III. Desafíos para el diseño institucional

Cómo establecer protocolos éticos en el diseño de aplicaciones de trazabilidad para pandemias

David Casacuberta

Introducción y estructura del capítulo

El objetivo de este capítulo es establecer los requisitos éticos y epistémicos necesarios para diseñar una aplicación de seguimiento de contactos entre individuos para luchar contra la expansión de una pandemia (como la reciente del COVID-19). Buscamos baremos de seguridad que nos permitan establecer 1) si los datos obtenidos por ese sistema son suficientemente fiables y precisos como para decidir las medidas políticas y sanitarias precisas de lucha contra la pandemia, 2) que la aplicación trata a los diferentes grupos poblacionales de forma similar y no se generan ni discriminaciones ni sesgos de etnia, género o económicos, y 3) que la privacidad de los usuarios que toman parte en la investigación no se pone en peligro en ningún momento del proceso, desde la recogida inicial de datos hasta su presentación final para desarrollar una política de acción contra el virus.

Aunque los ejemplos que vamos a discutir en este texto están focalizados en la lucha contra el COVID-19, ya se han utilizado con éxito los datos de teléfonos móviles para luchar contra el ébola (Sacks *et al*., 2015) o la gripe aviar en África (Breiman *et al*., 2007), con lo que es lógico suponer que este tipo de metodologías se volverán a utilizar en futuras pandemias. De ahí la necesidad de establecer protocolos éticos y epistémicos claros, que sirvan para esta y para futuras pandemias.

En la siguiente sección presentaremos las tecnologías más comunes para este tipo de estudios, describiendo diversas tipologías de aplicaciones, estableciendo cómo funcionan, detallando cuáles son sus principales ventajas e inconvenientes, su grado de fiabilidad, así como los posibles problemas éticos que puede generar su uso.

En la sección tercera analizaremos diversos protocolos que pueden usarse para minimizar estos problemas éticos y su dependencia de la legislación de la Unión Europea, la más restrictiva y con más protocolos de defensa de la privacidad.

Aunque defender la privacidad de los usuarios de un sistema así es evidentemente la necesidad más urgente a la hora de desarrollar un protocolo ético del diseño de aplicaciones, es importante entender también que existen otros problemas que pueden surgir de un uso no controlado de este tipo de servicios digitales, con lo que dedicaremos la sección cuarta a explorar de qué forma un sistema así puede generar sesgos y otro tipo de discriminaciones entre la población.

En la sección quinta, una vez recopilada toda esta información, la usaremos para establecer un protocolo de diseño que asegure la fiabilidad epistémica y ética de estas aplicaciones de trazabilidad y discutiremos el grado de fiabilidad ética y epistémica de un sistema así, finalizando el texto con unas conclusiones que recopilen lo defendido en el capítulo.

Principales sistemas para establecer la trazabilidad de un contagio con medios digitales

¿Cómo podemos calcular la localización de un usuario para saber si ha estado cerca o no de otros usuarios, y así establecer si un usuario puede haber con-

tagiado a otro? Tenemos acceso a diversos procedimientos, desarrollados a partir de alguna de las siguientes cinco tecnologías:

