CEPD apoya firmemente la propuesta de la Comisión sobre la adopción voluntaria de dichas aplicaciones, una decisión que las personas deberían tomar como muestra de responsabilidad colectiva. Es preciso señalar que la adopción voluntaria está ligada a la confianza individual, lo que ilustra más claramente si cabe la importancia de los principios de protección de datos.

El CEPD señala que el mero hecho de que el uso del rastreo de contactos tenga carácter voluntario no significa que el tratamiento de datos personales por parte de las autoridades públicas 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. La promulgación de leyes nacionales que promuevan el uso voluntario de las aplicaciones sin consecuencias negativas para las personas que no las utilicen podría servir de base jurídica al respecto. Por consiguiente, este tipo de intervenciones legislativas no deben concebirse como un medio para presionar en favor de la adopción obligatoria, y las personas deben tener la libertad de instalar y desinstalar la aplicación por decisión propia. Estas leyes podrían ir acompañadas de actividades de comunicación apropiadas a nivel nacional que promovieran esas herramientas mediante campañas de sensibilización y asistencia a los menores, a las personas discapacitadas y a las personas con menor formación y cualificación, a fin de evitar una adopción dispersa o unos conocimientos difusos acerca

Andrea Jelinek
Chair of the European Data Protection Board

rue Wiertz, 60
1047 Brussels

de la evolución de la epidemia, así como cualquier posible brecha sanitaria. En efecto, cualquier falta de datos provocada por el descuido en el uso de la aplicación por parte de los usuarios o incluso por un fallo de batería del dispositivo podría socavar gravemente la utilidad pública general de estas herramientas.

Las aplicaciones de rastreo de contactos no requieren rastrear la ubicación de los usuarios a título individual. Su objetivo no es seguir los movimientos de las personas ni controlar el cumplimiento de las normas. La principal función de estas aplicaciones es detectar circunstancias (contactos con personas con diagnóstico positivo) que solo son probables y que, para la mayoría de los usuarios, pueden no llegar a materializarse, especialmente en la fase de desescalada. La recogida de datos sobre los movimientos de una persona en el contexto del uso de una aplicación de rastreo de contactos violaría el principio de minimización de datos. Además, generaría importantes riesgos para la seguridad y la privacidad.

Las autoridades sanitarias y los científicos están en buena posición para determinar si, dónde y cuándo debe notificarse una circunstancia, con sujeción a una estricta prueba de necesidad acorde con la ley, y habrán de definir algunos de los requisitos funcionales de la aplicación. Otro aspecto que está debatiéndose es el almacenamiento de los datos relativos a esas circunstancias. Se contemplan dos opciones principales: el almacenamiento local de los datos en los dispositivos de los usuarios, o su almacenamiento centralizado. El CEPD considera que ambas opciones pueden ser válidas —siempre que se hayan establecido las medidas de seguridad adecuadas—, y que cabe prever que haya otras entidades responsables del tratamiento en función del objetivo último de la aplicación (por ejemplo, el responsable del tratamiento y los datos tratados pueden no ser los mismos si el objetivo es proporcionar información dentro de la aplicación o si consiste en ponerse en contacto con la persona por teléfono). En todo caso, el CEPD desea subrayar que la solución descentralizada se ajusta mejor al principio de minimización.

Por último, estas aplicaciones no son plataformas sociales para hacer cundir la alarma social ni generar ningún tipo de estigmatización. De hecho, deberían ser herramientas que empoderen a los ciudadanos para que asuman su parte. Según el proyecto de Directrices, su único objetivo es permitir a *las autoridades sanitarias públicas identificar a las personas que han estado en contacto con alguien infectado por la COVID-19 y pedirles que se sometan a autoaislamiento, hacerles rápidamente pruebas y aconsejarles acerca de las próximas etapas, si procede, incluso sobre lo que tienen que hacer si desarrollan síntomas*. La calidad de los datos tratados reviste una importancia crucial en este esfuerzo. Los pasos que deben darse para *identificar a las personas que han estado en contacto con alguien infectado por la COVID-19* no son sencillos ni fáciles. Se puede informar a una persona a través de una notificación interna de la aplicación, de manera que esta solo trate seudónimos aleatorios. Además, conviene que exista un mecanismo que garantice que, cuando una persona sea declarada positiva por COVID-19, la información introducida en la aplicación sea correcta, ya que esa información puede desencadenar notificaciones a otras personas sobre el hecho de que han estado expuestas al virus. Este mecanismo podría basarse, por ejemplo, en un código de un solo uso que la persona pueda escanear cuando reciba el resultado de la prueba. Cada contacto individual debe ser establecido exclusivamente por las autoridades sanitarias tras un sólido análisis de datos y con el mínimo nivel de

Andrea Jelinek
Chair of the European Data Protection Board

rue Wiertz, 60
1047 Brussels

inferencia. Además, la Comisión debe aclarar la función de la *lista de contactos del propietario del dispositivo* mencionada en las Directrices.

Los algoritmos utilizados en las aplicaciones de rastreo de contactos deberían estar sujetos a una estricta supervisión por parte de personal cualificado, con el fin de limitar la aparición de falsos positivos y negativos, y en modo alguno debería automatizarse por completo la labor de *aconsejarles acerca de las próximas etapas*. Conviene incluir un mecanismo de devolución de llamada de forma que el interesado pueda disponer de un número de teléfono o un canal de contacto donde obtener más información de un agente humano. Además, a fin de evitar la estigmatización, no debería incluirse en esos *consejos* ningún elemento que pueda permitir identificar a otros interesados, ni debe la aplicación o alguna parte de ella (como los paneles de control o los parámetros de configuración) permitir la reidentificación de cualquier otra persona, esté o no infectada por COVID-19. El CEPD recomienda encarecidamente que no se almacene directamente ningún dato de identificación en el dispositivo de los usuarios y que, en todo caso, esos datos se supriman lo antes posible.

El CEPD apoya firmemente el enfoque de las recomendaciones según el cual, una vez se supere esta crisis, este sistema de emergencia debe dejar de utilizarse y, como norma general, los datos recogidos han de suprimirse o anonimizarse.

Por último, el CEPD y sus miembros, encargados de garantizar la correcta aplicación del Reglamento General de Protección de Datos y la Directiva sobre la privacidad y las comunicaciones electrónicas, deben participar plenamente en todo el proceso de elaboración y aplicación de estas medidas. El CEPD recuerda que tiene previsto publicar en los próximos días una serie de directrices sobre geolocalización y otras herramientas de rastreo en el contexto de la pandemia de COVID-19.

En cualquier caso, el CEPD se mantiene a disposición de las instituciones de la UE y de todas las partes interesadas para seguir ofreciendo asesoramiento en el desarrollo y la utilización de las mencionadas aplicaciones móviles para la lucha contra la COVID-19.

Atentamente,

Andrea Jelinek

Andrea Jelinek
Chair of the European Data Protection Board

rue Wiertz, 60
1047 Brussels