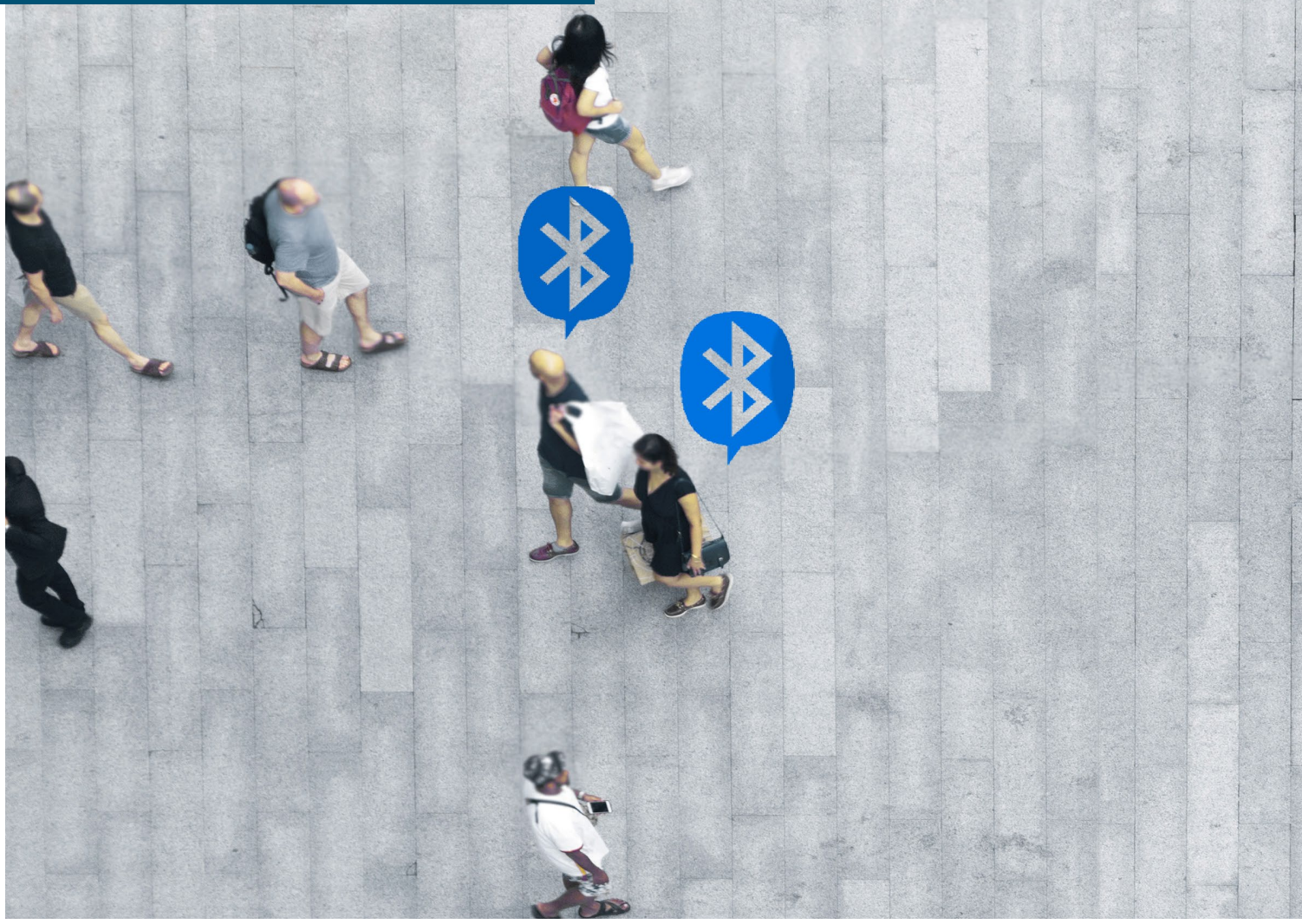
Las aplicaciones de trazabilidad de contactos y notificación de exposición como apoyo a la gestión de la pandemia



ALEJANDRO HEVIA

PhD en Ciencias de la Computación por la University of California, San Diego, Estados Unidos. Académico del Departamento Ciencias de la Computación, Universidad de Chile. Director del Laboratorio de Criptografía Aplicada y Ciberseguridad, CLCERT, Universidad de Chile.
ahevia@dcc.uchile.cl

ALEJANDRO JARA

PhD en Ciencias (Matemática) por la Catholic University of Leuven, Bélgica. Académico de la Facultad de Matemáticas, Pontificia Universidad Católica de Chile. Director del Núcleo Milenio MiDaS.
ajara@mat.puc.cl

ALEJANDRO JOFRÉ

PhD en Matemática Aplicada por la Université de Pau, Francia. Académico del Departamento de Ingeniería Matemática, Universidad de Chile. Investigador del Centro de Modelamiento Matemático, Universidad de Chile - UMI CNRS2807.
ajofre@dim.uchile.cl

ALEJANDRO MAASS

PhD en Matemática por la Université Aix-Marseille, Francia. Académico del Departamento de Ingeniería Matemática, Universidad de Chile. Director del Centro de Modelamiento Matemático, Universidad de Chile - UMI CNRS2807.
amaass@dim.uchile.cl

PABLO A. MARQUET

PhD en Biología por la University of New Mexico, Estados Unidos. Académico del Departamento de Ecología, Pontificia Universidad Católica de Chile.
pmarquet@bio.puc.cl

DIEGO SECO

PhD en Ciencias de la Computación por la Universidade da Coruña, España. Académico del Departamento de Ingeniería Informática y Ciencias de la Computación, Universidad de Concepción. Investigador del Instituto Milenio Fundamentos de los Datos (IMFD).
dseco@udec.cl