- **Datos de ubicación de una torre celular.** Los teléfonos móviles –no solo los smartphones, sino también un móvil clásico, para transmisión de voz y SMS– emiten continuamente señales para identificarse con las torres más cercanas y así poder recibir o hacer una llamada. Cada vez que un teléfono establece una conexión así, genera un registro con sello de tiempo conocido como información de ubicación del sitio celular (CSLI). Los proveedores de servicios inalámbricos recopilan y almacenan esta información. Sabiendo la ubicación física de la torre celular, podemos establecer de forma aproximada dónde están esos teléfonos.
- **GPS** son las siglas de Global Positioning System, es decir Sistema de Posicionamiento Global. Es una tecnología basada la localización de un dispositivo emisor a partir de las posiciones de un mínimo de cuatro satélites artificiales en órbita terrestre (de 31 en funcionamiento que ofrecen este servicio). Estimando el tiempo que tardan las señales en llegar y volver al dispositivo es posible calcular con bastante precisión la localización del dispositivo y, por extensión, de la persona que lo lleva. En su versión militar el sistema GPS es capaz de calcular la posición del objetivo con un margen de error de centímetros, mientras que el uso civil tiene normalmente una exactitud de unos pocos metros (NCO, 2019). La inmensa mayoría de smartphones tienen en la actualidad algún sistema de GPS que permite así localizar a sus usuarios con un margen de error mucho menor del que tendríamos basándonos solo en la posición relativa del usuario con las diferentes torres celulares de su entorno. Un ejemplo de aplicación basada en GPS es SafePaths, desarrollada en el MIT.
- **Wifi.** De manera automática, un smartphone con wifi va haciendo barridos para establecer si hay alguna conexión posible, aunque el usuario no haya indicado su interés por acceder a un punto de acceso wifi. Conociendo las localizaciones de esos puntos de acceso tenemos así un componente extra para ayudarnos a la geolocalización. Por sí sola, la capacidad de los smartphones de conectarse a internet en un punto de acceso no es suficiente para establecer la posición de una persona, pero si se combina con los datos de GPS puede ayudar a mejorarlos. La pro-

puesta de Apple y Google para localizar las posiciones de los usuarios y hacer predicciones sobre dónde están ubicados se basa en cruzar los datos de GPS, acceso al wifi y bluetooth.

- **Bluetooth** es un sistema de comunicación inalámbrico de corto alcance entre diferentes dispositivos electrónicos. Al contrario que los sistemas indicados anteriormente, no informa sobre la posición de la persona, pues su alcance es corto, sino que indica si la persona ha estado en las proximidades de otra al mismo tiempo. Así, el bluetooth puede detectar posibles contagios al compilar qué personas que usan la aplicación han estado juntas. Es necesario que las personas que se encuentran tengan ambas la aplicación y la conexión bluetooth activada para que queden registradas. Un ejemplo de una aplicación así es TraceTogether, desarrollada por el gobierno de Singapur y que incluye protocolos digitales de cifrado para proteger la privacidad de sus usuarios (Bay *et al*., 2020).
- **Códigos QR.** Las siglas refieren a Quick Response o respuesta rápida. Se trata de una evolución del código de barras reconvertido en una matriz bidimensional de puntos negros en un fondo blanco para codificar información de forma visual de manera que un lector con cámara pueda acceder. En algunos países, como Nueva Zelanda (Grant *et al*., 2020) o China (Wu *et al*., 2021), se usan códigos QR para que un usuario informe de forma voluntaria de su presencia en un lugar, quedando así registrado que estuvo en el lugar en el que está el QR y el momento en el que estuvo. Estos datos se almacenan después en una base de datos común para ser analizada.

Existen igualmente varias aplicaciones para smartphone que usan más de una de estas tecnologías. Por ejemplo, tenemos así Care19, en el estado de Dakota del Norte (Althoff *et al*., 2020), que combina datos de wifi, GPS y bluetooth; o Smittestopp, en Noruega (Sandvik, 2020), que combina los datos de geolocalización con la señal bluetooth.

Protección de la privacidad de los usuarios en un sistema de trazabilidad

Hay pocos sistemas tan invasivos para nuestra privacidad como un sistema de trazabilidad de contagios. Por un lado, buena parte de estos sistemas de trazabilidad son aplicaciones que indican nuestra posición en todo momento y, como todas registran encuentros, también informan de con quién nos hemos visto en todo momento. Por otro lado, al ser datos que van incluidos en un historial médico, un acceso de terceros no deseados a una base de datos de privacidad revelaría así toda una serie de datos sensibles y confidenciales de las personas incluidas.

Por ello es necesario diseñar estas aplicaciones con un fuerte sentido de la privacidad. La forma concreta a nivel matemático y algorítmico en que ello es posible queda fuera de los objetivos de este capítulo, que forma parte de un libro sobre diseño institucional. En su lugar, vamos a establecer criterios éticos y políticos de protección de la privacidad que ha de seguir un sistema así. Para ello nos basaremos en las ideas presentadas en Cavoukian (2009) y en Parker *et al*. (2020).

