Abriendo la caja de Pandemia: por qué necesitamos repensar el rastreo digital de contactos

CYPRIAN · Cybersecurity, Privacy and Anonymity Lab

01 · MAYO · 2020

Resumen ejecutivo

Durante las primeras fases de la expansión del COVID-19 en Europa, impulsados en buena parte por las experiencias de buena gestión en determinados países asiáticos que vivieron antes el impacto del virus, múltiples expertos europeos de diferentes ámbitos (académico, privado, gubernamental) señalaron el uso de las nuevas tecnologías como uno de los elementos clave para hacer frente a la pandemia. En concreto, las aplicaciones de rastreo digital de contactos se identificaron como una herramienta no sólo útil para frenar la expansión de la pandemia, sino como un elemento esencial para las fases de desescalada o desconfinamiento, que se prevé se puedan prolongar durante un tiempo significativo.

El debate en curso sobre dos métodos alternativos (centralizado y descentralizado) para implementar aplicaciones de rastreo digital de contactos ha servido para poner en evidencia carencias graves de dichas aplicaciones que las convierten, en su concepción actual, en desaconsejables. En la raíz de estas carencias se encuentran unos requisitos de privacidad que no son alcanzables con una tecnología que, como es el caso de Bluetooth Low Energy (BLE), nunca fue concebida para este fin.

En el presente documento se ofrecen argumentos que justifican que, tal como han sido propuestas, las aplicaciones de seguimiento de contactos no ofrecen una garantía total de privacidad a los usuarios, ni son 100% robustas frente a ataques maliciosos, algunos de ellos relativamente sencillos de implementar, escalables, con capacidad de convertirse en masivos y con potenciales consecuencias muy negativas.

Asimismo, se justifica que la tecnología BLE está inherentemente limitada en la fiabilidad de los datos que puede proporcionar, cuestionando su validez como mecanismo de detección de contactos de riesgo. Además, el grado de adopción de BLE, siendo apreciable, dista mucho de alcanzar el nivel necesario para ser efectivo en la contención de la epidemia. Por otra parte, los requisitos de privacidad hacen que estas aplicaciones ni siquiera puedan servir de complemento al rastreo manual.

Concluimos que las tecnologías de base no son suficientemente fiables, robustas ni extendidas como para alcanzar las tasas deseables de detección de contactos. Su adopción, sin consciencia de estas limitaciones, puede conducir a una falsa seguridad que, una vez refutada, se convierta en un elemento desincentivador para su uso.

Desde una perspectiva meramente técnica, desaconsejamos firmemente la adopción inmediata de aplicaciones de rastreo de contactos en tanto no se solucionen satisfactoriamente los problemas identificados.

Esta crisis epidemiológica hubiese supuesto una oportunidad sin precedentes para desplegar el potencial tecnológico europeo y dar una respuesta conjunta a un problema acuciante, poniendo en valor además nuestro marco legal de respeto a la privacidad y a los derechos fundamentales de los ciudadanos. En cambio, las rencillas entre los defensores de los dos modelos propuestos no sólo han complicado la existencia de un sistema europeo interoperable, sino que han puesto en manos de Google y Apple la solución, renunciando una vez más a la soberanía tecnológica y abriendo muchos más interrogantes sobre la privacidad. Buscando evitar un Gran Hermano, los europeos estamos poniendo nuestra privacidad en manos de un Mayor Hermano.

1. Funcionamiento de las aplicaciones digitales de rastreo de contactos

La forma general de operar de estas aplicaciones se basa en el envío, recepción y almacenamiento por parte de los teléfonos móviles, utilizando el protocolo Bluetooth Low Energy (BLE[1]), de una serie de identificadores anónimos (EBID[2]) que cambian continuamente. Cuando una prueba de diagnóstico de COVID-19 determina que una persona está infectada se utilizan los EBID recibidos por su teléfono móvil para determinar los individuos con quien esta persona haya podido estar en contacto, con la proximidad y tiempo suficientes, como para que pudiera existir riesgo de contagio.

Estos identificadores EBID son anónimos y cambian con el tiempo para evitar que se pueda rastrear geográficamente a una persona conociendo simplemente los EBID que transmite su teléfono. Para evitar este riesgo no debe ser posible, dado un conjunto de EBID cualesquiera y sin conocer la clave que los genera, deducir si provienen del mismo dispositivo.

Es importante señalar que la elección de la tecnología BLE responde a una doble necesidad: 1) el intercambio de los EBID entre teléfonos móviles; 2) la medición/estimación de proximidad entre esos teléfonos móviles. BLE es una tecnología de comunicación inalámbrica de bajo consumo, que funciona en la banda ISM de 2.4 GHz. Está disponible comercialmente desde 2009, y en la actualidad está ampliamente extendida en los smartphones. Además, BLE puede establecer comunicación directa entre dos teléfonos (suficientemente cercanos) sin necesidad de usar la red de operador, y por tanto puede llevar a cabo el intercambio de los EBID sin depender de la cobertura disponible en cada momento. En cuanto a su idoneidad como tecnología para estimar la proximidad entre contactos, se discutirá en detalle en la Sección 3. En cualquier caso, es importante decir que para esto último otras tecnologías como el GPS o la triangulación desde estaciones base quedan descartadas debido a que proporcionan una estimación de la posición demasiado burda y/o no funcionan en interiores.

En la actualidad se han definido dos familias de protocolos de rastreo según su nivel de centralización. En ambos casos la protección de la privacidad de los usuarios es un requisito por diseño, y por tanto solo se revela la información estrictamente necesaria para realizar el rastreo de contactos con relevancia epidemiológica:

- **Modelo centralizado**: todos los EBID se generan en un sistema centralizado en base a una clave única, que cambia cada cierto intervalo de tiempo, con la que se cifra un identificador único de cada dispositivo. Este identificador único es también anónimo, pero permanece constante en el sistema. Los teléfonos solicitan periódicamente al sistema los EBID que enviarán en las siguientes horas para que el protocolo pueda funcionar sin conexión a Internet.

  En caso de detectarse una infección, las autoridades sanitarias permitirán que la persona infectada envíe al sistema, de forma anónima, todos los EBID de otros usuarios

[1] https://www.bluetooth.com/learn-about-bluetooth/bluetooth-technology/radio-versions/

[2] EBID es el nombre de los identificadores anónimos temporales en uno de los protocolos, en otros protocolos reciben nombres tales como EphID, Rolling Proximity Identifiers, … Como el propósito del identificador es el mismo en todos los casos, para facilitar la comparación de los protocolos se utilizará siempre el término EBID para referirnos a ellos.

que ha detectado su teléfono móvil en el periodo de tiempo en el que el individuo haya podido contagiar a otras personas.

De manera centralizada se procederá al descifrado de los EBID, para obtener los identificadores únicos de los dispositivos de las personas que están en riesgo de haber sido infectadas y se comunicará este riesgo a los afectados. Los protocolos centralizados incorporan mecanismos para evitar que este aviso suponga un riesgo a la privacidad.

La evaluación del riesgo de contagio tendrá en consideración tanto información obtenida asociada a los EBID (potencia de transmisión y recepción de la señal, número de EBID recibidos, etc.) como información asociada a una epidemia concreta. Adicionalmente podrá utilizar la propia información centralizada del sistema de rastreo para optimizar la evaluación del riesgo.

- **Modelo descentralizado**: Los EBID se generan en cada dispositivo en base a una clave única por móvil que cambia diariamente. En base a esa clave se genera un conjunto de EBID que se transmitirán durante ese día.
  En caso de detectarse una infección, las autoridades sanitarias permitirán que la persona infectada envíe a un repositorio centralizado, de forma anónima, las claves diarias correspondientes al periodo de tiempo en el que el individuo haya podido contagiar a otras personas. Estas claves se denominan claves de diagnóstico.