Introducción

La Organización Mundial de la Salud (OMS) recomienda como una de las estrategias centrales para contener la pandemia COVID-19, la de testeo, trazabilidad y aislamiento (TTA)[1], la cual fue acogida por el Ministerio de Salud de Chile [1]. Aplicada de manera adecuada, esta estrategia permite romper la cadena de contagio al detectar tempranamente casos COVID positivos, identificar a sus contactos, y aislarlos de manera oportuna. Se trata de una estrategia clásica en epidemiología, cuya aplicación más tradicional se basa en disponer de *trazadores* que entrevistan a los casos confirmados para obtener información de las personas con las que han estado en contacto *estrecho*[2] durante los últimos días. Entre las principales dificultades para aplicar la estrategia de manera exitosa es conocida la necesidad de contar con un número elevado de trazadores con una capacitación adecuada[3], además de ser un proceso sujeto a ineficiencias en la detección de contactos, debido principalmente a que las personas entrevistadas pueden olvidar algunos de los contactos que tuvieron durante el período de tiempo en el cual podrían haber transmitido la enfermedad y, además, debido a que pueden haber transmitido la enfermedad a personas desconocidas, al compartir espacios comunes como el transporte público. Por otro lado, el número requerido de trazadores depende de la carga de la enfermedad en el tiempo y espacio, lo que genera complicaciones adicionales en países de gran extensión territorial y donde la epidemia no se desarrolla de forma sincrónica. Es en este contexto donde los sistemas de información pueden servir de ayuda para mejorar la eficacia y eficiencia de la estrategia.

Esta tecnología no ha sido creada como un reemplazo a la trazabilidad manual, sino como un complemento.

En Chile, el principal sistema de información en la gestión de la pandemia ha sido Epivigila, sistema desarrollado por el equipo de la Dra. Carla Taramasco (Universidad de Valparaíso) entre diciembre de 2013 y noviembre de 2015. Se trata de un sistema de registro y vigilancia de los casos de enfermedades de notificación obligatoria, como es el caso del COVID-19. Dada la magnitud de la pandemia, este sistema se ha ido reforzando durante el desarrollo de la misma, además de avanzar hacia una interoperabilidad que facilite su integración con otros sistemas de apoyo en la gestión de la pandemia. Un ejemplo de dichos sistemas es el Monitor Esmeralda, desarrollado por el Servicio de Salud de Iquique, con el objetivo de facilitar el seguimiento de los casos en todos sus estados hasta el término de la cuarentena.

En este artículo nos centramos en una tecnología complementaria a las anteriores denominada *trazabilidad digital de contactos y notificación de exposición*, conocida también internacionalmente como *digital contact tracing*, o bien *exposure notification*. Ella busca identificar potenciales contagios vía contactos estrechos, o simplemente notificar de tal contacto directamente a la persona expuesta.[4] Esta tecnología se basa en el uso de dispositivos que detectan usuarios que estuvieron en contacto con casos confirmados, por tanto automatizando el proceso de trazabilidad, mejorando sus ineficiencias e incrementando su alcance, o bien, automatizando el proceso de alerta (o notificación) de exposición al usuario. Antes de entrar en los detalles, es importante destacar que esta tecnología no ha sido creada como un reemplazo a la trazabilidad manual, sino como un complemento, debido principalmente a las limitaciones que también revisaremos en este artículo. También se debe resaltar que, si bien todavía no hay estudios concluyentes que muestren su eficacia, es una apuesta a nivel mundial cuyos resultados posiblemente se verán *a posteriori*.

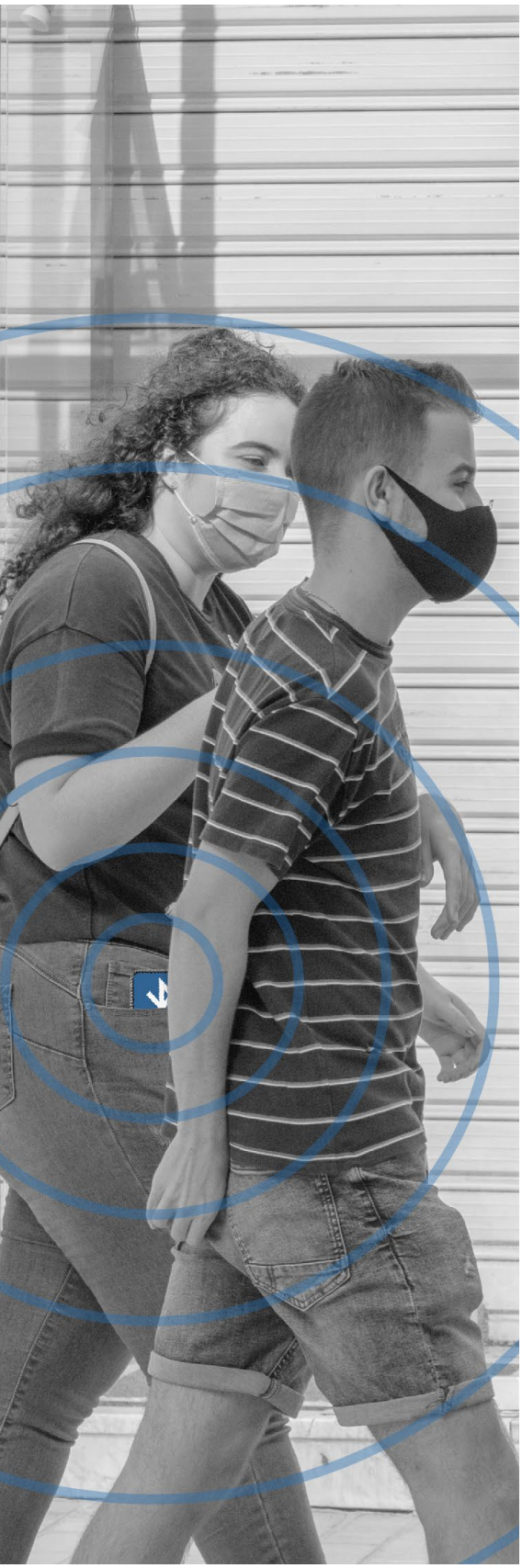
A nivel general, las tecnologías de *trazabilidad de contactos o notificación de exposición* se pueden clasificar en centralizadas versus descentralizadas [4]. El término hace referencia a dónde se almacena la mayor cantidad de la información y se realiza su procesamiento. En una aproximación centralizada, los dispositivos son principalmente generadores de información que transmiten a servidores centralizados, los cuales se encargan de todo el almacenamiento y procesamiento, enviando como resultado de vuelta las alertas oportunas. Por otro lado, en una aproximación descentralizada gran parte de la información se almacena en los propios dispositivos, que también

