Boletín N°. 10

COVID-19: Uso de apps con rastreo de contactos y respeto a la privacidad

Antecedentes

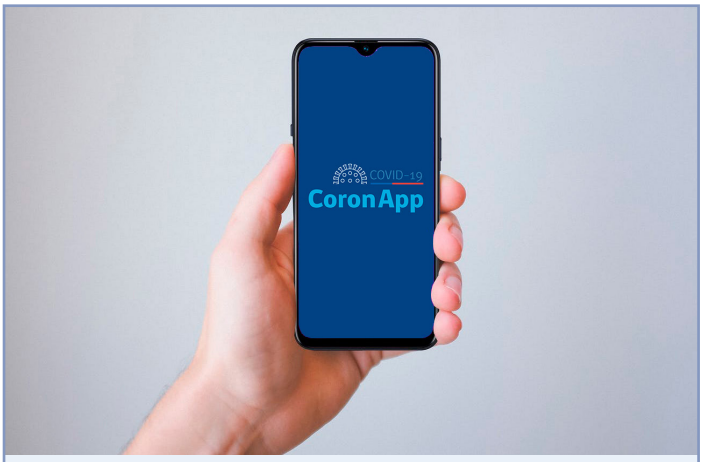
En la crisis sanitaria actual, diversos países han desarrollado aplicaciones ("apps") para teléfonos móviles que permiten entregar información sobre la pandemia y rastrear a personas con examen COVID-19 positivo y sus contactos. Su objetivo, además de hacer el seguimiento de enfermos, es alertar a quienes hayan estado físicamente cerca de un paciente COVID-19, tomen las medidas sanitarias pertinentes y así ayudar a contener la propagación del virus[1].

No obstante la implementación de este tipo de apps en una veintena de países a finales de mayo de 2020, aún no existe un consenso científico acerca de su utilidad para el rastreo en el marco de la pandemia. De hecho, también han sido objeto de controversias, tanto por el almacenamiento de los datos como por la precisión real de la ubicación de posibles infectados[2].

Al desarrollar este tipo de aplicaciones, la determinación de tales cercanías se realiza a través de distintas tecnologías disponibles y las diversas combinaciones de ellas, a través de las cuales se obtienen resultados muy diferentes desde el punto de vista del respeto del derecho de privacidad y del nivel de legitimidad e inclusión social que logran estas tecnologías[3][4].

En ese sentido, hay dos decisiones técnicas esenciales al momento de desarrollar una app con rastreo de contactos: i) la manera de almacenar la información sanitaria que se procesa y ii) la tecnología base que se utiliza.

La Unión Europea (UE) se inclinó por el uso de Bluetooth ya que, a su juicio, resulta más fácil anonimizar los datos y resguardar



CoronApp, la aplicación chilena

El 16 de abril[45] se anunció a la ciudadanía la nueva aplicación CoronApp (Chile), con la que se busca informar, acompañar y orientar a la población ante el Coranavirus. La cual el gobierno puso a disposición tanto para teléfonos iPhone como Android.

La aplicación, desarrollada por la División de Gobierno Digital del Ministerio Secretaría General de la Presidencia (SEGPRES), declara los siguientes objetivos[46]:

- **Autoevaluación de síntomas para clasificación de riesgo.**
- **Monitoreo de síntomas de hasta 8 personas.**
- **Notificaciones del Ministerio de Salud.**
- **Informes y/o denuncias de conductas o eventos de alto riesgo.**
- **Indicar lugares de cuarentena.**

La información oficial, disponible en los Términos y Condiciones[47] y las Políticas de Privacidad[48] de la aplicación, no es completa, a pesar de lo cual, se puede deducir que:

1. **El desarrollador de la app es una entidad pública, aunque no se establece quién administra los datos. Al respecto, el Consejo para la Transparencia solicitó identificar al órgano responsable de**

la privacidad de las personas, además de considerar que es más precisa que el GPS para detectar "contactos estrechos"[5].