  Todos los dispositivos consultan periódicamente el repositorio centralizado para obtener las claves de diagnóstico. Con estas claves se generan todos los EBID asociados y se comprueba si están presentes en la lista de los EBID detectados por el dispositivo el día correspondiente a cada clave de diagnóstico.

  En caso de que haya coincidencias, se ejecuta localmente en el dispositivo un algoritmo de evaluación del riesgo, que tendrá en cuenta la duración y proximidad estimada del contacto. Si se supera un determinado umbral se determinará que existe riesgo de contacto y se alertará al usuario.

Las principales diferencias entre ambos modelos son las siguientes:

- **Generación de los EBID**
  En el caso centralizado, los EBID se generan en el servidor y, conociendo la clave correspondiente, es posible obtener el identificador único de la aplicación en un dispositivo concreto. Este identificador es anónimo, pero identifica unívoca y permanentemente[3] un dispositivo.

  En el modelo descentralizado, los EBID se generan en el dispositivo a partir de una clave diaria única en el móvil. Los EBID no contienen ninguna información en sí mismos.

- **Mecanismo de detección de posibles contagios**
  En el modelo centralizado la detección se realiza descifrando los EBID, que fueron recibidos mediante Bluetooth en los dispositivos de las personas diagnosticadas

[3] A no ser que el usuario reinstale la aplicación.

positivas, buscando a continuación los identificadores únicos de aplicación obtenidos al descifrar los EBID en la base de datos centralizada.

En el caso descentralizado se regeneran en cada dispositivo los EBID de las personas diagnosticadas positivas, utilizando las claves de diagnóstico descargadas del repositorio central, y se comparan con los EBID recibidos mediante Bluetooth por el dispositivo. En ningún caso ni los EBID ni las claves diarias de las personas no diagnosticadas abandonan el dispositivo.

- **Evaluación del riesgo de contagio**
  En la versión centralizada el algoritmo de evaluación del riesgo de contagio se puede adaptar rápidamente a la evaluación de la pandemia, aumentando o reduciendo la sensibilidad del algoritmo. Adicionalmente, se puede ajustar progresivamente con información proveniente de nuevos contagios.

  En el modelo descentralizado la adaptación del algoritmo es más lenta, pudiendo suponer una modificación de la aplicación. Al no existir una visión global del rendimiento de la evaluación del riesgo es más complejo ajustar el algoritmo.

Al respecto de la privacidad en ambos modelos, es importante destacar que el Comité Europeo de Protección de Datos (*European Data Protection Board*, EDPB), en el informe [1] donde marca las pautas para el uso de herramientas de rastreo de contactos, ha señalado que ambos modelos, tanto el centralizado como el descentralizado, pueden considerarse opciones viables siempre que se implementen con las medidas de seguridad adecuadas.

Actualmente, los principales actores en cada uno de los modelos son los siguientes:

- Modelo centralizado:
  - Pan-European Privacy Preserving Proximity Tracing (PEPP-PT) [2]
  - ROBust and privacy-presERving proximity Tracing (ROBERT) [3]
- Modelo descentralizado
  - Decentralized Privacy-Preserving Proximity Tracing (DP-3T) [4]
  - Apple & Google Exposure Notification [5][6]

2. Principales críticas a los protocolos de rastreo de contactos

2.1 Críticas respecto a la seguridad y a la privacidad

En este punto se describen las principales críticas a las dos familias de protocolos. Éstas han sido extraídas principalmente de los análisis realizados por cada uno de los defensores de uno de los modelos frente al otro [7][8][9][10][11]. Las críticas se basan en determinadas vulnerabilidades y posibles ataques a cada uno de los protocolos. Tan solo trataremos aquellos que se consideran de mayor impacto o relevancia.

Gran Hermano/Abuso de poder

Esta es la principal crítica de los defensores del modelo descentralizado y presupone posibles usos o procesados maliciosos de la información centralizada que permitan el rastreo de usuarios. Entre los posibles abusos en este sentido se apuntan los siguientes:

- Rastrear usuarios a lo largo del tiempo: Con la información de contactos subidos a la plataforma por las personas infectadas y desanonimizando los mismos (utilizando otras fuentes de datos como cámaras de vigilancia) se podría, a gran escala, rastrear a los usuarios, infectados o no, en su vida diaria. Este objetivo solo es abordable desde un Estado dispuesto a utilizar los datos con propósitos distintos de aquellos para los que fueron adquiridos, contraviniendo así la legislación europea al respecto.
- Etiquetar a usuarios para que sean reconocidos por terceras partes: Como los EBID se generan de forma centralizada en el servidor, se podrían enviar EBID especiales a ciertas personas para que, cuando sus dispositivos los transmitan, puedan ser identificados. Esto simplificaría la desanonimización de los usuarios y su seguimiento persistente a largo plazo.

Aprendizaje del grafo social de usuarios

Otra crítica al modelo centralizado es la capacidad del mismo para generar el grafo de contactos de las personas infectadas. Aunque esto es así por diseño y podría considerarse una ventaja desde el punto de vista del estudio epidemiológico, los detractores de dicho modelo apuntan a que es posible, aunque sea de forma parcial, deducir los grafos de contactos de personas no infectadas, por ejemplo, cuando hayan estado en contacto simultáneamente con una persona infectada.

Creación de falso riesgo individual

Este es un ataque que afecta de forma similar a ambos modelos. Un atacante podría tener interés en señalar a una persona en particular como en riesgo de estar infectada. Para ello, el atacante debe adquirir la capacidad de actuar como un infectado. Esto podría obtenerlo en colusión con algún sanitario que realice las pruebas o mediante otro mecanismo dependiente de cómo se genere la autorización para enviar información a la plataforma centralizada. Según el modelo, el atacante debería conseguir lo siguiente:

- Modelo centralizado: Sería suficiente con añadir un conjunto de EBID del dispositivo de la persona a señalar como potencial contagiada. Para ello debería estar en proximidad de dicha persona en algún momento previo a la subida de los EBID a la plataforma.
- Modelo descentralizado: El atacante debería “inyectar” un conjunto de sus EBID en el dispositivo de la persona a señalar como potencial contagiado. Igualmente tendrá que haber estado en la proximidad de dicha persona.

Creación de falso riesgo masivo

Este ataque es una extensión del anterior, pero en vez de estar dirigido a crear un falso riesgo de contagio a una persona determinada, el objetivo es crear un número alto de falsos contagios potenciales, con el propósito de minar la confianza en el sistema o para elevar el estado de alarma en un país.

Al contrario que en el caso anterior, este ataque no afecta de forma similar a ambos modelos. Aunque el ataque es semejante, en el modelo centralizado se podrían implementar mecanismos para su detección, evitando así lanzar los avisos masivos.

Creación de falso riesgo masivo mediante reenvío de EBID

El propósito de este ataque es el mismo que el anterior: crear un número alto de falsos contagios potenciales, pero utilizando para ello la captura y reenvío de EBID. El ataque es ligeramente distinto según el modelo:

- En el modelo centralizado se debe obtener el mayor número posible de EBID de población en general y emitirlos de nuevo en zonas de gran afluencia de personas, preferiblemente en zonas donde haya una mayor incidencia de la enfermedad o, en general, donde sea más probable que existan personas que acaben dando resultado positivo al COVID-19, como hospitales o centros de salud. En el probable caso de que alguna de estas personas dé positivo y suba sus EBID al sistema centralizado, el atacante habrá conseguido insertar en el sistema un gran número de falsos contactos con una persona infectada.
- En el modelo descentralizado, el ataque funciona a la inversa. El atacante intentará conseguir EBID de personas con probabilidad de dar positivo (por ejemplo, en hospitales o centros de salud) y emitirá de nuevo estos EBID en zonas de gran afluencia. Cuando alguna de las personas cuyos EBID se han reenviado masivamente den positivo y suban a la plataforma sus claves de diagnóstico, un gran número de dispositivos informarán a sus propietarios de haber estado en contacto con una persona infectada.