1 | La estrategia se conoce internacionalmente como *contact tracing*, definida como el proceso de identificación, evaluación y manejo de personas que han estado expuestas a una enfermedad para prevenir la transmisión posterior.

2 | La CDC (Centers for Disease Control and Prevention) lo define como alguien que ha estado a menos de 2 metros de una persona contagiada durante al menos 15 minutos, contando desde 2 días antes del inicio de síntomas (o 2 días antes de la toma de muestra para asintomáticos).

3 | https://www.cdc.gov/coronavirus/2019-ncov/php/principles-contact-tracing.html.

4 | La terminología utilizada ha variado en el tiempo. Las primeras referencias fueron a *digital contact tracing* y *proximity tracing* por analogía a la trazabilidad. La refocalización en alertar a los usuarios más que trazar los contagios hizo surgir los términos *proximity alerting* o *exposure alerting*. Finalmente, *exposure notification* se ha popularizado al ser la terminología utilizada por Google y Apple [2]. Para una discusión, ver [3].



juegan un rol más activo en el procesamiento y generación de alertas.

Una segunda clasificación se basa en la tecnología empleada para detectar los contactos, siendo las alternativas predominantes el GPS y el Bluetooth (BLE). La primera alternativa se basa en comparar las ubicaciones geográficas de los usuarios, mientras que la segunda se basa en el intercambio dispositivo-a-dispositivo de datos vía una señal de Bluetooth.

En cuanto a los dispositivos en los que se pueden implementar dichas aproximaciones, también existe cierta diversidad. Por legibilidad del artículo, y debido a su mayor generalidad y uso, nos centraremos en aplicaciones instaladas en teléfonos inteligentes (apps). Otras alternativas que se han empleado son pulseras (*smart bands*) y dispositivos electrónicos portátiles simples (*wearables*). Estas últimas alternativas tienen una mayor aplicabilidad en monitoreo de contactos en empresas del sector privado, a diferencia de las basadas en apps, las cuales son de más amplia aplicabilidad. Tampoco discutiremos aquí los sistemas basados en el monitoreo de infraestructura existente, como cámaras de circuitos cerrados de televisión (CCTV), recolección de señales de Bluetooth por sensores ubicados en centros comerciales o la vía pública, o análisis de patrones de uso de tarjetas de crédito, credenciales de salud o transporte [5], en las cuales mediante algoritmos de inteligencia artificial se puede identificar a las personas que han estado en contacto.

Aproximación centralizada basada en GPS

Los usuarios, a través de una app instalada en su teléfono inteligente, generan registros de ubicaciones recorridas durante un período de tiempo, las que transmiten a un repositorio centralizado. Cuando un usuario es diagnosticado como COVID-positivo, esos registros se comparan con los usuarios que han estado en la misma área durante el mismo período de tiempo en función de estos datos de ubicación, notificando las alertas de exposición a aquellos usuarios que cumplen dicha condición. Esta aproximación tiene la ventaja de ayudar a identificar posibles áreas de transmisión del virus por lo que, si esta solución es utilizada por un gobierno, los funcionarios de salud pública cuentan con información adicional para el rastreo manual de contactos. En contra, su potencial impacto en la privacidad de las personas ha sido ampliamente cuestionado pues la autoridad puede obtener no sólo información de contacto de los usuarios, sino potencialmente un registro geolocalizado de los lugares donde el usuario ha estado.

Aproximaciones basadas en Bluetooth

En este caso, cuando dos teléfonos inteligentes con la app instalada se encuentran próximos (lo cual se detecta a través de la intensidad de la señal de Bluetooth) intercambian un identificador de proximidad. Cada teléfono inteligente se encarga de almacenar los identificadores de todos los otros usuarios que estuvieron cerca. Dependiendo de cómo se generan los identificadores y cómo se comparten con la autoridad, este enfoque da pie a dos aproximaciones, una centralizada y una descentralizada (ver Figura 1).

En la primera, los identificadores típicamente creados por la autoridad sanitaria en forma centralizada, son comunicados a cada teléfono inteligente, el cual los va emitiendo en los encuentros. Cada teléfono almacena los identificadores de sus contactos y, ante una notificación de infección, comunica a la autoridad la lista de todos los identificadores *que ha escuchado*. De esa manera, la autoridad puede luego identificar a todos los teléfonos cuyos dueños han sido expuestos al virus.

En la segunda variante, cada teléfono inteligente escoge en forma interna una lista de identificadores aleatorios y variables en el tiempo, los cuales intercambiará con otros teléfonos, en forma indepen-

diente de la autoridad central. Luego, en caso de ser notificado como COVID-positivo, el teléfono comparte públicamente (en un servidor público) la lista de todos los identificadores *que ha enviado hacia otros*. Al compartirla, otros usuarios de la app pueden consultar por estos identificadores en forma pública y determinar si han sido expuestos: basta verificar *si han recibido dichos identificadores* desde otros teléfonos. Este análisis se realiza en cada teléfono inteligente, en forma distribuida, generando una alerta local al usuario en caso de haber sido expuesto bajo este criterio. Si bien esta aproximación no puede generar conocimiento acerca de zonas de potencial contagio, es mucho más respetuosa con la privacidad de las personas, lo que tiene un efecto positivo en su adopción.