Aunque estas apps han sido efectivas en países asiáticos como Singapur, Vietnam, Corea del Sur o China, siempre han sido implementadas junto a otras medidas sanitarias, e incluso a otros esfuerzos de rastreo, por lo que no resulta posible cuantificar su impacto de manera aislada[67].

Este boletín explica y analiza las funciones de rastreo y de almacenamiento de información personal de estas aplicaciones. Atendido el rápido desarrollo de la contingencia, las materias tratadas en el presente boletín son esencialmente dinámicas y se encuentran en constante cambio.

Qué es y cómo funciona el rastreo de contactos

La lógica del rastreo de contactos es la misma que ha sido utilizada tradicionalmente por los servicios de salud[8]. Se trata de cualquier registro escrito que identifica a un paciente y sigue su historia clínica, la que es monitoreada por trabajadores de la salud, quienes a su vez, pueden entregarle recomendaciones médicas personal o telefónicamente. Lo nuevo de estas apps es la automatización de ese proceso, usando los teléfonos móviles de las personas para que la autoridad sanitaria pueda orientar el comportamiento de quienes estén, sin saberlo, en riesgo de contagio[9].

Así, el rastreo de contactos no descansa en la memoria del paciente (y si se acuerda a quienes tuvo cerca en las últimas 48 horas), ni tampoco de que el paciente pueda identificarlas (con quienes compartió la locomoción pública, por ejemplo)[10]. Además, la información que pueda entregar un paciente que acaba de enterarse que es COVID-19 positivo, con la carga emocional y malestar físico que ello implica, no necesariamente es rigurosa.

Cuando una persona es notificada por las autoridades de salud de un examen COVID-19 positivo, de manera voluntaria puede ingresar esta información a la app, la que rastrea a quienes tuvieron contacto con ella en las últimas 48 horas[11]. Técnicamente, el "contacto" se genera cuando el dispositivo móvil del paciente COVID-19 positivo se acerca al dispositivo de una persona sana, en un período que va desde las 48 horas antes del inicio de los síntomas hasta 14 días después de iniciados éstos[12]. En tanto, un "contacto estrecho" ocurre cuando los dispositivos de las mencionadas personas están cerca durante al menos 15 minutos y a menos de 1,5 metros de distancia[13]. La app discrimina entre "contactos estrechos" y "de bajo riesgo" y notifica a los dispositivos para que sus usuarios tomen los resguardos pertinentes, los que pueden ser, por ejemplo, sólo cuarentena voluntaria si no tienen síntomas, o realizarse el test en caso de que los tengan[14].

En teoría, a las apps se les delega la función de detectar situaciones de riesgo sanitario, analizando la cercanía entre teléfonos móviles. Delegar una función sanitaria, -originalmente realizada por humanos- a una máquina (app), gatilla acciones complementarias como, por ejemplo, verificar el funcionamiento de la app respecto del derecho de privacidad de las personas y cuán inclusiva y legítima socialmente es ésta[15] [16]. En ese sentido, hay dos decisiones técnicas esenciales al momento de desarrollar una app con rastreo de contactos: i) la manera de almacenar la información sanitaria que se procesa y ii) la tecnología base que se utiliza:

los datos y otras recomendaciones para el cumplimiento de la Ley N°19.628 sobre protección de la vida privada[49].

2. **Sobre la tecnología base de rastreo no hay información concluyente. Se podría deducir que CoronApp utilizaría un híbrido Bluetooth-GPS.**

3. **Sobre el sistema de almacenamiento, su Política de Privacidad señala que "la información registrada en la aplicación será almacenada y replicada en una nube privada bajo la completa administración del MINSAL en Amazon Web Services (AWS)". Por tanto, podría tratarse de un sistema de almacenamiento de datos centralizado o, considerando que también utiliza Bluetooth, de almacenamiento "híbrido-centralizado". Estas son sólo hipótesis.**