El primer principio básico de diseño que garantice la privacidad es que se trate de un diseño proactivo y no reactivo. Es decir, ha de ser un sistema que prevenga de forma directa ataques y brechas de terceros no deseados. No ha de ser un sistema pensado para poner remedio al problema y minimizar daños una vez que un intruso ha conseguido acceso a la base de datos.

Un segundo principio establece que la privacidad ha de ser la forma natural de funcionamiento de la aplicación. La privacidad no puede ser –como sucede en redes sociales como Facebook o Instagram– una posible opción enterrada en un mar de alternativas en la pestaña de preferencias de la aplicación. La privacidad ha de ser la opción por defecto y el usuario no ha de necesitar de ninguna acción por su parte para establecerla.

Un tercer principio define que la privacidad ha de fluir de forma natural en la interacción. Es inaceptable, como afirma Cavoukian (2009), que la experiencia del usuario o la usabilidad del sistema se vean comprometidas en aras de proteger la privacidad.

Un cuarto principio establece, tal y como exigen las directivas de protección de datos de la Unión Europea, que no puede haber negociaciones a la hora de proteger la privacidad. No es aceptable poner en riesgo la privacidad

del usuario para facilitar investigaciones posteriores por parte de centros médicos o para hacer más sencillo el uso de la aplicación.

Un quinto principio determina que la privacidad ha de estar protegida en todas las fases del sistema, desde la recogida inicial de los datos de posición del usuario con su smartphone, a la posterior exportación de la base de datos por un equipo de investigación médica que quiera analizar esos datos para establecer correlaciones relevantes en la transmisión del virus. Todo el ciclo de vida de los datos personales ha de estar protegido contra ataques a la privacidad de los usuarios.

Un sexto principio indica la necesidad de garantizar la integridad de los datos, con sistemas automáticos de registro de dónde han ido los datos y quién los ha procesado de manera que, en caso de que finalmente haya una brecha, sea posible establecer los responsables de esta, establecer cuáles son los daños y reintegrar la base de datos a su estado original sin brechas en la privacidad.

Finalmente, queremos una aplicación donde el usuario esté plenamente informado de las diferentes maneras en que su privacidad está protegida de una forma no técnica, sin hacer referencias a oscuros protocolos criptográficos de manera que pueda confiar en ella plenamente.

En paralelo, debemos asegurar que los usuarios preocupados por su privacidad puedan consultar de qué forma están incluidos en las diferentes bases de datos y pedir la eliminación de aquellas entradas que consideren que erosionan su privacidad. El Reglamento General de Protección de Datos de la Unión Europea (conocido normalmente por sus siglas RGPD) establece la necesidad de garantizar ese acceso a todos los ciudadanos y así poder establecer qué se sabe sobre ellos y quién tiene acceso a esa información (Yebra, 2016).

Desde una perspectiva epistémica, este tipo de protección es también muy relevante, pues la información que ofrece una base de datos sobre una ciudadana o ciudadano puede ser errónea, ya sea porque los datos no se han obtenido de forma correcta, porque ha habido una identificación incorrecta de usuario o porque en el análisis posterior de datos se han creado confusiones. Facilitar el libre acceso de los ciudadanos a su propio registro es la forma más sencilla y fiable de evitar este tipo de errores.

Afortunadamente, existen protocolos lo suficientemente robustos que garantizan estos procesos. En ese sentido es posible hacer un seguimiento de trazabilidad de personas sin comprometer su privacidad.

Consideremos, por ejemplo, el protocolo DP-3T (Avitabile *et al*., 2020; Troncoso *et al*., 2020), que garantiza un sistema descentralizado de trazabilidad. Sin entrar en complejidades matemáticas, este sistema ofrece una aplicación de código abierto con el que la comunidad científica e informática puede revisarlo sin problemas y contrastar cualquier problema de fiabilidad. Una vez instalada, la aplicación envía códigos semialeatorios –al estilo de los generadores automáticos de contraseñas– cada cinco minutos a todos los dispositivos cercanos usando bluetooth, mientras escucha también a otros dispositivos que también estén generando mensajes.