A nivel internacional se pueden encontrar ejemplos de las aproximaciones anteriores. Sin embargo, la evolución temporal de las mismas parece marcar una tendencia hacia soluciones descentralizadas. En los primeros meses de la pandemia, varios gobiernos orientales como China, Corea del Sur y Singapur, implementaron soluciones centralizadas, varias de ellas basadas fuertemente en GPS. En Europa, en un primer momento países como Francia y Reino Unido también optaron por una aproximación centralizada usando Bluetooth. Sin embargo, éstas últimas recientemente han migrado hacia soluciones descentralizadas debido a dificultades técnicas de sus apps y a la baja adopción por parte de los usuarios. Otros países como Alemania, Austria e Italia apostaron directamente por soluciones descentralizadas, siendo el caso alemán el más exitoso en cuanto a adopción por parte de la población. Una primera revisión de las decisiones adoptadas por diversos países se puede encontrar en [6]. Un acuerdo entre Apple y Google permitió que ambas empresas liberasen un API para el desarrollo de la aproximación descentralizada en sus dispositivos el 20 de mayo de 2020 [2]. Éste se considera un hito importante para el éxito y mayor adopción de la

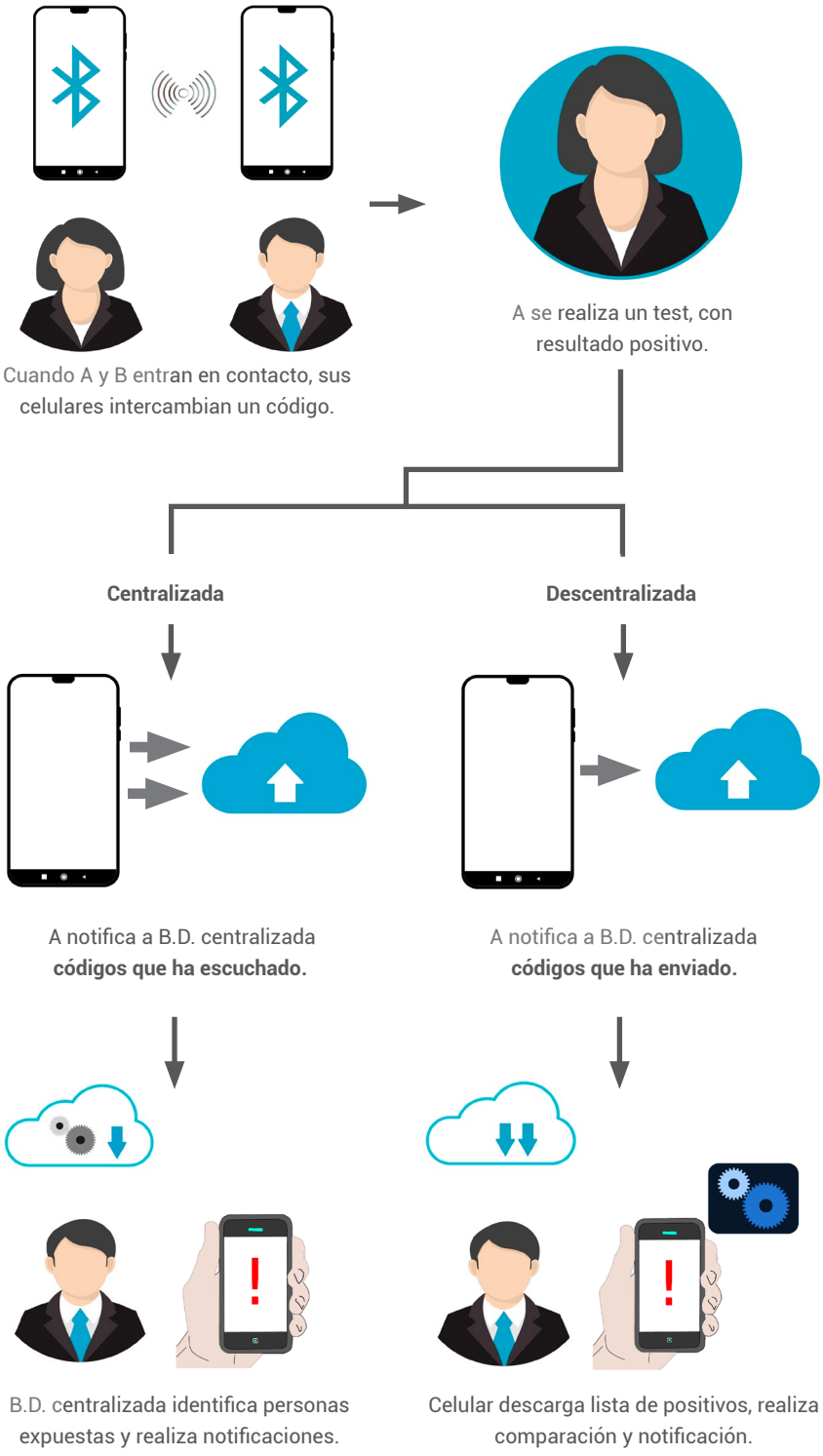


Figura 1. Funcionamiento de aplicaciones basadas en Bluetooth.

Fuente: Adaptada de https://www.bbc.com/news/uk-northern-ireland-53253628.