4. **Respecto de la eliminación de datos, CoronApp declara que podrá tener los datos hasta por 15 años, en determinados casos. El análisis internacional comparado (figura 3) muestra que 6 de las 13 apps estudiadas eliminan los datos en 30 días o menos, en tanto la app española los guarda por 2 años y la israelí por 7.**

La aplicación está disponible en las dos principales tiendas de descarga de aplicaciones para celulares, App Store (Apple) y Play Store (Android). A la fecha de este informe, se habían efectuado poco más de 50.000 descargas de la versión Android, mientras que App Store no publica la cantidad de descargas.

i) **El sistema de almacenamiento de los datos.** La mayoría de las aplicaciones con rastreo de contactos utilizan enfoques que minimizan la recopilación y el almacenamiento de datos, y los gestionan a través de sistemas "descentralizados" o "centralizados" de almacenamiento de la información de sus usuarios[17]. En los sistemas centralizados, una vez anonimizados los datos de las personas, éstos son almacenados en un servidor central gestionado por la autoridad a cargo de la aplicación. En los modelos descentralizados, en cambio, la información se almacena localmente, es decir, en el teléfono móvil de cada persona, compartiéndose con la autoridad sanitaria la menor cantidad de información privada posible[18].

   La "ventaja" del modelo centralizado es que recopila información útil para que las autoridades monitoreen la evolución del COVID-19, en tanto, su "desventaja" es que los datos almacenados centralizadamente pueden ser utilizados para propósitos diferentes a los sanitarios, en cuyo caso se vulneraría el derecho a privacidad de las personas[19]. Por otra parte, la "ventaja" de un sistema descentralizado es que no genera esa instancia central de almacenamiento de la información, por lo que, en principio, es más amigable con el respeto de la privacidad, aunque, por otro lado, su "desventaja" es que no permite un monitoreo global de la pandemia[20].

ii) **Tecnología de base.** Como ya se mencionó, las tecnologías de rastreo más comunes son Bluetooth y GPS. Las aplicaciones que usan esta última, identifican los contactos de una persona al rastrear los movimientos del teléfono y buscando otros teléfonos que hayan pasado tiempo en esa misma ubicación. En cambio, las apps basadas en Bluetooth utilizan el "seguimiento de proximidad", en el cual los teléfonos intercambian tokens cifrados con cualquier otro teléfono cercano[21].

Normativa aplicable: derecho internacional de los DDHH, normativa supranacional y nacional

En general, solo bajo circunstancias excepcionales que sean oficialmente proclamadas (como los estados de excepción constitucional), el derecho a la privacidad puede ser suspendido (art. 4 Pacto Internacional de Derechos Civiles y Políticos y art. 27 Convención Americana sobre Derechos Humanos), aunque dicha suspensión queda sujeta al principio de proporcionalidad y de mínima intervención[22]. En consecuencia, conforme a los organismos competentes en DDHH, en el contexto del COVID 19, tal suspensión, conforme al derecho internacional de los derechos humanos, debe ser legal, necesaria y proporcional[23].

En términos del uso de aplicaciones para enfrentar la pandemia, lo anterior podría interpretarse como un llamado a los gobiernos a utilizar todos los medios que tengan a su disposición para evitar la suspensión del derecho a la vida privada durante la crisis, es decir, a utilizar la tecnología disponible que mejor preserve dicho derecho. Respecto de los principios internacionales de DDHH aplicables a las tecnologías de rastreo de contactos durante la pandemia y el uso de los datos personales, la Relatoría de Libertad de Expresión de Naciones Unidas señaló que:

> d) Se ha de proteger estrictamente la confidencialidad de los datos reunidos a fin de impedir que se divulgue información personal a terceros no autorizados por razones de salud pública;
>
> e) Deben quedar expresamente excluidos de la recopilación ciertos datos personales, como el contenido de las comunicaciones de las personas, y se han de aplicar salvaguardias sólidas para evitar que los Gobiernos u otros terceros puedan hacer un uso indebido de esos datos, por ejemplo, para fines que no estén relacionados con la emergencia de salud pública;
>
> f) Cuando los datos personales se anonimicen, el Estado y todo tercero que participe en la recopilación de datos deberán poder demostrar que efectivamente los datos son anónimos[24].