Observemos que en el proceso no hay forma de identificar los móviles que generan estas señales, pues el código generado no contiene ningún elemento de localización GPS, ni de identificación única del móvil. Si dos teléfonos están juntos más de 5 minutos intercambian mensajes, que quedan registrados en los dos teléfonos durante 14 días. Son mensajes sin información, solo combinaciones aleatorias de números y letras.

Supongamos que el propietario de uno de esos teléfonos se le diagnostica como positivo de COVID-19. Entonces su móvil sube a un servidor del hospital los códigos pseudoaleatorios que ha ido registrando en los últimos 14 días. Esos códigos no sirven para identificar al propietario, pues su identidad está protegida. El móvil de la segunda persona va haciendo conexiones regulares al servidor del hospital para establecer si alguno de sus contactos ha dado positivo a COVID. Reconoce los códigos que intercambió con un móvil, con lo que el móvil le avisa que podría estar infectado y le recomienda un autoconfinamiento.

En todo el proceso resulta eminentemente complejo establecer la identidad de nadie, pero todo el mundo recibe la información que necesita, tanto los usuarios individuales como los epidemiólogos, que pueden seguir la evolución de la pandemia sin tener acceso a la identidad de ninguno de los miembros de la base de datos.

Esta seguridad de que nuestra privacidad está protegida es mucho más difícil de establecer si usamos información basada en geolocalización. Aunque los datos de posición de un individuo no estén asociados en su perfil a ningún dato identificador como nombre y apellidos, dirección o número de teléfono, existen diversos métodos estadísticos de análisis que podrían facilitar la reidentificación de buena parte de los usuarios contenidos en una base de datos aparentemente anonimizada (Cecaj *et al*., 2015; Yin *et al*., 2015).

Sin embargo, esta peligrosidad es más teórica que real. Para establecer esta reidentificación es necesario cruzar los datos de geolocalización con otras bases de datos, como información en las redes sociales, y no se puede escoger a un usuario particular del que tengamos un interés especial en identificar; se trata más bien de explorar la base de datos y ver de qué individuos, por una serie de casualidades, tenemos suficiente información para identificar, y lo que finalmente obtendríamos es asignar haber dado positivo a COVID a una serie de usuarios con una probabilidad determinada. Es ciertamente un riesgo posible, pero que ha de valorarse contra otros riesgos, como el de ser víctima de una pandemia.

Otras implicaciones epistémicas y éticas de las tecnologías de trazabilidad

Siguiendo el listado de tecnologías relevantes que presentamos en la segunda sección, podemos preguntarnos por su fiabilidad. Una precaución básica para darle sentido a todo este ejercicio es entender que "localización del usuario en tiempo real" es la meta final y no es ni mucho menos el dato de salida que las aplicaciones generan.

Recordemos, en primer lugar, la información que necesitamos de base. Las autoridades sanitarias definen un contacto cercano como una distancia de dos metros o inferior con una persona infectada, y estar al menos diez minutos con esa persona (Burke *et al*., 2020). Revisemos seguidamente las cinco tecnologías que hemos descrito anteriormente y veamos de qué forma nos ofrecen información sobre la posición de una persona y establecer así si sería suficiente.

Los datos de ubicación a partir la torre celular son interesantes para estudios de corte urbanístico, como para saber cuántos coches entran cada día a una ciudad por sus diferentes rutas de entrada, o cuántas personas hay congregadas en un espacio público; pero no ofrecen exactitud suficiente como para establecer que una persona ha estado con seguridad a una distancia de dos metros o inferior de otra.

Además, los datos de ubicación a partir de las torres celulares pueden crear sesgos. Si bien en ciudades pobladas hay gran cantidad de antenas receptoras y podemos tener información más detallada de dónde ha estado una persona, en zonas rurales las torres son mucho más escasas, y la información

sobre geoposicionamiento de una persona nos llegará con un margen de error de varios kilómetros cuadrados, con lo que es completamente inútil. Ello llevaría además a un tipo de estudio y acciones políticas sesgadas a favor de los usuarios en zonas urbanas pobladas. El GPS nos daría una información mucho más detallada, en el mejor de los casos con un margen de error de un metro.