Hay dos puntos importantes a tener en cuenta. En primer lugar, el ataque no tiene por qué limitarse a una zona concreta, se pueden capturar EBID en múltiples localizaciones, enviarlos por Internet a otras zonas y reenviarlos de forma masiva. En segundo lugar, por la incidencia de la enfermedad, si el ataque se realiza de forma masiva es muy probable que tenga éxito ya que el número de infectados es muy alto.

De nuevo, este ataque no afecta por igual a ambos modelos:

- En el modelo centralizado, los EBID solo son válidos durante un corto periodo de tiempo, en PEPP-PT se pone como ejemplo 1 hora. Esto limita la ventana en la cual sería válida la reemisión de los EBID. Adicionalmente, al igual que en el ataque anterior, en el backend se pueden implementar mecanismos para detectar esta anomalía (un número excesivamente alto de EBID en un periodo de tiempo), y evitar lanzar avisos masivos de riesgo.

- Sin embargo, en el modelo descentralizado los EBID son válidos durante un día[4], y es así por diseño, en un intento de aumentar la privacidad, evitando que la persona avisada pueda deducir el contacto concreto que ha dado positivo. En este caso la ventana es mucho más amplia y no existe un ente centralizado que pueda detectar el ataque, al menos no antes de avisar al usuario del riesgo.

Rastreo de infectados

Esta vulnerabilidad está especialmente presente en el modelo descentralizado, y está señalada como tal en el documento que describe el modelo [4]. Es técnicamente posible instalar sondas que permitan obtener los EBID de todas las personas que acceden a determinados lugares de interés para un atacante. La información de los EBID obtenidos podría ser complementada con otras fuentes de información, por ejemplo, con la instalación de cámaras de vigilancia y acompañarla de un registro del momento exacto en el que se recibe cada EBID. En caso de que, posteriormente, algunos de estos EBID se deriven de alguna clave de diagnóstico, se podría identificar de forma sencilla a la persona infectada.

El modelo centralizado tampoco está totalmente libre de este ataque. En este caso el atacante podría crear múltiples cuentas en el sistema centralizado (ataque *Sybil)* y usar cada una en un intervalo distinto del día, por ejemplo cada 15 minutos, enviando durante ese periodo los EBID correspondientes. Igualmente se podría acompañar de un sistema de videovigilancia. Si posteriormente el atacante es avisado en alguna de sus múltiples cuentas de un contagio podría llegar a reidentificar a la persona infectada, al conocer el intervalo de tiempo exacto en el que estuvo activa esa cuenta particular y con quién estuvo en contacto en dicho momento. Como se puede intuir la complejidad del ataque es mayor, por el número de cuentas a crear, y la eficacia mucho menor, ya que durante el intervalo de tiempo asociado a una de las cuentas se pueden haber "inyectado" los EBID a un mayor número de personas, preservándose en ese caso, hasta cierto punto, la privacidad. Adicionalmente se podrían incorporar controles en el servidor para evitar este tipo de ataques.

Problemas de implementación

Apple y Google se han unido para incluir en sus sistemas operativos móviles, iOS y Android respectivamente, un servicio de rastreo de contactos descentralizado. Cuando este servicio se encuentre disponible, los servicios de salud de los países podrán publicar aplicaciones que utilicen el servicio, siempre y cuando el modelo utilizado por el mismo cubra las expectativas esperadas.

El problema es que, debido a la dificultad de enviar mensajes Bluetooth cuando una aplicación móvil no se encuentra en primer plano, principalmente en iOS, existen dudas de si se podrán implementar de forma eficiente otros protocolos de rastreo de contactos independientes o distintos de los prestados por el servicio del sistema operativo. Esto, aunque celebrado como un éxito inicialmente por los partidarios del modelo descentralizado, también comporta sus problemas, indicados en el siguiente punto.

[4] Valor correspondiente al protocolo DP-3T. En el caso del protocolo de Apple y Google la ventana de ataque sería de dos horas.

2.2 Críticas respecto a la implementación de Apple y Google

Las principales críticas al servicio de rastreo de Apple y Google y señaladas en [12] son las siguientes:

- El servicio de rastreo se integra en el sistema operativo: inicialmente el rastreo de contactos se diseñó como una funcionalidad proporcionada por una aplicación y controlada por ella. El usuario podría en cualquier momento desinstalarla y deshabilitar de esta forma por completo el rastreo de contactos. Al implementarse por Apple y Google en el sistema operativo estará siempre presente, quizás activa, quizás no, creando una función "durmiente" con potencial de vigilancia masiva.
- Confianza en Google y Apple: si la única forma de implementar el rastreo de contactos es la proporcionada por estas empresas, nos obliga a confiar en que no abusarán de esta capacidad en el futuro. Este riesgo se podría mitigar mediante auditorías de software, pero no está claro que estas grandes compañías se vayan a prestar a ello. A este respecto, el Comité Europeo de Protección de Datos se ha pronunciado [1] claramente exigiendo la auditoría independiente de las implementaciones por transparencia, responsabilidad, y para comprobar el cumplimiento estricto de las leyes. El Comité también recomienda encarecidamente la publicación del código fuente para que sea sometido a escrutinio. Estas exigencias se unen a las recomendaciones adoptadas previamente por la Comisión Europea sobre la auditoría de las aplicaciones COVID por parte de entidades independientes.
- Centralización: Aunque Google y Apple implementan a bajo nivel el protocolo descentralizado es posible igualmente construir sobre su implementación una aplicación que realiza una gestión centralizada del rastreo de contactos. Es más, hasta se podría implementar una aplicación que utilizase geolocalización, descartada por todas las partes por considerarla excesivamente intrusiva. Esta debilidad es consecuencia del hecho de que los proveedores del sistema operativo (e incluso fabricantes del terminal) sean los mismos que proporcionan otras aplicaciones y servicios intrusivos con la privacidad; es perfectamente posible para Google o Apple combinar estos datos con las búsquedas de Internet, la geolocalización basada en GPS o en firmas de redes WiFi, los sensores del terminal móvil, etc. para extraer información que ni siquiera está al alcance de los Estados.

3. Sobre la fiabilidad de Bluetooth Low Energy (BLE) para la medición de proximidad entre personas

El 15 de abril la Comisión Europea publicó una guía con los requisitos acordados por los Estados Miembros para el desarrollo de aplicaciones de rastreo de contactos de acuerdo con unos criterios comunes para toda la Unión Europea [13]. Dicha guía define una serie de requisitos funcionales de diferentes tipos: epidemiológicos, técnicos, de interoperabilidad, ciberseguridad, etc.

Los requisitos relativos a la detección de contactos cercanos “epidemiológicamente relevantes” son los mostrados en la siguiente tabla.