Por otra parte, la UE estableció lineamientos a las normativas nacionales de sus Estados miembros que decidan desarrollar este tipo de aplicaciones. El 8 de abril de 2020, la Comisión Europea adoptó una Recomendación sobre el uso de la tecnología y los datos en el abordaje de la crisis de COVID-19. Esta responde a los llamados para la adopción de un enfoque común de la UE para el uso de aplicaciones móviles que considere tanto la eficacia de la tecnología utilizada como su respeto de la privacidad individual y la seguridad de los datos, evitando, además, la vigilancia y la estigmatización[25]. La Recomendación señaló que cualquier aplicación debería:

- Limitarse estrictamente al procesamiento de datos para combatir el COVID-19;
- Garantizar una revisión periódica sobre la necesidad de tal procesamiento de datos personales; y

- Tomar medidas para garantizar que, una vez que el procesamiento ya no sea estrictamente necesario, éste finalice de manera efectiva y los datos personales se destruyan irreversiblemente.

Estos tres lineamientos generales fueron desarrollados en detalle por la Carta del Comité Europeo de Protección de Datos. Así, las recomendaciones específicas de dichas app incluyeron: evitar la identificación de los usuarios, que sean de uso voluntario, evitar el uso de localización (GPS) ya que violaría el principio europeo de minimización de los datos, y preferir el uso de un sistema de almacenamiento de datos descentralizado, entre otras[26].

Finalmente, resulta interesante en términos normativos a nivel nacional la reforma a la ley australiana de protección de datos personales, ya que se realizó especialmente para regular su app nacional en pandemia, y fue tramitada en un cortísimo plazo (tres días desde la introducción del proyecto de ley hasta su total aprobación por ambas cámaras). La Privacy Amendment (Public Health Contact Information) Act 2020 No. 44, 2020, del 18 de mayo de 2020, modificó la Ley de Privacidad (Privacy Act 1988), al incorporar específicamente la regulación de su aplicación COVIDSafe. Con ello, se elevó a nivel de ley la normativa reglamentaria que originalmente autorizó la recopilación de datos personales en el contexto de la emergencia por COVID-19, e introdujo medidas adicionales para reforzar la protección de la privacidad[27].

Entre las principales modificaciones incorporadas se encuentran la creación de nuevos tipos penales por: uso no autorizado de los datos personales recopilados por COVIDSafe; cargar los datos sin consentimiento; retener o divulgar los datos cargados fuera de Australia, "desencriptar" (unencrypt) los datos cifrados de la app; y obligar a otros a usar la aplicación. Todos ellos acarrean penas de hasta 5 años de prisión y multa. Además, la norma reafirma que los datos recopilados por medio de la aplicación constituyen datos personales, y por tanto, están protegidos por la Ley de Privacidad de 1988.

La reforma define conceptos tales como contact tracing (rastreo de contactos); establece la obligación de borrar los datos recopilados en un plazo de 21 días desde su obtención; define que el tiempo de funcionamiento de COVIDSafe será determinado por el ministro de salud (cuando ya no sea necesaria/efectiva para prevenir o controlar el COVID-19), y prohíbe que los datos sean administrados por agencias de inteligencia o policiales. Por último, establece que el ministro de salud debe entregar, dentro de seis meses desde la promulgación de la norma, un informe sobre el funcionamiento y eficacia de COVIDSafe, así como de su sistema de almacenamiento de datos (National COVIDSafe Data Store).