Sin embargo, su nivel de precisión baja notablemente en entornos urbanos, especialmente en lugares con edificios altos, pues complican la recepción de señal, y el margen de error puede llegar a los 20 metros. Lo mismo sucede cuando estamos en el interior de una casa o edificio. También tendríamos problemas de sesgo, en este caso económico, pues perderíamos los datos de aquellas personas que no pueden pagarse un smartphone con GPS y el pago mensual de subscripción a Internet asociado. La inclusión de los datos obtenidos vía wifi mejoraría algo el sistema, pero seguirá sin tener la efectividad que necesitamos para establecer que personas coinciden en un rango de dos o menos metros.

Bluetooth parece la tecnología más fiable sobre el papel, pues no pone en peligro la privacidad de dónde hemos estado –ya que no registra ese dato– y simplemente establece cuándo dos o más personas han estado en contacto. Cruzar esa información con datos sobre contagios nos permitiría a la vez modelizar la difusión de la enfermedad, así como advertir a una persona de un posible contagio al haber estado en contacto con alguna portadora del virus.

Sin embargo, a la hora de la verdad, bluetooth es una tecnología caprichosa y comete muchos errores a la hora de establecer si dos usuarios de smartphone han estado juntos o no. Tal y como argumenta Vaugham (2020), en espacios como supermercados o trenes, la aplicación no era capaz de distinguir entre mantener una separación mínima de 2 metros o caminar muy juntos, y cometía por tanto muchos falsos positivos y falsos negativos. Las razones son varias, pero una muy relevante es que buena parte de dispositivos móviles detectan señales bluetooth hasta los 30 metros, pero no son capaces de establecer la distancia a la que está el emisor de la señal, con lo que no son útiles para indicar si realmente los usuarios se han mantenido siempre a la distancia segura de dos metros, dato necesario para que el sistema tenga sentido.

Los puntos de control vía QR son los más fiables de todos, y tienen además el añadido de que sea el usuario quien activamente acepta hacer pública su localización. Pero, para poder ser realmente útiles, sería necesario disponer de un amplio número de códigos QR distribuidos de forma sistemática en todos los centros de población, y muy pocos países disponen de una estructura así.

De todas formas, en la práctica es fácil imaginar la facilidad con la que los usuarios olvidarían leer el código QR con su cámara para indicar su posición, la fatiga y el desinterés que provocaría un comportamiento sistemático cada vez que saliéramos a la calle, o la no lectura intencionada de un código cuando no queremos que quede registrada nuestra presencia allí. Así pues, sería un sistema que generaría datos muy poco fiables.

Protocolos epistémicos y éticos para el desarrollo de aplicaciones de trazabilidad fiables y sin sesgos

El primer paso en el diseño de una aplicación de trazabilidad para ser usada en tiempos de pandemia es establecer unos criterios muy rígidos en su definición y uso. Una definición relajada de usos u objetivos puede acabar produciendo un sistema inseguro que acabe en manos de un equipo que no tenga muy claras cuáles son las salvaguardas del sistema y lo acabe usando de una forma que erosione derechos básicos de los usuarios.

Siguiendo la propuesta de la American Civil Liberties Union (ACLU), en Stanley y Granick (2020), antes de crear cualquier tipo de registro de trazabilidad de usuarios es necesario establecer un protocolo bien definido que establezca:

- El *objetivo* para el que se están recopilando esos datos. Ha de quedar muy claro cuál es su uso exclusivo y eliminar de forma tajante la posibilidad de usar esos datos para otros estudios no relacionados.
- Es importante *limitar qué datos se van a recopilar* de forma muy clara. Cuantos menos datos sensibles haya de entrada en el registro, más fácil será proteger la privacidad de los usuarios y más difícil será que se generen sesgos discriminatorios.
- Si entre los objetivos de la aplicación está localizar individuos susceptibles de estar contagiados para alertarlos, con lo que es necesario establecer sistemas de reidentificación, deben crearse protocolos criptográficos de privacidad diferencial (Dwork, 2008) para asegurar que terceros no deseados no puedan reidentificar a usuarios sin su permiso expreso.