Id	Functionality	Description and Recommendation
EF-01	Epidemiological relevance for “close contacts”	Adopt the heuristics as commonly agreed by ECDC (guidance on contact tracing) with Member States as to what is epidemiologically sufficient in terms of proximity as: (i) time duration, (ii) distance, (iii) environmental context
TF-01	Proximity technology	In order to reliably determine the epidemiologically targeted 1.5 meters distance, a resolution of 0.5 meters should be provided, minimizing false positives. 1) App (in conjunction with device/OS) should be able to send and receive and record Bluetooth signals even in the background mode (even when the phone is locked). 2) App should be able to estimate with sufficient accuracy the proximity between mobile phones via Bluetooth signals or other effective and non-tracking techniques 3) App should advertise continuously its presence using a temporary anonymous ID that permits establishing contact with other app users in proximity. 4) App should record and store IDs observed from other mobile phones in epidemiologically relevant proximity on the device 5) App should be able to indicate the Member State in which it is registered
TF-02	Physical proximity	Actual physical proximity should be recorded accurately. Only if a mobile phone is in “epidemiologically relevant” proximity to another mobile phone for an “epidemiologically relevant” period of time as commonly agreed by NHAs (see rows 1 and 2 in part a above), the ID of each phone is stored in encrypted form in the respective other phone.

Tabla 1: requisitos establecidos por la Comisión Europea para las aplicaciones de rastreo de contactos en términos de detección de contactos epidemiológicamente relevantes y proximidad física

El requisito EF-01 hace referencia directa a los criterios heurísticos [14] adoptados por el Centro Europeo para la Prevención y Control de Enfermedades (ECDC, de sus siglas en inglés), recomendados para la realización manual de rastreo de contactos, que distinguen entre **contactos de alto riesgo** y **contactos de bajo riesgo**, según la tabla siguiente:

Alto riesgo	Bajo riesgo
● Mantener contacto cara a cara con un infectado por COVID-19 a dos metros o menos durante 15 minutos o más ● Mantener contacto físico directo con un caso de COVID-19 o haber estado en contacto directo con sus secreciones (por ejemplo a través de un estornudo) ● Compartir un espacio cerrado (por ejemplo un piso, aula, sala de reuniones, etc.) con un caso de COVID-19 durante más de 15 minutos ● En un avión, sentarse a dos asientos de distancia (en cualquier dirección) de un caso COVID-19 ● Ser un sanitario tratando con un caso de COVID-19 sin los preceptivos EPI.	● Mantener contacto cara a cara con un caso COVID-19 a dos metros o menos durante menos de 15 minutos ● Compartir un espacio cerrado con un caso de COVID-19 durante menos de 15 minutos ● Compartir un medio de transporte con un caso de COVID-19, excepto en el caso del avión mencionado arriba ● Ser un sanitario tratando con un caso de COVID-19 provisto de EPI

Tabla 2: criterios para la clasificación de contactos en base al nivel de exposición

Por otra parte, partiendo de la referencia de 2 metros definida por la ECDC, el requisito TF-01 establece una "distancia objetivo" de 1.5 metros para la detección de contacto epidemiológicamente relevante, contando con que la “tecnología de proximidad” utilizada proporcione una resolución mínima de al menos 0.5 metros. El requisito TF-02 establece que un contacto se considerará epidemiológicamente relevante si dicha distancia objetivo se mantiene durante al menos 15 minutos.

Es importante hacer notar que el umbral temporal de 15 minutos se establece forma arbitraria por razones prácticas. A medida que avanza el conocimiento sobre las dinámicas de transmisión del virus, este umbral así como el de distancia epidemiológicamente relevante estarán sujetos a revisión continua por las autoridades sanitarias de cada país. Por esta razón, la guía de la Comisión Europea recomienda que dichos umbrales se puedan variar dinámicamente en las aplicaciones durante el período de evolución de la pandemia. En consecuencia, no es conveniente circunscribir el análisis de viabilidad de la tecnología exclusivamente a una referencia concreta (p.ej., 2 metros). Lo que es más, la distancia podría variar en función de la actividad del usuario: varios expertos recomiendan ya que la distancia de seguridad aumente hasta 4 o 5 metros en caso de deporte activo para evitar el rebufo.

La selección de BLE como tecnología de medición de proximidad supone de entrada una serie de limitaciones importantes para la detección de contactos epidemiológicamente relevantes, de acuerdo con los criterios recogidos en la Tabla 2. Por ejemplo:

- Imposibilidad de distinguir entre espacios cerrados y espacios abiertos, conduciendo por tanto a la imposibilidad de determinar el nivel de riesgo en determinados tipos de contactos.
- Imposibilidad de distinguir entre personas llevando EPI o no, resultando de nuevo inviable distinguir entre contactos de bajo y alto riesgo

- Imposibilidad de detectar contacto directo (por ejemplo, un apretón de manos).

Las dos primeras limitaciones se pueden soslayar asumiendo todos los contactos como de alto riesgo, lo cual lleva de partida a una sobreestimación del número de contactos epidemiológicamente relevantes.

En cuanto a la posibilidad de satisfacer los requisitos TF-01 y TF-02, es necesario preguntarse si la tecnología BLE puede proporcionar la precisión requerida en la estimación de distancias.

En primer lugar es necesario aclarar que BLE no es una tecnología concebida para la estimación de distancias. A pesar de ello, y debido a que es un estándar de comunicaciones muy popular que se puede encontrar en prácticamente la totalidad de dispositivos smartphone modernos, se han realizado numerosos estudios y aplicaciones que tratan de utilizar esta tecnología para localización en interiores y estimación de distancia entre terminales y dispositivos de balizamiento.

Por lo general, la estimación de distancia entre emisor y receptor se calcula en el propio receptor de los mensajes BLE a partir de:

- La potencia de señal transmitida, en caso de que sea incluida por el emisor en el mensaje enviado.
- La potencia de señal recibida por el receptor.
- Las características de propagación radio a la frecuencia de operación (2.4 GHz).

Sin embargo, en la práctica, esta estimación de distancia es poco precisa debido a diversas fuentes de error que hay que tener en cuenta, especialmente:

- La mayoría de circuitos integrados Bluetooth no ofrecen directamente la información de potencia de señal recibida a través de sus interfaces de control, sino que devuelven un parámetro denominado RSSI (*Received Signal Strength Indication*). Este parámetro es definido de forma arbitraria por cada fabricante, y lo único que ha de cumplir es que cuanto más intensa es la señal recibida, mayor debe ser el valor de RSSI[5]. Esto obligaría a calibrar los sistemas de estimación de distancia para cada uno de los circuitos integrados de diferentes fabricantes para que la medida sea equivalente entre ellos.
- La potencia de señal recibida por un terminal depende de la dirección de llegada de dicha señal en relación al diagrama de radiación de su antena receptora. Del mismo modo, el diagrama de radiación de la antena del dispositivo emisor influye en la potencia emitida efectivamente al espacio en una dirección concreta. Por lo tanto, la orientación relativa entre transmisor y receptor afecta de forma muy relevante a la medida de potencia realizada por el receptor.
- Las características de propagación radio a la frecuencia de operación dependen en gran medida del entorno en el que se encuentran los terminales; las posibles reflexiones en objetos y paredes y los fenómenos de dispersión radioeléctrica, que puedan provocar efectos de multitrayecto y desvanecimientos de naturaleza variante en el tiempo; la

[5] Bluetooth Blog, Proximity and RSSI (Online, last visited 28/04/2020) https://www.bluetooth.com/blog/proximity-and-rssi/

existencia de obstáculos en la línea de visión entre los terminales; la absorción radioeléctrica de dichos obstáculos en el rango de frecuencias de trabajo de Bluetooth, etc. [15]

- En el caso concreto de dispositivos tipo smartphone, que los usuarios suelen llevar pegados al cuerpo, también es necesario tener en cuenta que los propios usuarios tienen una gran influencia sobre la propagación de la señal radio Bluetooth [16]. En concreto, la posición sobre el cuerpo del smartphone (bolsillo lateral, bolsillo trasero, bolso, mano…) y la orientación relativa de los cuerpos de los usuarios (de frente, de espaldas, en paralelo…) afectan en gran medida a la propagación y, por lo tanto, a la potencia de señal recibida.