Sin embargo, información de prensa reciente destaca que, no obstante la reforma señalada, a casi un mes de su lanzamiento, COVIDSafe apenas habría sido utilizada, pasando "de vital a irrelevante"[28]. Ello mostraría lo complejo que resulta, en la práctica, coordinar simultáneamente aspectos normativos y tecnológicos, además del nivel de uso de la app por parte de la población.

Análisis de trece apps en actual funcionamiento

Como se señaló, cada gobierno ha debido enfrentar diversas decisiones al momento de desarrollar su aplicación con rastreo de contactos. Con el objetivo de analizar dichas decisiones a través de casos concretos, se seleccionaron aplicaciones con rastreo de contactos que cumplieran con los siguientes criterios: i) estar actualmente en operación; ii) estar respaldadas por los respectivos gobiernos nacionales; iii) desarrolladas solo utilizadas para fines de control del COVID-19; iv) que sean de uso voluntario (no se consideraron los casos de China, India, Turquía, entre otros); y v) que operen sobre las plataformas móviles Android e iOS. El resultado de esta sistematización arrojó las trece aplicaciones que muestra la Figura 1[29][30].

Figura 1. Nombre de las trece aplicaciones seleccionadas y país donde son usadas.

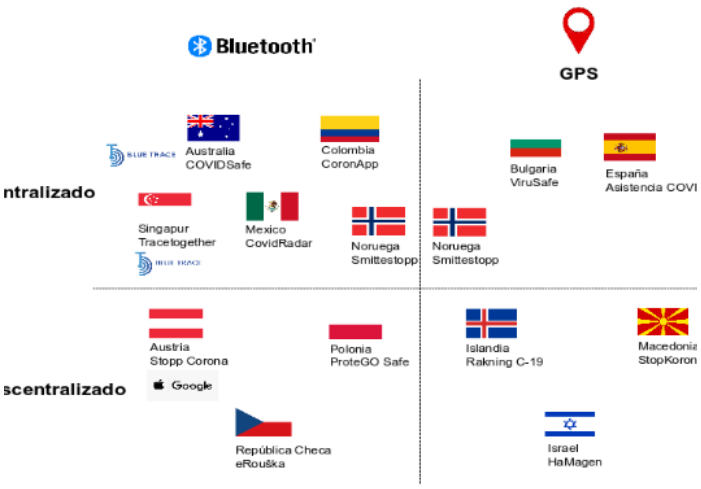
País	Nombre de la aplicación	País	Nombre de la aplicación
Australia	COVIDSafe[31]	Macedonia	StopKorona![32]
Austria	Stopp Corona[33]	México	CovidRadar[34]
Bulgaria	ViruSafe[35]	Noruega	Smittestopp[36]
Colombia	CoronApp[37]	Polonia	ProteGO Safe[38]
España	Asistencia COVID-19[39]	República Checa	eRouška[40]
Islandia	Rakning C-19[41]	Singapur	Tracetogether[42]
Israel	HaMagen[43]		

Fuente: La que se indica en la nota al pie de cada caso.

Considerando la velocidad con la que se desarrollan estas aplicaciones en la actualidad, la sistematización que presenta la figura 1 no es exhaustiva ni definitiva.

Las trece aplicaciones para enfrentar el COVID-19 analizadas se encuentran actualmente en funcionamiento, todas ellas están respaldadas por sus respectivos gobiernos nacionales y son de uso voluntario. Al considerar las dos decisiones técnicas fundamentales ya descritas, esto es, el sistema de almacenamiento de datos (centralizado o descentralizado) y la tecnología de base (Bluetooth o GPS), estas aplicaciones se distribuyeron de la manera que muestra la figura 2.

Figura 2. Cuadrante sobre tecnología base de rastreo de contactos (eje x) y sistema de almacenamiento de datos (eje y), trece aplicaciones analizadas.