- Igualmente, es importante dejar bien claro desde la definición del proyecto *qué individuos y organizaciones tienen acceso* a esos datos y hacer imposible que otras organizaciones tengan acceso a esos datos *a posteriori*. Es fácil imaginar lo tentador que sería para la policía saber dónde ha estado un sospechoso con anterioridad a partir de una base de datos de trazabilidad, pero ello pondría en peligro la confianza de los usuarios en sistema. Esto, debido a que es de una legalidad poco clara, debe impedirse a toda costa.
- También ha de quedar claro *cómo se van a usar esos datos*, cuál es su función. Los usuarios del sistema han de saber de antemano qué consecuencias puede tener para ellos su inclusión en una base datos. Si, por ejemplo, no queda claro si esos datos puede usarlos el gobierno para establecer quién se ha saltado un toque de queda y ponerle una multa, muchos usuarios pueden decidir no usar el sistema por miedo a represalias.

Finalmente, tal y como hemos mencionado arriba, es necesario establecer la *integridad y fiabilidad de los datos* en todo su ciclo de vida. Así, es importante también establecer en qué momento esos datos dejarán de tener sentido para el uso específico con el que fueron recopilados y borrarlos completamente una vez su función se haya conseguido. Así, si la función de la aplicación es avisar a los ciudadanos de un posible contagio y que se pongan en cuarentena, no tiene sentido mantener esos datos más de 20 días, un mes a lo sumo.

Es importante observar que, si queremos darle una dimensión preventiva a nuestra aplicación y evitar que la epidemia se extienda, la información ha de procesarse de forma rápida. Esto está muy claro en el caso del COVID-19. Cuando una persona queda infectada por COVID-19 pasan tres días hasta que esa persona se convierte a su vez en foco de contagio. Sin embargo, todavía han de pasar un par de días más hasta que empezamos a mostrar síntomas claros. Ello significa que si podemos poner en cuarentena a alguien si ha estado en contacto con otra persona enferma antes de que se convierta en vector de la enfermedad, podemos ir un paso por delante y detener la extensión de la enfermedad. Y la cantidad de contagios que han tenido lugar de esa forma no es precisamente baladí. De hecho, al menos 50% de los contagios de COVID-19 tuvieron lugar sin que la persona transmisora fuera consciente de que tenía la enfermedad (Ferretti *et al*., 2020).

Quiero hacer hincapié en un punto clave del argumento: si queremos que este tipo de aplicaciones tengan una función preventiva, tenemos que tomar la decisión de mantener en cuarentena a una persona durante diez días *basándonos exclusivamente* en los resultados del algoritmo que procesa los datos recopilados de la aplicación, aunque la persona en cuestión no muestre aún ningún síntoma. Ello significa que, además de una amenaza abstracta a la privacidad del usuario, existe una restricción inmediata y más problemática de su capacidad de movilidad, forzándola a estar encerrada en su casa, sin tener contacto ni siquiera con las personas que cohabitan en su domicilio, basándonos exclusivamente en unos resultados técnicos que, como hemos argumentado en la sección tercera, no son tan fiables como uno podría pensar.

El sistema solo es fiable si un número considerable de personas lo usan. En una simulación epidemiológica en la que se tomó de base al Reino Unido, se argumenta que para notar un efecto real en la disminución de la transmisión del COVID sería necesario que al menos 56% de los ciudadanos del Reino Unido tuvieran la aplicación instalada y en funcionamiento, con la suposición adicional que hacía el sistema de que los mayores de 70 años estarían confinados en su domicilio (Hinch *et al*., 2020).

Esto nos lleva a otro problema relevante a la hora de considerar la efectividad de estos sistemas. Con la excepción de China y otros países donde la cuarentena a los ciudadanos se establece de forma obligatoria, con participación policial si es preciso, en las democracias occidentales el sistema confía en que la ciudadana o ciudadano que recibe el mensaje de confinarse durante diez días realmente lo hará, y eso es un supuesto demasiado optimista.