Todas estas limitaciones, sumadas además a otras fuentes de distorsión (temperatura de los circuitos integrados encargados del procesado de señal, interferencias electromagnéticas producidas por otras fuentes de radiación, etc.), hacen que Bluetooth no sea una tecnología suficientemente fiable para la estimación precisa de distancia entre dos usuarios que portan dispositivos de tipo Smartphone [17].

Teniendo en cuenta estas consideraciones, es posible poner como ejemplo de escenarios realistas con cálculos sencillos que facilitan la comprensión de este diagnóstico:

Ejemplo A: Supongamos un par de personas en un entorno abierto, sin obstáculos entre ellas y cada una con un smartphone con capacidad de emitir y recibir mensajes Bluetooth. Supongamos también, por simplicidad del análisis, que los smartphones tienen los mismos circuitos integrados Bluetooth, la misma antena, y que se encuentran orientados en la dirección de máxima ganancia de sus respectivas antenas. Por último, supongamos que los smartphones se encuentran en los bolsillos traseros de los usuarios, y que ambos están dentro de uno de los escenarios considerados de alto riesgo de contagio por el ECDC (a un metro de distancia y frente a frente).

En este escenario, es sencillo calcular las pérdidas en espacio libre asociadas con la propagación de la señal Bluetooth en la distancia que separa a ambos usuarios, que son de aproximadamente 40 dB[6] si los usuarios se encuentran a 1 m de separación. Si a esta atenuación añadimos el efecto del cuerpo humano que, siendo conservadores, incrementaría en unos 10 dB las pérdidas [16] por cada usuario en el trayecto de la señal, obtenemos una atenuación total de 60 dB por propagación.

Suponiendo que ninguno de los otros parámetros (potencia transmitida, orientación de antenas, pérdidas por conexiones, etc.) cambian, consideremos otro escenario, en esta ocasión uno de los considerados completamente fuera de riesgo por el ECDC, con los usuarios de espaldas y con una separación entre ellos de unos 10 m. En este escenario, al no estar los usuarios interpuestos en la línea de comunicación Bluetooth, podemos asumir que las pérdidas por propagación se deben exclusivamente al espacio libre entre los terminales, que repitiendo el cálculo anterior serían de unos 60 dB.

[6] Calculado utilizando la herramienta online: https://www.pasternack.com/t-calculator-fspl.aspx

Es decir, ya en un escenario simplificado como el que se ha analizado, **no sería posible distinguir, atendiendo únicamente a la potencia recibida, entre una situación de alto riesgo infeccioso y una de riesgo prácticamente nulo.**

Ejemplo B: Supongamos un par de personas en un entorno abierto, sin obstáculos entre ellas y cada una con un smartphone con capacidad de emitir y recibir mensajes Bluetooth. Supongamos también, por simplicidad del análisis, que los smartphones tienen el mismo chipset Bluetooth, la misma antena, y que se encuentran orientados en la dirección de máxima ganancia de sus respectivas antenas. Por último, supongamos que los smartphones se encuentran en los bolsillos frontales de los usuarios, y que ambos están dentro de uno de los escenarios considerados de alto riesgo de contagio por el ECDC (a un metro y medio de distancia y frente a frente). Aplicando los cálculos de propagación en espacio libre, en este caso obtenemos unas pérdidas aproximadas de 43 dB debidas a la distancia que separa a ambos usuarios.
Suponiendo que ninguno de los otros parámetros (potencia transmitida, orientación de antenas, pérdidas por conexiones, etc.) cambian, consideremos una modificación del escenario en la que los usuarios se acercan a 1m de distancia, igualmente cara a cara, pero separados por una mampara de cristal (del tipo que se puede encontrar habitualmente en las ventanas domésticas), transformando el escenario en uno de riesgo nulo. Al igual que en el Caso A, las pérdidas por distancia serían de aproximadamente 40 dB, a las que habría que añadir unos 3 dB de atenuación extra debido al obstáculo de cristal interpuesto [18] resultando en un total aproximado de 43 dB de pérdidas.

De nuevo, en un escenario simplificado como el que se ha analizado, **no sería posible distinguir, atendiendo únicamente a la potencia recibida, entre una situación de alto riesgo infeccioso y una de riesgo nulo.**

En los casos revisados solo se han tenido en cuenta algunos de los parámetros mencionados inicialmente, buscando deliberadamente escenarios en los que se pone de manifiesto la complejidad para estimar distancias en función únicamente de la potencia de señal recibida. En las situaciones reales, esta estimación de distancia es si cabe más compleja, por lo que no es recomendable seguir este mecanismo para alcanzar un resultado preciso y confiable. Asimismo, se puede argumentar que las mismas conclusiones son aplicables a otras tecnologías de comunicación en la banda de frecuencias de 2.4 GHz (p.ej. Bluetooth EDR, WiFi o Zigbee), siempre que la estimación de distancias se base exclusivamente en la potencia de señal recibida.

Todas estas limitaciones nos llevan a pensar en la necesidad de otras tecnologías, complementarias o alternativas, para el cálculo de la proximidad entre usuarios. Por una parte, se puede obtener información contextual a partir de otras señales:

- Triangulación o trilateración a partir de estaciones base de telefonía móvil.
- Identificadores de las redes WiFi recibidas en un punto. Esta modalidad y la anterior, disponibles en el propio smartphone, pueden servir para discriminar entre exterior o interior.
- Sensores adicionales, como acelerómetros para saber la orientación de la antena del móvil, o de infrarrojos, para conocer si está guardado en un bolsillo.

Las prestaciones alcanzables con las tecnologías anteriores, en todo caso limitadas, se pueden mejorar sustancialmente con técnicas de procesado de señales que, por ejemplo, hagan una monitorización inteligente de las señales recibidas con el objeto de mejorar la información contextual. Asimismo, se pueden establecer fuentes adicionales de información que permitan ayudar a la estimación de distancias en entornos concretos, por ejemplo balizas que indiquen si los usuarios se encuentran en un entorno cerrado o en exteriores, la densidad de obstáculos, etc.

Por otra parte, se pueden emplear otras soluciones complementarias, aunque la mayor parte de ellas tienen la desventaja de no estar disponibles en terminales de uso común, por ejemplo:

- Estimación de distancias basada en ultrasonidos [19], que eliminarían los problemas de falsos positivos asociados a la transmisión de señales radio a través de separadores físicos (paredes, mamparas, etc.).
- Estimación de distancias basada en tiempos de propagación de la señal radio (Time of Arrival, ToA), en lugar de potencia, como por ejemplo mediante el uso de UWB (ultrawideband) [20].
- Uso de dispositivos específicos con capacidad de comunicación óptica para la identificación de contactos

4. Sobre la adopción de aplicaciones de rastreo de contactos

Complementando nuestro análisis, cabe dedicar un apartado al grado de adopción necesario para el adecuado funcionamiento de este tipo de aplicaciones. En primer lugar, es menester señalar que el país que probablemente ha tenido más éxito conteniendo el avance del virus ha sido Corea del Sur y, aunque lo ha conseguido aplicando un enorme celo al rastreo de contactos, no ha puesto en marcha una app como las que se discuten en Europa. El rastreo ha sido "manual", a base de investigar concienzudamente los potenciales contactos de los infectados, empleando todos los medios disponibles: entrevistas, rastreo de usos de tarjetas de crédito, análisis de grabaciones de cámaras de videovigilancia, etc. Este rastreo manual se ha complementado con una app gubernamental,[7] que vigila mediante GPS si los infectados cumplen la cuarentena, y otras aplicaciones[8] que alertaban a los ciudadanos de la presencia de infectados en zonas próximas, detallando incluso sus recorridos en transporte público. Ni que decir tiene que este caso de éxito es enormemente invasivo con la privacidad, pero da una idea de los sacrificios a los que puede ser necesario llegar, aun de forma transitoria, para conseguir un rastreo de contactos efectivo.