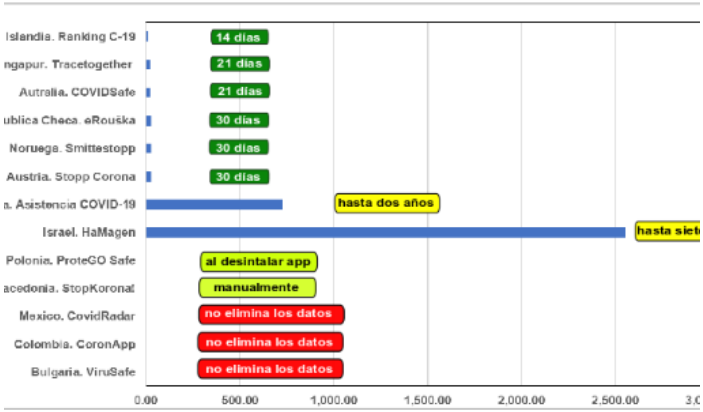
Fuente: Elaboración propia en base a los documentos y fuentes referidos en las notas al pie 8 a 20 del documento principal cuyo link se muestra al principio. En los casos de las aplicaciones COVIDSafe (Australia) y Tracetogether (Singapur), además de Bluetooth utilizan BlueTrace (creada en Singapur). Algo similar ocurre con Stopp Corona (Austria) que, además de Bluetooth, utiliza el protocolo Apple-Google. Por su parte, Smittestopp (Noruega) aparece en dos cuadrantes porque utiliza tanto tecnología Bluetooth como GPS.

Cada una de las subdivisiones de la figura 2 muestra un ensamblaje técnico-normativo específico[44], con funcionalidades particulares que resguardarían, unas más que otras, determinados derechos. El grupo del cuadrante inferior izquierdo -Stopp Corona (Austria), eRouška (República Checa) y ProteGO Safe (Polonia)- por una parte, utiliza Bluetooth (y no GPS) como tecnología base, lo que implica que no procesa datos georreferenciados de sus usuarios, y por otra, utiliza un sistema descentralizado de almacenamiento de datos, de modo que la información personal no es almacenada en una instancia central sino que en los dispositivos de los propios usuarios.

El cuadrante opuesto (superior derecho) -formado por Asistencia COVID-19 (España), ViruSafe (Bulgaria) y Smittestopp (Noruega)- agrupa apps que procesan datos georreferenciados de sus usuarios, al tiempo que almacenan la información utilizando un sistema centralizado. El almacenamiento centralizado de los datos entrega información que el órgano (central) responsable de la aplicación puede utilizar para fines sanitarios. Pero, la mera existencia de dicha instancia centralizada puede constituir un "incentivo" para que la seguridad de la aplicación sea vulnerada por terceros que pretendan acceder a los datos personales de los usuarios, con fines de diversa índole.

Si bien la tecnología de base y el sistema de almacenamiento de datos entregan información fundamental para conocer la estructura general de estas aplicaciones, lo central acá es indagar en el tratamiento de los datos personales de sus usuarios, específicamente: el tipo de datos que recopilan, si éstos son eliminados o no, y, de hacerlo, cuánto tiempo le toma a cada aplicación borrarlos (figura 3).

Figura 3. Eliminación de los datos personales almacenados por la aplicación.



Fuente: Elaboración propia en base a los documentos referidos en las notas al pie 43 a 55.

Las tres apps que utilizan Bluetooth como tecnología base y un almacenamiento descentralizado de los datos, eliminan los datos que procesan. Para ello, Stopp Corona (Austria) y eRouška (República Checa) se toman 30 días, en tanto que ProteGO Safe (Polonia) los elimina cuando el usuario desinstala la aplicación.