Si bien [una] aproximación [descentralizada, basada en Bluetooth] no puede generar conocimiento acerca de zonas de potencial contagio, es mucho más respetuosa con la privacidad de las personas.

aproximación descentralizada. En el continente americano, varios países como Uruguay, Brasil y Canadá han apostado por esta aproximación. En Estados Unidos, la decisión se está tomando a nivel estatal, siendo ya varios los estados y universidades que han apostado por esta alternativa.

En el resto del artículo analizamos algunas de las dimensiones principales de estas aplicaciones, comenzando por una que consideramos fundamental: la privacidad.

Privacidad

En principio, todas las aplicaciones basadas en apps buscan automatizar la trazabilidad de contactos, identificando a individuos que han estado en contacto estrecho con otros individuos infectados a fin de aislarlos y reducir subsecuentes contagios. Sin embargo, el proceso para lograrlo difiere en las distintas aproximaciones y, en particular, las características y escala de la información recopilada por la autoridad puede ser fundamentalmente distinta. Por ejemplo, las aplicaciones basadas en GPS no sólo pueden revelar un encuentro cercano entre dos individuos, sino la ubicación geográfica de este evento. Más aún, dependiendo de la aplicación, patrones de movimiento geográfico detallado de usuarios identificados (patrones de viajes, lugares más visitados) pudieran ser accesibles a la autoridad central, dando espacio para potenciales violaciones de la privacidad de los usuarios e incluso vulneraciones de derechos civiles. En países democráticos, esto ha motivado fuertes cuestionamientos a algunas de dichas aproximaciones, notablemente las basadas en GPS y en infraestructura de monitoreo (ej. cámaras en lugares públicos).

Intuitivamente, un sistema basado en apps para identificar usuarios expuestos y detener la cadena de contagios capaz de respetar la privacidad de los usuarios potencialmente expuestos no parece fácil de lograr. Sin embargo, esto es precisamente lo que hace el enfoque descentralizado usando Bluetooth, originalmente propuesto por DP3T, un consorcio académico internacional [7], y luego adoptado por Google y Apple. En este enfoque, el teléfono de un usuario infectado voluntariamente colabora revelando la lista de identificadores por sí emitidos en los encuentros con otros teléfonos, de manera que cada uno de los otros teléfonos inteligentes, al recibir esta lista puede evaluar local y *privadamente* su nivel de riesgo (esto es, si los ha visto, cuántos de ellos, etc.). El usuario expuesto es quién debe tomar la decisión de actuar, no la autoridad. El sistema privilegia entonces el consentimiento del usuario expuesto respecto a la decisión a tomar (aislarse, hacerse un test, o compartir su información con la autoridad) por sobre la habilidad de la autoridad de determinar proactivamente la red de contactos de un usuario infectado. Esta decisión ha sido justificada en base a que tal red de contactos conlleva información privada no del usuario infectado, sino de los potencialmente expuestos, afectando la privacidad de *éstos últimos* [8]. Google y Apple, al apoyar este enfoque incluso agregan condiciones que cualquier aplicación de la autoridad sanitaria debe cumplir, como ser de carácter voluntario (*opt-in*) con posibilidad de revocar consentimiento en cualquier momento, y no recopilar información identificable de cualquier usuario sin su consentimiento (nombre, identificador del teléfono), entre otras [2].

La aproximación centralizada usando Bluetooth precisamente intenta darle a la autoridad sanitaria la habilidad de armar la red de contactos sin depender de la voluntad del usuario potencialmente expuesto. Países como Francia o Reino Unido inicialmente buscaron construir aplicaciones con este enfoque. Sin embargo, en poco tiempo migraron al enfoque distribuido, no debido al potencial de abuso por parte de la autoridad, o al riesgo de filtración de datos sensibles de los ciudadanos, sino probablemente debido a las dificultades derivadas de no contar con funcionalidades técnicas cruciales en los teléfonos, las cuales Google y Apple sólo otorgan a aplicaciones compatibles con su enfoque. Por ejemplo, aplicaciones no compatibles con la API de Google y Apple tienen alto consumo de batería, lo cual limita seriamente su uso prolongado.

El factor privacidad de estas apps no sólo es teórico. La experiencia internacional en países donde el uso de estas apps es voluntario parece indicar que apps percibidas (correcta o incorrectamente) como no respetuosas de la privacidad de sus usuarios logran bajas tasas de adherencia por parte de la población. Este punto se discute en más detalle después.

Consideraciones éticas

Si bien el concepto de pandemia implica inevitablemente un sentido de urgencia, las aproximaciones desarrolladas para el control de la misma deberían estar regidas por un marco ético [9]. En este sentido, la Organización Mundial de la Salud publicó un informe [10] con principios éticos, así como consideraciones y requerimientos técnicos que están de acuerdo con dichos principios. Se trata de un conjunto de 17 principios, entre los que nos permitimos destacar los más

En las aplicaciones basadas en GPS [...] los patrones de movimiento [...] pudieran ser accesibles a la autoridad central, dando espacio [...] a vulneraciones de derechos civiles.

relacionados con el contenido de este artículo. *Evaluación*, las tecnologías son novedosas y deben ser evaluadas rigurosamente y por agencias independientes para determinar su efectividad. *Uso voluntario*, los gobiernos no deberían imponer el uso de las tecnologías, por lo que las campañas para lograr una amplia adopción y adherencia son fundamentales. *Preservación de la privacidad*, tal como ya se ha mencionado en este artículo, la OMS indica que hay un consenso en que las aproximaciones descentralizadas mejoran la privacidad. Sin embargo, alientan el resguardo de la misma sea cual sea la aproximación empleada. *Sociedad civil y compromiso público*, enfatiza el rol de la sociedad civil para que gobiernos y empresas se responsabilicen del funcionamiento de las tecnologías. Estos principios ponen de manifiesto la necesidad de una responsabilidad colectiva, como sociedad, en armonía con el respeto de los derechos individuales, como es el caso de la privacidad.