Otro caso que ha sido discutido con detalle en los medios generalistas es el de Singapur, que inicialmente se puso como caso de éxito de efectividad de las aplicaciones de seguimiento de contactos[9], por su capacidad de contener la expansión de la CoVid-19 en fases iniciales. Sin

[7] Self-quarantine safety protection app: http://ncov.mohw.go.kr/upload/ncov/file/202004/1585732793827_20200401181953.pdf

[8] Por ejemplo: Corona 100, CoronaNow, Corona Map…

[9] https://www.businessinsider.com/singapore-coronavirus-app-tracking-testing-no-shutdown-how-it-works-2020-3?IR=T

embargo, cada vez más indicios apuntan a que la app de Singapur (Tracetogether[10]) poco o nada tuvo que ver en ese éxito[11] (Singapur también recurrió al rastreo manual, como en Corea del Sur), dado que su tasa de adopción por parte de la población fue muy baja, inferior al 20%. De hecho, Singapur ha sido mucho menos exitoso en frenar un segundo rebrote[12].

Es razonable, por tanto, preguntarse cuál es la tasa de adopción de las aplicaciones de rastreo de contactos a la que éstas comienzan a ser efectivas. El trabajo más citado que da respuesta a esta pregunta es el de Ferretti et al. [21], publicado recientemente, y que está basado en un modelo estadístico de variación temporal de la infectividad, con parámetros e intervalos de confianza estimados a partir de datos empíricos, para obtener un valor del índice de reproducción básico R_0. El estudio relaciona la rapidez y efectividad con que se pone en cuarentena a los contactos de un infectado que presenta los primeros síntomas, con la tasa de éxito en la detección de casos. Esencialmente, para alcanzar una alta efectividad en contener la epidemia se deben combinar unas tasas de detección de contagiados sintomáticos y de sus contactos suficientemente altas, con una alta rapidez de respuesta en el aislamiento de contactos. En este último aspecto, las aplicaciones son imbatibles, porque permiten una comunicación casi instantánea a los contactos. En el estudio de Ferretti et al. se concluye que un exponente de crecimiento menor que 1 (equivalente a la contención de la epidemia) es alcanzable para una comunicación instantánea a partir de un 50% de éxito en la detección de contagiados sintomáticos y de aproximadamente un 60% en la detección de sus contactos. Teniendo en cuenta que no todos los individuos (ni sus contactos) tendrán instalada la aplicación, para alcanzar una tasa del 60% de éxito es necesaria una tasa de adopción del 77%, que sube al 80% si un 10% de los contactos notificados no se llegan a poner en cuarentena.

Por desgracia, una tasa de adopción del 80% parece difícilmente alcanzable en la práctica: a las personas que no emplean un smartphone, hay que sumar aquellas que no disponen de comunicaciones BLE o que las desactivarán en el suyo para ahorrar batería, además de todas aquellas que no instalarán la aplicación, o que la instalarán pero no la llegarán a abrir o a activar.

La tasa de adopción del 80% además debería incrementarse considerando, como se ha visto en este documento, que no todos los contactos son correctamente detectables por las limitaciones de la tecnología BLE. Si supusiésemos que un 15% de los contactos con un infectado no se detectan correctamente, la tasa de adopción necesaria aumentaría hasta un 83%.

Para hacernos una idea de lo difícil que es alcanzar estas tasas, el porcentaje de penetración de los smartphones en España según algunos análisis puede ser cercano al 90% [22]; de ellos, una estimación bastante optimista es que el 90% implementan BLE[13]. Incluso en EE.UU., donde el empleo de Bluetooth está más extendido, solo el 45% de los usuarios lo mantiene encendido[14]. Estos porcentajes nos dicen que una tasa de adopción realista en nuestro país no sería superior al 36%, incluso siendo optimistas. Muy lejos, por tanto, del porcentaje deseable.

---

[10] https://www.tracetogether.gov.sg/

[11] https://www.reuters.com/article/us-health-coronavirus-apps/bluetooth-phone-apps-for-tracking-covid-19-show-modest-early-results-idUSKCN2232A0

[12] https://www.nytimes.com/2020/04/20/world/asia/coronavirus-singapore.html

[13] https://m.rover.io/the-straight-goods-on-bluetooth-how-many-consumers-have-it-on-d0ebe3b5d718

[14] https://blog.beaconstac.com/2016/05/7-ways-businesses-can-encourage-users-to-turn-their-bluetooth-on/

Por otra parte, la relativa facilidad con que se pueden lanzar ataques contra el protocolo con los que generar de forma masiva falsos contactos con infectados, como hemos discutido en la Sección 2.1, tendría un indudable efecto desmotivador si se reciben falsas alarmas en los smartphones de los usuarios, hasta el punto de que éstos podrían desinstalar la aplicación o, lo que es equivalente en términos de adopción efectiva, hacer caso omiso a sus notificaciones.

Finalmente cabe indicar que, conscientes de la práctica imposibilidad de alcanzar las tasas de adopción requeridas, algunos defensores de las aplicaciones de rastreo de contactos propugnan su despliegue a pesar de todo, alegando que pueden servir de complemento al rastreo manual[15]. Desgraciadamente, una vez más la anonimidad extrema que se persigue en dichas aplicaciones se vuelve en su contra a la hora de emplearlas como complemento, ya que no hay forma (sin quebrantar el anonimato) de eliminar potenciales contactos ya notificados y, en consecuencia, reducir el trabajo de los investigadores dedicados al rastreo manual. Tampoco deja de llamar la atención que defensores acérrimos de la privacidad sugieran ahora complementarse con métodos que entrañan un peligro para la misma, como sin duda ocurre con el rastreo manual.

5. Otros aspectos a considerar

Este documento se ha centrado fundamentalmente en los aspectos técnicos de las aplicaciones de rastreo de contactos. Sin embargo, el tratamiento de este tema desde una perspectiva exclusivamente técnica deja al margen de momento otras perspectivas complementarias, relacionadas entre sí, que consideramos necesarias.

Dado que estos ámbitos de conocimiento quedan lejos de las competencias de los autores, nos limitaremos aquí principalmente a formular algunas preguntas que consideramos relevantes. Desde un punto de vista epidemiológico

- En primer lugar cabe preguntarse si la información proporcionada por las aplicaciones de rastreo de contactos al sistema sanitario es suficiente en una situación de emergencia sanitaria como la que estamos viviendo. Uno de los argumentos de los partidarios de los sistemas centralizados es la capacidad de estos sistemas para reconstruir grafos de contacto social de los infectados, que pueden aportar información muy relevante para entender las dinámicas de expansión de la pandemia, especialmente si se cruzan con datos complementarios de tipo demográfico, temporal, geográfico, etc. Es evidente que estos datos revelan más información privada que el mero tiempo de exposición y distancia de contacto, y es precisamente por esto que los sistemas descentralizados tratan de evitar, por diseño, que se pueda inferir este tipo de información, por considerarse demasiado intrusiva. Los investigadores M. Salathé y C. Cattuto (parte del equipo detrás del protocolo descentralizado DP-3T) abordan esta cuestión brevemente [24] pero sin entrar a valorar la utilidad epidemiológica de los datos complementarios.