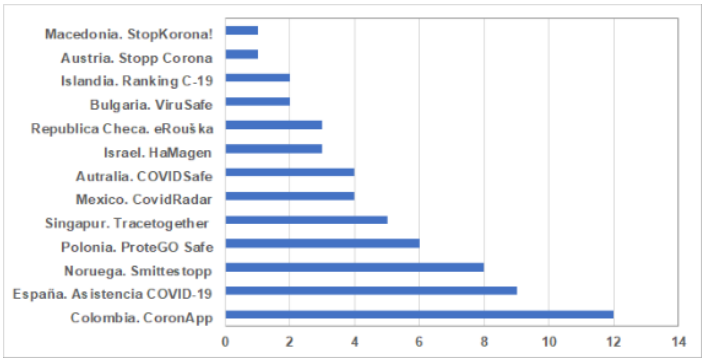
Respecto de las tres aplicaciones que usan GPS y un sistema centralizado de almacenamiento, ViruSafe (Bulgaria) no elimina los datos de sus usuarios, en tanto que Asistencia COVID-19 (España) puede tomarse hasta dos años en hacerlo. En cambio, Smittestopp (Noruega) los elimina en 30 días, al igual que la aplicación austríaca y la checa. El caso de

ViruSafe (Bulgaria) combina un almacenamiento centralizado de datos, que incluyen la georreferenciación de sus usuarios con la no eliminación de dichos datos, lo que puede resultar problemático en términos de asegurar el resguardo de la privacidad de los primeros. En un sentido similar, la app española mezcla un sistema de almacenamiento centralizado con registro de GPS y un periodo extenso de eliminación de datos.

Al igual que ViruSafe (Bulgaria), las aplicaciones CoronApp (Colombia) y CovidRadar (México), ambas con un sistema de almacenamiento centralizado de datos, tampoco eliminan los datos de sus usuarios. En tanto, HaMagen de Israel (almacenamiento descentralizado y GPS) puede tomarse hasta 7 años en hacerlo.

Otra característica importante es la cantidad de tipos de datos de sus usuarios que estas apps declaran almacenar. Al respecto, como muestra la figura 4, las apps colombiana y española son las que mayor cantidad de tipos distintos de datos almacenarían. Así, para mostrar los extremos, mientras CoronApp (Colombia) afirma almacenar 12 tipos de datos de sus usuarios y Asistencia COVID-19 (España) almacenaría 9, las apps Stopp Corona (Austria) y StopKorona! (Macedonia) declaran almacenar solamente el número de teléfono.

Figura 4. Cantidad de tipos de datos almacenados por cada aplicación



Fuente: Elaboración propia en base a los documentos referidos en las notas al pie 8 a 20.

Por último, es interesante indagar en las instituciones que desarrollan las aplicaciones y las encargadas de administrar los datos recopilados. Respecto al primer aspecto, casi la mitad (6 de las 13 aplicaciones analizadas) fueron desarrolladas por organismos estatales; cuatro fueron desarrolladas en un trabajo conjunto entre organismos públicos y privados (Colombia, España, Israel y Macedonia); dos fueron desarrolladas por empresas privadas (en Bulgaria, ScaleFocus y en México, LERTEK S.A); y una fue desarrollada por una ONG, la Cruz Roja, en el caso de la app austríaca.

Respecto al órgano responsable de administrar los datos recopilados, en los 13 casos analizados dicho órgano se trata de una entidad pública de salud, siendo la mayoría de las veces (7 de 13) directamente el Ministerio de Salud de cada país el responsable de la administración de los datos, tal como lo recomienda la UE.

Consideraciones finales

En conclusión, las tecnologías pueden acoplarse de distintas formas a determinadas exigencias normativas y sociales. Concretamente, esto significa, por ejemplo, que si un Estado miembro de la UE implementa las directrices europeas en su territorio, está comunicando formalmente a sus ciudadanos que, además de intentar protegerlos del COVID-19, está protegiendo su derecho a privacidad. Ello resulta fundamental, de acuerdo con las agencias europeas de protección de datos personales, aunque no suficiente para lograr que una app de rastreo de contactos tenga éxito en su implementación.