En Estados Unidos, la National Security Commission on Artificial Intelligence elaboró un *white paper* que da recomendaciones para poner las libertades civiles en el centro y para tratar de evitar que la tecnología produzca más sesgos e injusticias [11].

En Chile, el Centro Nacional en Sistemas de Información en Salud (CENS) elaboró una *Guía de Buenas Prácticas y Recomendaciones para el uso de Telemedicina durante la Epidemia de COVID-19 en Chile* [12]. Si bien el foco de dicha guía no es la trazabilidad, sí recoge en su sección 6 una serie de recomendaciones éticas y legales a tener en cuenta en el contexto de la pandemia. Por otro lado, la telemedicina puede ser un fuerte aliado en la mejora de estrategias de TTA.

Adopción, adherencia y efectividad

Como toda solución diseñada para ser empleada por la población en general, la adopción y adherencia a la misma son factores determinantes en su efectividad. En el contexto de las apps descritas en este artículo, la adopción se refiere al número de personas que las instalan, mientras que la adherencia se refiere al número de personas que las utilizan con regularidad. La experiencia internacional, en particular en occidente, ha mostrado una mayor adherencia en la estrategia descentralizada, lo cual probablemente está asociado a su mayor respeto por la privacidad. La estrategia centralizada, en la cual se almacena información relativa al movimiento de las personas, está muy asociada a problemas de confianza sobre todo en cuanto al no uso de la información para el monitoreo de las personas, incluidas las COVID-positivo, siendo éste uno de los principios éticos señalados por la OMS y otras organizaciones de derechos civiles [10, 8].

Si bien la privacidad se puede considerar que es un factor importante en la adopción y adherencia, existen otros asociados a barreras tecnológicas como versión mínima de sistema operativo, consumo de batería, o usabilidad de la aplicación, en particular entre sectores de la población de mayor edad. Todos estos factores limitan el alcance que puede lograr la adherencia de estas soluciones. Por ese motivo es importante estudiar la efectividad que puede lograr la solución en función de la adherencia de la misma.

Si bien la tecnología es todavía joven y no existen estudios definitivos sobre su efectividad, sí hay algunos estudios y simulaciones preliminares acerca de la misma [13, 14]. Uno de los primeros estudios en abordar el tema [13], afirmaba que bajo ciertas condiciones, la pandemia se podía contener si un 56% de la población adoptaba esta tecnología. Esta afirmación fue, en palabras de los propios autores, malinterpretada como que la tecnología sólo sería un aporte en la contención de la pandemia si se alcanzaba un 60% de adherencia [14]. Sin embargo, el modelo de los autores muestra que la solución es un aporte en la reducción de contactos potencialmente contagiosos incluso a niveles tan bajos de adherencia como 20%.[5]

Otra arista importante a considerar es la penetración potencial en diferentes sectores o rangos etarios de la población y el efecto que eso podría tener. Al 4 de septiembre de 2020, la tasa de incidencia acumulada es más alta en el grupo de 30 a 39 años (3.379 por cada 100.000 habitantes), seguida por los grupos de 20 a 29 (2.974 por cada 100.000 habitantes), 50 a 59 años (2.930 por cada 100.000 habitantes), y 40 a 49 años (2.881 por cada 100.000 habitantes). Los dos primeros son grupos ciertamente tecnológicos, los que no tendrían problemas de adopción de tecnologías. Por tanto, si bien se puede esperar una adherencia desigual entre grupos etarios, la tecnología podría ser un aporte en los grupos que presentan mayor prevalencia.

5 | Reportes preliminares recientes sobre la aplicación Suiza (SwissCovid) indican efectividad comparable al asociado a trazabilidad de contactos manual asumiendo disponibilidad de testeo eficiente e infraestructura de trazabilidad manual [15].

Finalmente, pensando en la efectividad, se debe señalar que una de las limitantes de esta tecnología es que identifica muchos falsos positivos, por lo que su uso es más eficiente cuando el número de personas infectadas diarias no es muy alto. Por ese motivo, están siendo más empleadas como apoyo a la estrategia de salida de la pandemia, la cual tiene que ser acompañada con una buena capacidad de testeo de casos expuestos.

Código abierto

Uno de los mensajes importantes de las secciones anteriores es que, dado que el uso de la tecnología debe ser voluntario y la efectividad mejora con el nivel de adopción, las soluciones deben ir acompañadas de medidas que promuevan la misma, principalmente en base a la confianza en la tecnología.[6] En ese sentido, muchas de las soluciones están optando por publicar las apps como código abierto.

Hace unos años, esto podría parecer una decisión sorprendente, sin embargo no es más que el reflejo de la evolución que ha tenido el uso del código abierto. El informe OSSRA que realiza la empresa Synopsys, y en el que se analizan riesgos y la seguridad de las soluciones de código abierto empleadas por empresas de diferentes sectores, muestra varios indicadores importantes para sustentar esta afirmación. Por ejemplo, en el informe 2020 se refleja que el 70% del código auditado es código abierto (con respecto al 36% del primer informe) y que el 99% de las bases auditadas contenían algún componente de código abierto.

En esa línea, el publicar las apps como código abierto hereda los beneficios de dicho paradigma. Mejora la transparencia y confianza, al tener una amplia comunidad que puede auditar el uso exacto que se hace de los datos. También puede mejorar la seguridad de las soluciones desarrolladas dado que las vulnerabilidades se suelen exponer, y por tanto corregir, más rápido. Por último, también se puede mencionar que permite la colaboración y compartición de costes entre diferentes países; así como la interoperabilidad.