[15] https://maldita.es/malditatecnologia/2020/04/30/contact-tracing-rastreo-contactos-apps/

- Por tanto, la pregunta anterior puede reformularse de un modo más general de la siguiente forma: ¿cuál es el equilibrio óptimo entre privacidad y utilidad epidemiológica?

Desde una perspectiva legal

- El Comité Europeo de Protección de Datos, en respuesta a consultas específicas sobre las aplicaciones de rastreo de contactos [1], ha concluido sobre estas que tanto los modelos centralizados como los descentralizados pueden cumplir perfectamente con la normativa europea de protección de datos, siempre que se implementen las medidas de seguridad adecuadas. Es cierto que la Comisión Europea ha expresado su preferencia por el modelo descentralizado [23], por estar más alineado con el principio de minimización de datos, pero como señalamos más arriba, el modelo centralizado puede ser ventajoso a la hora de proporcionar más información útil desde el punto de vista epidemiológico.
- En vista de esto, surgen múltiples preguntas. Por ejemplo: ¿hasta qué punto debe primar el derecho a la privacidad sobre la utilidad sanitaria? En caso de ser diagnosticado positivo, ¿es razonable poder decidir individualmente si aportar a los epidemiólogos, a través de la app, información valiosa para identificar posibles contagiados? (recordemos que en un escenario de rastreo manual se pide que se revelen los potenciales contagiados) ¿Tiene sentido desactivar la app de rastreo a voluntad para evitar detectar ciertos contactos?

Por último, desde un punto de vista sociológico

- ¿Estamos los ciudadanos dispuestos a ceder más información privada a cambio de ayudar en la lucha contra la propagación de la pandemia? ¿Hasta qué punto? ¿Cuál es el beneficio mínimo exigido para que colaboremos?
- ¿Cómo afecta a la sensación de protección/seguridad el hecho de usar las aplicaciones de rastreo de contactos? ¿Seremos más propensos a incurrir en actitudes de riesgo por sentirnos protegidos?

6. Conclusiones

El enfrentamiento de las facciones PEPP-PT y DP-3T ha contribuido a identificar graves problemas inherentes a las aplicaciones de rastreo de contactos que afectan tanto a las implementaciones centralizadas como a las descentralizadas. Ninguna de ellas ofrece una garantía total de privacidad a los usuarios, ni es 100% robusta frente a ataques maliciosos, algunos de ellos relativamente sencillos de implementar, escalables, con capacidad de convertirse en masivos y con potenciales consecuencias muy negativas. Como se ha justificado, **además de existir un compromiso entre privacidad y utilidad epidemiológica, también hay otro entre privacidad y robustez frente a ataques**: las soluciones descentralizadas entrañan menores riesgos para la privacidad, pero son más vulnerables a ataques masivos, que resultan más difíciles de detectar por ausencia de una entidad central que descubra la anomalía.

Por otra parte, el análisis de **la tecnología seleccionada para la medición de proximidad (BLE) revela serias limitaciones**, inherentes a la propia tecnología, que comprometen su validez para aportar información adecuada y relevante desde un punto de vista epidemiológico.

Podemos concluir que **las tecnologías de base no son suficientemente fiables y robustas como para alcanzar los requisitos deseables en una aplicación de rastreo de contactos**. Su adopción, sin consciencia de estas limitaciones, puede conducir a una falsa seguridad que, una vez refutada, se convierta en un elemento desincentivador para su uso.

Por tanto, desde una perspectiva meramente técnica y sin entrar a valorar otros aspectos, **desaconsejamos firmemente la adopción inmediata de aplicaciones de rastreo de contactos** en tanto no se solucionen satisfactoriamente los problemas identificados. **Esta conclusión es independiente de si se emplea un protocolo centralizado o descentralizado y es consecuencia de la combinación de unos requisitos de privacidad muy exigentes con una tecnología de medición de proximidad poco adecuada para este propósito.**

Al margen de las limitaciones de la tecnología, **el grado de adopción de BLE, siendo apreciable, dista mucho de alcanzar el nivel necesario** para ser efectivo en la contención de la epidemia; por otra parte, con unos requisitos de anonimidad tan elevados, **el rastreo de contactos propuesto ni siquiera encuentra fácil acomodo como complemento a métodos de rastreo manual**.

El rastreo de contactos es sin duda una valiosa herramienta en la lucha contra la propagación del COVID, y como tal es muy deseable desarrollar tecnologías digitales que permitan una implementación más eficiente y efectiva. Desgraciadamente, todavía no nos encontramos en condiciones de dar ese paso con garantías. Países como Bélgica y Holanda que inicialmente estaban entre los promotores del despliegue de aplicaciones de rastreo digital han renunciado recientemente a ellas y optarán por un rastreo manual[16].

La problemática del rastreo digital de contactos motivada por la crisis del COVID nos deja también otros aprendizajes.

Esta crisis epidemiológica ha supuesto una oportunidad sin precedentes para desplegar el potencial tecnológico europeo y dar una respuesta conjunta a un problema acuciante, poniendo en valor además nuestro marco legal de respeto a la privacidad y a los derechos fundamentales de los ciudadanos. Sin embargo, el objetivo inicial de consensuar un sistema europeo de rastreo digital de contactos se ha visto truncado desde el momento en el que PEPP-PT y DP-3T rompieron su colaboración. Desde entonces existen, como mínimo, dos sistemas distintos que van a convivir en Europa, complicando enormemente la disponibilidad de un sistema europeo interoperable, limitando aún más la utilidad de estas aplicaciones. Y, lo que es peor, **se ha roto la confianza entre instituciones y se han instaurado rivalidades que costará reconciliar**.

La implementación eficiente de las aplicaciones de rastreo de contactos requiere el acceso de bajo nivel a ciertas características del sistema operativo de los teléfonos móviles, que en un 99% están controlados por Google y Apple.[17] Esta situación hace evidente la **dependencia de los**

[16] https://elpais.com/tecnologia/2020-04-23/francia-pide-a-apple-y-google-que-limiten-la-privacidad-de-los-usuarios-para-crear-su-app-de-rastreo.html

[17] https://www.statista.com/statistics/272698/global-market-share-held-by-mobile-operating-systems-since-2009/

gobiernos europeos de Google y Apple a la hora de implantar sus propias estrategias de rastreo de contactos, poniendo de manifiesto el ya conocido problema europeo de soberanía tecnológica. No deja de ser paradójico que buscando evitar un Gran Hermano, los europeos estemos poniendo nuestra privacidad en manos de un Mayor Hermano.

Por último, los autores de este documento creemos que para abordar adecuadamente el problema del rastreo digital de contactos es necesario considerar al menos cuatro dimensiones:

1. Tecnológica: adecuada medición de proximidad y protocolos que garanticen la seguridad y la privacidad, tanto en el diseño como en la implementación.
2. Epidemiológica: definición de criterios de riesgo, datos esenciales vs. deseables para el control de la epidemia, ...
3. Legal: prevalencia de derechos de privacidad sobre salud, voluntariedad vs. obligación de aportar datos, ...
4. Social: grado de aceptación por parte de la sociedad, percepción de beneficio y protección, motivación de uso...

De estas cuatro dimensiones, tan solo la primera ha sido analizada con cierta profundidad en el presente documento, y es importante señalar que todas ellas están interrelacionadas. Dado que este pretende ser un documento vivo y abierto, desde aquí invitamos a expertos de campos complementarios al nuestro a que contribuyan en versiones futuras.