A manera de conclusión

Las aplicaciones de trazabilidad para contener la extensión de una pandemia como el COVID-19, para asegurar su funcionalidad epistémica y ética, deben cumplir con los siguientes requisitos:

1. Un uso extensivo por parte de la mayoría de la población susceptible de contagio de alguna de las aplicaciones de trazabilidad accesibles en el mercado.

2. Una aplicación gratuita, de fácil acceso y uso, con mensajes sencillos y con un funcionamiento lo más transparente posible.
3. Protocolos informáticos fiables para asegurar que los usuarios no puedan ser reidentificados.

El tercer requisito es fácilmente conseguible con la tecnología apropiada, tal y como hemos argumentado en la sección tercera. Es posible crear sistemas criptográficos seguros en los que sea muy complejo tecnológicamente establecer la identidad de un usuario y, si nos limitamos a códigos bluetooth, prácticamente imposible.

El segundo requisito, una aplicación clara y transparente, es el más central, pues no sirve de nada tener un sistema seguro de protección de la privacidad si los usuarios no lo entienden y no lo van a querer usar. De la misma forma, el segundo requisito es también central para asegurar el primero. Si una aplicación es compleja de usar, o el usuario no entiende los mensajes que recibe de la aplicación, los usuarios dejarán de usarla.

Desgraciadamente, incluso aunque el segundo y tercer requisito se desarrollen a la perfección, el primer requisito, un uso universal de la aplicación, sigue siendo problemático, pues existen toda una serie de barreras de acceso a lo digital, desde la imposibilidad económica de comprarse un smartphone, analfabetismo digital que impide entender una aplicación por muy sencilla que esté definida, así como las sospechas y cultura conspiranoica asociada a un estatus social inferior.

Considerando el hecho de que estas barreras al primer requisito afectarían de forma más clara a personas de un nivel económico y social inferior, con lo que las propuestas de actuación que se obtuvieran de esos datos estarían sesgadas ética y epistémicamente, proponemos que se usen estas aplicaciones como herramientas relevantes para recabar información sobre una pandemia, pero no que constituyan el eje central informativo a la hora de tomar decisiones políticas en el control de la enfermedad.

Referencias

Althoff, K. N., Coburn, S. B. y Nash, D. (2020). "Contact tracing: Essential to the public health response and our understanding of the epidemiology of coronavirus disease 2019". *Clinical Infectious Diseases, 71*(8): 1960-1961.

Avitabile, G., Botta, V., Iovino, V. y Visconti, I. (2020). "Towards defeating mass surveillance and SARS-CoV-2: The Pronto-C2 fully decentralized automatic contact tracing system". *IACR Cryptology ePrint Archive, 493*. URL=<https://eprint.iacr.org/2020/493.pdf>

Bay, J., Kek, J., Tan, A., Hau, C. S., Yongquan, L., Tan, J. y Quy, T. A. (2020). "BlueTrace: A privacy-preserving protocol for community-driven contact tracing across borders". Government Technology Agency-Singapore. URL=<https://bluetrace.io/static/bluetrace_whitepaper-938063656596c104632def383eb33b3c.pdf>

Breiman, R. F., Nasidi, A., Katz, M. A., Njenga, M. K. y Vertefeuille, J. (2007). "Preparedness for highly pathogenic avian influenza pandemic in Africa". *Emerging infectious diseases, 13*(10): 1453.

Ghinai, I., Jarashow, M. C., Lo, J., McPherson, T. D., Rudman, S., Scott, S., Hall, A. J., Fry, A. M. y Rolfes, M. A. (2020). "Active monitoring of persons exposed to patients with confirmed COVID-19–United States, January–February 2020". *Morbidity and Mortality Weekly Report, 69*(9): 245-246.

Cecaj, A., Mamei, M. y Zambonelli, F. (2016). "Re-identification and information fusion between anonymized CDR and social network data". *Journal of Ambient Intelligence and Humanized Computing, 7*(1): 83-96.

Cavoukian, A. (2009). "Privacy by design: The 7 foundational principles". *Information and privacy commissioner of Ontario, Canada*, *5*: 1-12.