Más allá de la API de Google-Apple

Actualmente, las soluciones basadas en la API de Google y Apple se encuentran más avanzadas y pueden lograr un nivel de adopción más alto en el corto plazo. Sin embargo, partiendo de la misma base y posiblemente utilizando técnicas criptográficas más sofisticadas, se pueden desarrollar soluciones que, pre-

6 | Las mejores prácticas han sido recogidas en diversas iniciativas, notablemente [16].

[Con el fin de promover la confianza] muchas de las soluciones están optando por publicar las apps como código abierto.

servando la privacidad de los usuarios puedan resolver algunos de los problemas abiertos, como por ejemplo, mejorar la seguridad ante ciertos ataques [17], o proveer información epidemiológica más detallada, posiblemente otorgando beneficios en el largo plazo (ver por ej. [18, 19, 20, 21]). Además del valor académico de dichas soluciones, no se debe ignorar el argumento de estar mejor preparado para nuevas pandemias en el mundo globalizado e interconectado en el que vivimos.

Una solución atractiva en esta línea de dar un paso más es SafetyScore [21]. La principal característica diferenciadora de esta solución es que no se queda únicamente en los contactos directos, sino que realiza propagación de información a contactos indirectos (segundo grado y mayor), lo que le permite realizar un cálculo de la exposición al riesgo más preciso. Si bien ésta es una característica atractiva, también supone consideraciones de privacidad y robustez más avanzadas que deben ser abordadas. Para ello, la arquitectura propuesta sigue un esquema distribuido similar a *blockchain* y utiliza algoritmos criptográficos para revelar la identidad de los usuarios.[7] Además, también permite calcular para cada persona un indicador de riesgo en función de sus contactos, lugares visitados (geo-regiones) y sus diagnósticos médicos, el cual puede ser utilizado para determinar las medidas de autocuidado que debe tomar cada persona. En las simulaciones realizadas por los propios autores, SafetyScore puede ser hasta tres veces más efectivo para prevenir contagios que soluciones basadas en la API de Google y Apple.

El CMM de la Universidad de Chile ha realizado varias simulaciones[8] para evaluar la efectividad que tendría una plataforma similar a SafetyScore en el Gran Santiago. Los resultados obtenidos muestran que, combinando la tecnología con una política de distanciamiento social, se puede lograr una reducción significativa en el número de infectados, poniendo en aislamiento simultáneo únicamente a una pequeña parte de la población (aquellas personas cuyo indicador de riesgo supera un determinado umbral). También se destaca que la capacidad de testeo y entrega oportuna de resultados es importante para la eficacia de la aplicación, cuyo impacto se ve reducido por retrasos en la enrega de los resultados de los tests.

Lecciones preliminares

En este artículo se revisan algunas de las principales aplicaciones de trazabilidad de exposición y cómo pueden ayudar en la gestión de una pandemia como la causada por el SARS-CoV-2. Si bien todavía es pronto para juzgar su aporte [22], sí existen resultados preliminares prometedores. Además, es importante rescatar algunas otras lecciones aprendidas. En primer lugar, es interesante destacar cómo han ido evolucionando, desde una etapa inicial basada en un esquema centralizado que recopilaba información georeferenciada muy valiosa pero poco respetuosa de la privacidad, a la situación actual donde se está apostando más fuertemente por soluciones descentralizadas que llegan a un compromiso de capturar menos información a cambio de un mayor respeto a la privacidad de las personas. Esto genera mayor confianza, lo que se traduce en una mejor adopción por parte de la población. Además, los grupos de mayor prevalencia actualmente en Chile son los segmentos de 30 a 39 años y 20 a 29, grupos claramente tecnológicos donde se puede esperar una alta adherencia. Las estrategias centralizadas pueden tener una oportunidad de éxito mayor en el sector privado, en particular en ciertos rubros donde los empleados están más acostumbrados a diferentes medidas de monitoreo durante la jornada laboral. También se rescatan diferencias entre las estrategias de implantación en los diferentes países, donde algunos realizaron pilotos en regiones bien acotadas (por ejemplo islas), mientras que otros lanzaron la aplicación directamente en todo el país. Esto pone de manifiesto la necesidad de probar los sistemas en crisis de verdad para poder ganar experiencias reales.

Por último, nos permitimos cerrar el artículo con dos invitaciones, una a la comunidad académica para involucrarse en el proceso de implantación de este tipo de soluciones, revisando/colaborando con los proyectos existentes (muchos de ellos de código abierto), explicando el funcionamiento de las mismas para generar mayor confianza, o realizando simulaciones y estudios que permitan evaluar su aporte real. Una segunda invitación a la sociedad en su conjunto para tener la mente abierta a la tecnología, incluso si es nueva y su evaluación completa será muy *a posteriori*. Nos encontramos en el momento de probar paradigmas y generar comunidades donde el uso de las aplicaciones es para el bien común, no sólo para fines individualistas, como muchas aplicaciones actuales. ■

7 | El diseño de SafetyScore, si bien es público, no ha sido *peer reviewed* todavía.
8 | Presentación disponible en: https://github.com/Instituto-Milenio-de-Datos/modelamiento-covid.

REFERENCIAS

[1] Subsecretaría de Salud Pública, División de Planificación Sanitaria, Departamento de Epidemiología. Protocolo de coordinación para acciones de vigilancia epidemiológica durante la pandemia COVID-19 en Chile: Estrategia nacional de testeo, trazabilidad y aislamiento. Reporte técnico. 2020. Disponible en: https://www.minsal.cl/wp-content/uploads/2020/07/Estrategia-Testeo-Trazabilidad-y-Aislamiento.pdf.

[2] Apple Newsroom. Apple and Google partner on COVID-19 contact tracing technology. Mayo 2020. Disponible en: https://www.apple.com/newsroom/2020/04/apple-and-google-partner-on-covid-19-contact-tracing-technology.