Autores

Juan González Martínez, GRADIANT (jgonzalez@gradiant.org)

Fernando Pérez González, AtlantTIC - Universidad de Vigo (fperez@gts.uvigo.es)

Luis Pérez Freire, GRADIANT (lpfreire@gradiant.org)

David Chaves Diéguez, GRADIANT (dchaves@gradiant.org)

Sobre CYPRIAN

CYPRIAN, CYbersecurity, PRIvacy and Anonymity Lab, fue creado en 2018 como un laboratorio conjunto de investigación en ciberseguridad entre el centro de investigación atlanTTic de la Universidad de Vigo y Gradiant.

CYPRIAN tiene como objetivo principal la generación de conocimiento experto y su transferencia al mercado en los campos de la ciberseguridad, la privacidad y la anonimidad, para dar respuesta a los retos modernos de la sociedad digital. CYPRIAN aúna la investigación en criptografía y técnicas de preservación de la privacidad con un compromiso por el desarrollo de soluciones prácticas a problemas reales. Para ello, AtlantTIC y Gradiant suman en CYPRIAN a investigadores e ingenieros con años de experiencia y probada valía profesional.

Las actividades concretas que se desarrollan en el marco de CYPRIAN incluyen el desarrollo conjunto de proyectos de I+D, la realización conjunta de tesis doctorales, acciones conjuntas de transferencia con la industria, la compartición de equipamientos, y el asesoramiento tecnológico.

CYPRIAN supone dar forma institucional a la trayectoria de colaboración entre la Universidad de Vigo y Gradiant, que desde 2008 han colaborado en más de 70 proyectos de I+D. Algunos ejemplos de la fructífera colaboración entre ambas entidades han sido el proyecto europeo WITDOM, enmarcado en el programa H2020 cuya finalidad se centraba en administrar mecanismos que garanticen que los datos de los usuarios estén en todo momento protegidos y que ni tan siquiera el proveedor de la nube los conozca; o la investigación desarrollada en el marco de SCAPE, enfocado al procesado seguro de la información en entornos *cloud*.

Referencias

[1] European Data Protection Board. Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak. Adopted on 21 April 2020. https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-042020-use-location-data-and-contact-tracing_en

[2] PEPP-PT - Data Protection and Information Security Architecture https://github.com/pepp-pt/pepp-pt-documentation/blob/master/10-data-protection/PEPP-PT-data-protection-information-security-architecture-Germany.pdf

[3] PRIVATICs team, INRIA - Fraunhofer AISEC - ROBERT: ROBust and privacy-presERving proximity Tracing https://github.com/ROBERT-proximity-tracing/documents/blob/master/ROBERT-specification-EN-v1_0.pdf

[4] Troncoso et al - Decentralized Privacy-Preserving Proximity Tracing https://github.com/DP-3T/documents/blob/master/DP3T%20White%20Paper.pdf

[5] Apple/Google - Exposure Notification - Bluetooth especification https://covid19-static.cdn-apple.com/applications/covid19/current/static/contact-tracing/pdf/ExposureNotification-BluetoothSpecificationv1.1.pdf

[6] Apple/Google - Exposure Notification - Cryptography Specification https://covid19-static.cdn-apple.com/applications/covid19/current/static/contact-tracing/pdf/ExposureNotification-CryptographySpecificationv1.1.pdf

[7] The DP-3T Project - Security and privacy analysis of the document 'PEPP-PT: Data Protection and Information Security Architecture' https://github.com/DP-3T/documents/blob/master/Security%20analysis/PEPP-PT_%20Data%20Protection%20Architechture%20-%20Security%20and%20privacy%20analysis.pdf

[8] The DP-3T Project - Security and privacy analysis of the document 'ROBERT: ROBust and privacy-presERving proximity Tracing' https://github.com/DP-3T/documents/blob/master/Security%20analysis/ROBERT%20-%20Security%20and%20privacy%20analysis.pdf

[9] The DP-3T Project - Privacy and Security Risk Evaluation of Digital Proximity Tracing Systems https://github.com/DP-3T/documents/blob/master/Security%20analysis/Privacy%20and%20Security%20Attacks%20on%20Digital%20Proximity%20Tracing%20Systems.pdf

[10] Inria - Proximity Tracing Applications: The misleading debate about centralised versus decentralised approaches https://github.com/ROBERT-proximity-tracing/documents/blob/master/Proximity-tracing-discussion-EN.pdf

[11] Vaudenay S. - Analysis of DP3T Between Scylla and Charybdis https://eprint.iacr.org/2020/399.pdf

[12] Hoepman J. - Google Apple Contact Tracing (GACT): a wolf in sheep's clothes https://blog.xot.nl/2020/04/19/google-apple-contact-tracing-gact-a-wolf-in-sheeps-clothes/

[13] eHealth Network. Mobile applications to support contact tracing in the EU's fight against COVID-19 - Common EU Toolbox for Member States.Version 1.0. 15 April 2020. https://ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19_apps_en.pdf

[14] European Centre for Disease Prevention and Control. Contact tracing: public health management of persons, including healthcare workers, having had contact with COVID-19 cases in the European Union – second update 8 April 2020. Technical report. https://www.ecdc.europa.eu/sites/default/files/documents/Contact-tracing-Public-health-management-persons-including-healthcare-workers-having-had-contact-with-COVID-19-cases-in-the-European-Union%E2%80%93second-update_0.pdf

[15] NIST Smart Grid Interoperability Panel, Guidelines for Assessing Wireless Standards for Smart Grid Applications (Online, last visited 28/04/2020). https://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.7761r1.pdf

[16] Januszkiewicz, Ł. (2018). Analysis of Human Body Shadowing Effect on Wireless Sensor Networks Operating in the 2.4 GHz Band. Sensors, 18(10), 3412.

[17] Dong, Q., & Dargie, W. (2012, August). Evaluation of the reliability of RSSI for indoor localization. In 2012 International Conference on Wireless Communications in Underground and Confined Areas (pp. 1-6). IEEE.

[18] Mohammad, L., & El-Hakim, R. A. (Eds.). (2019). Sustainable Issues in Transportation Engineering: Proceedings of the 3rd GeoMEast International Congress and Exhibition, Egypt 2019 on Sustainable Civil Infrastructures–The Official International Congress of the Soil-Structure Interaction Group in Egypt (SSIGE). Springer Nature.

[19] Filonenko, V., Cullen, C., & Carswell, J. (2010, September). Investigating ultrasonic positioning on mobile phones. In 2010 International Conference on Indoor Positioning and Indoor Navigation (pp. 1-8). IEEE.

[20] Electronic Design, What's The Difference Between Measuring Location By UWB, Wi-Fi, and Bluetooth? (Online, last visited 28/04/2020) https://www.electronicdesign.com/technologies/communications/article/21800581/whats-the-difference-between-measuring-location-by-uwb-wifi-and-bluetooth

[21] L. Ferretti, C. Wymant, M. Kendall, L. Zhao, A. Nurtay, L. Abeler-Dörner, M. Parker, D. Bonsall, C. Fraser: Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing. Science, 31 March 2020. http://science.sciencemag.org/content/early/2020/04/09/science.abb6936.abstract

[22] Deloitte. Estudio de consumo móvil en España. 2017. https://www2.deloitte.com/es/es/pages/technology-media-and-telecommunications/articles/consumo-movil-espana.html

[23] European Commission. Guidance on Apps supporting the fight against COVID 19 pandemic in relation to data protection. 16 April 2020. https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1587141168991&uri=CELEX:52020XC0417(08)

[24] M. Salathé, C. Cattuto.COVID-19 Response: What Data Is Necessary For Digital Proximity Tracing? https://github.com/DP-3T/documents/blob/master/COVID19%20Response%20-%20What%20Data%20Is%20Necessary%20For%20Digital%20Proximity%20Tracing.pdf