Dwork, C. (2008). "Differential privacy: A survey of results". En Agrawal, M., Du, D., Duan, Z. y Li, A. (eds.) *International Conference on Theory and Applications of Models of Computation. TAMC 2008. Lecture Notes in Computer Science, vol 4978* (pp. 1-19). Heidelberg: Springer.

Ferretti, L., Wymant, C., Kendall, M., Zhao, L., Nurtay, A., Abeler-Dörner, L. y Fraser, C. (2020). "Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing". *Science, 368*(6491): eabb6936.

Hinch, R., Probert, W., Nurtay, A., Kendall, M., Wymant, C., Hall, M., Lythgoe, K., Bulas-Cruz, A., Zhao, L., Stewart, A., Ferretti, L., Parker, M., Meroueh, A., Mathias, B., Stevenson, S., Montero, D. Warren, J., Mather,

N. K., Finkelstein, A., Abeler-Dörner, L., Bonsall, D. y Fraser, C. (2020). "Effective configurations of a digital contact tracing app: A report to NHSX". URL=<https://cdn.theconversation.com/static_files/files/1009/Report_-_Effective_App_Configurations.pdf?1587531217>

Grant, C., Griffin, I., McConnell, M., Quiñones-Mateu, M., Schumayer, D. y Hutchinson, D. (2020). "Re-Opening after COVID-19 in New Zealand". *Journal of Conservation and Museum Studies, 18*(1): 4.

NCO. (2019). *Official US Government Information about the Global Positioning System (GPS) and Related Topics*. URL =< https://www.gps.gov/>

Parker, M. J., Fraser, C., Abeler-Dörner, L., & Bonsall, D. (2020). "Ethics of instantaneous contact tracing using mobile phone apps in the control of the COVID-19 pandemic". *Journal of Medical Ethics, 46*(7): 427-431.

Sacks, J. A., Zehe, E., Redick, C., Bah, A., Cowger, K., Camara, M. y Liu, A. (2015). "Introduction of mobile health tools to support Ebola surveillance and contact tracing in Guinea". *Global Health: Science and Practice, 3*(4): 646-659.

Sandvik, K. B. (2020). "'Smittestopp': If you want your freedom back, download now". *Big Data & Society, 7*(2). DOI: 2053951720939985.

Stanley, J. y Granick, J. S. (2020). "The limits of location tracking in an epidemic". *American Civil Liberties Union*. URL=<https://www.aclu.org/sites/default/files/field_document/limits_of_location_tracking_in_an_epidemic.pdf>

Troncoso, C., Payer, M., Hubaux, J. P., Salathé, M., Larus, J., Bugnion, E., Lueks, W., Stadler, T., Pyrgelis, A., Antonioli, D., Barman, L., Chatel, S., Paterson, K., Čapkun, S., Basin, D. Beutel, J., Jackson, D., Roeschlin, M. Leu, P., Preneel, B., Smart, N, Abidin, A., Gürses, S. Veale, M., Cremers, C., Backes, M., Tippenhauer, N. O., Binns, R., Cattuto, C., Barrat, A., Fiore, D., Barbosa, M., Oliveira, R. y Pereira, J. (2020) "Decentralized privacy-preserving proximity tracing". URL=<https://arxiv.org/abs/2005.12273>

Vaughan A. (2020). "Bluetooth may not work well enough to trace coronavirus contacts" *New Scientist,* May 12. URL=<https://www.newscientist.com/article/2243137-bluetooth-may-not-work-well-enough-to-trace-coronavirus-contacts/>

Wu, J., Xie, X., Yang, L., Xu, X., Cai, Y., Wang, T. y Xie, X. (2021). "Mobile health technology combats COVID-19 in China". *Journal of Infection, 82*(1): 159-198.

Yebra, J. M. (2016). "El acceso a la información pública y los requerimientos de identificación". *Revista Española de la Transparencia, 3:* 65-68.

Yin, L., Wang, Q., Shaw, S. L., Fang, Z., Hu, J., Tao, Y. y Wang, W. (2015). "Re-identification risk versus data utility for aggregated mobility research using mobile phone location data". *PloS one, 10*(10): e0140589.