[3] Harper Reed. Digital Contact Tracing and Alerting vs Exposure Alerting. Abril 2020. Disponible en: https://harper.blog/2020/04/22/digital-contact-tracing-and-alerting-vs-exposure-alerting/.

[4] Mark Zastrow. Coronavirus contact-tracing apps: can they slow the spread of COVID-19? Nature. Mayo 2020.

[5] New York Times. New Covid-19 Outbreaks Test South Korea's Strategy. Septiembre 2020. Disponible en: https://www.nytimes-com/2020/09/02/world/asia/south-korea-covid-19.html.

[6] Patrick Howell O'Neill, Tate Ryan-Mosley, and Bobbie Johnson. A flood of coronavirus apps are tracking us. Now it's time to keep track of them. *MIT Technology Review.* Mayo 2020.

[7] DP3T Consortium. DP3T - Decentralized Privacy-Preserving Proximity Tracing. Mayo 2020. Disponible en: https://github.com/DP-3T/documents.

[8] Daniel Kahn Gillmor. ACLU Principles for Technology-Assisted Contact-Tracing. Abril 2020. Disponible en: https://www.aclu.org/sites/default/files/field_document/aclu_white_paper_-_contact_ tracing_principles.pdf.

[9] Jessica Morley, Josh Cowls, Mariarosaria Taddeo, y Luciano Floridi. Ethical guidelines for COVID-19 tracing apps. *Nature*. Mayo 2020.

[10] Health Ethics Governance, WHO Global. Ethical considerations to guide the use of digital proximity tracking technologies for COVID-19 contact tracing. Reporte técnico. 2020. Disponible en: https://www.who.int/publications/i/item/WHO-2019-nCoV-Ethics_Contact_tracing_apps-2020.1.

[11] Eric Horvitz, and Mignon Clyburn, and José-Marie Griffiths, and Jason Matheny. Privacy and Ethics Recommendations for Computing Applications Developed to Mitigate COVID 19. Reporte técnico. 2020. Disponible en: https://epic.org/foia/epic-v-ai-commission/ NSCAI-contact-tracing-white-paper.pdf.

[12] Equipo CENS. Guía de Buenas Prácticas y Recomendaciones para el uso de Telemedicina durante la Epidemia de COVID-19 en Chile. Reporte técnico. 2020. Disponible en: https://cens.cl/ guia-buenas-practicas-telemedicina/.

[13] Robert Hinch, Will Probert, Anel Nurtay, Michelle Kendall, Chris Wymant, Matthew Hall, Katrina Lythgoe, Ana Bulas Cruz, Lele Zhao, Andrea Stewart, Michael Parker, Daniel Montero, James Warren, Nicole K Mather, Anthony Finkelstein, Lucie Abeler-Dörner, David Bonsall, y Christophe Fraser. Effective Configurations of a Digital Contact Tracing App: A report to NHSX. Reporte técnico. 2020. Disponible en: https://github.com/BDI-pathogens/covid-19_instant_tracing.

[14] Patrick Howell O'Neill. No, coronavirus apps don't need 60% adoption to be effective. *MIT Technology Review*. Junio 2020.

[15] Marcel Salathé, Christian L. Althaus, Nanina Anderegg, Daniele Antonioli, Tala Ballouz, Edouard Bugnion, Srdjan Čapkun, Dennis Jackson, Sang-Il Kim, James R. Larus, Nicola Low, Wouter Lueks, Dominik Menges, Cédric Moullet, Mathias Payer, Julien Riou, Theresa Stadler, Carmela Troncoso, Effy Vayena, y Viktor von Wyl. Early Evidence of Effectiveness of Digital Contact Tracing for SARS-CoV-2 in Switzerland. Septiembre 2020. Disponible en: https://github.com/digitalepidemiologylab/swisscovid_efficacy/blob/master/Swiss-Covid_efficacy_MS.pdf.

[16] Andrew Trask, Cari Spivack, Clara Fischer, Dana Lewis, Harper Reed, Martin Hacker, Scott Leibrand, Sebastian Presiner, y Tina White. Data Rights for Exposure Notification. Abril 2020. Disponible en: http://exposurenotification.org/.

[17] Rosario Gennaro, Adam Krellenstein, y James Krellenstein. Exposure notification system may allow for large-scale voter suppression. Reporte técnico. Agosto 2020. Disponible en: https://preview.tinyurl.com/yxmx4c9p.

[18] Justin Chan, Shyam Gollakota, Eric Horvitz, Joseph Jaeger, Sham Kakade, Tadayoshi Kohno, John Langford, Jonathan Larson, Sudheesh Singanamalla, Jacob Sunshine, y otros. Pact: Privacy sensitive protocols and mechanisms for mobile contact tracing. 2020. Disponible en: https://arxiv.org/abs/2004.03544.

[19] Gennaro Avitabile, Vincenzo Botta, Vincenzo Iovino, y Ivan Visconti. Towards defeating mass surveillance and SARS-CoV-2: The Pronto-C2 fully decentralized automatic contact tracing system. Reporte técnico. 2020. Disponible en: https://eprint.iacr.org/2020/493.

[20] Wasilij Beskorovajnov, Felix Dörre, Gunnar Hartung, Alexander Koch, Jörn Müller-Quade, y Thorsten Strufe. Contra corona: Contact tracing against the coronavirus by bridging the centralized–decentralized divide for stronger privacy. Reporte técnico. 2020. Disponible en: https://eprint.iacr.org/2020/505.

[21] Tav, Luke Robinson, Tom Salfield, Alice Fung, y Oliver Zahn. SafetyScore: Containing epidemics through privacy-preserving network-level tracing. Reporte técnico. Mayo 2020. Disponible en: https://safetyscore.app/whitepaper.

[22] Charlotte Jee. Is a successful contact tracing app possible? These countries think so. *MIT Technology Review*. Agosto 2020.