La relevancia de tal aproximación, en un marco voluntario, radica en que la operación efectiva de las apps de rastreo de contacto en el control de la pandemia exige que estas sean utilizadas por una parte importante de la población. Ello implica, entre otros aspectos, una implementación adecuada y una base de legitimidad social. Es decir, no se trata de que por un carril vaya la "efectividad técnica" de la app y por otro, su "legitimidad social". En este punto particular, efectividad técnica y legitimidad social se identifican: si la aplicación no puede acceder a determinados datos personales de una porción significativa de la población, esta simplemente no puede cumplir de manera efectiva su función sanitaria en relación con el COVID-19.

Así, desde un punto de vista meramente estratégico, el cumplimiento de la normativa nacional e internacional de respeto a la privacidad puede constituir un primer elemento, entre varios otros necesarios de coordinar, que permita a la población confiar en la entrega –proporcional y estrictamente necesaria- de sus datos personales a la autoridad sanitaria, con el solo fin de que esta pueda tomar medidas sanitarias para enfrentar la pandemia actual.

Autores:
Christine Weidenslaufer y Matias Meza- Lopehandía – Área de Análisis Legal
Carlos Medel - Área de Políticas Sociales

Editores:
M. Pilar Lampert – Área de Políticas Sociales
Raimundo Roberts – Área de Recursos Naturales, Ciencia y Tecnología.

Diagramación: David Manríquez - Unidad de Arquitectura de Información

1 BBC. 2020. Coronavirus contact-tracing: World split between two types of app. May 7, 2020. Disponible en: https://www.bbc.com/news/technology-52355028 (junio, 2020).

2 Landau, Susan. 2020. Location Surveillance to Counter COVID-19: Efficacy Is What Matters. Lawfare, 25/03/2020. Disponible en: http://bcn.cl/2e56w (Junio, 2020).

3 De Montjoye, Yves-Alexandre; Florimond Houssiau, Andrea Gadotti, Florent Guepin. 2020. Evaluating COVID-19 contact tracing apps? Here are 8 privacy questions we think you should ask. Disponible en: https://cutt.ly/EyMLBN7 (junio, 2020).

4 Hidalgo, Cesar. 2020. Privacidad, datos y pandemias. Disponible en: https://cutt.ly/tySjJzz (junio, 2020).

5 European Data Protection Board (EDPB). 2020. Carta de 14 de abril, 2020. Disponible en: http://bcn.cl/2e584 (junio, 2020).

6 Landau, Susan. 2020. Op. cit.

7 European Centre for Disease Prevention and Control (ECDC). 2020. Contact tracing for COVID-19: current evidence, options for scale-up and an assessment of resources needed. May 5, 2020. Disponible en: http://bcn.cl/2e58w (junio, 2020).

8 WHO. 2019. Guideline: recommendations on digital interventions for health system strengthening. Geneva: World Health Organization. Disponible en: https://cutt.ly/RySsvT6 (junio, 2020).

9 Parliamentary Office of Science and Technology, POST. 2020. Contact tracing apps for COVID-19. Disponible en: http://bcn.cl/2e56t (junio, 2020).

10 eHealth Network. 2020. Mobile applications to support contact tracing in the EU's fight against COVID-19. Common EU Toolbox for Member States. Disponible en: http://bcn.cl/2e58y (junio, 2020).

11 European Centre for Disease Prevention and Control (ECDC). 2020. Op. cit.

12 European Centre for Disease Prevention and Control (ECDC). 2020. Op. cit.

13 eHealth Network. 2020. Op. cit.

14 (ECDC). 2020. Contact tracing for COVID-19: current evidence, options for scale-up and an assessment of resources needed. Opcit.

15 Latour, Bruno. 1992. "Where are the missing masses? The sociology of a few mundane artifacts", in Bijker, Wiebe E.; Law, John (eds.), Shaping technology/building society: studies in sociotechnical change, Cambridge, Massachusetts: MIT Press, pp. 225–258.

16 De Montjoye, Yves-Alexandre; Florimond Houssiau, Andrea Gadotti, Florent Guepin. 2020. Evaluating COVID-19 contact tracing apps? Op cit.

17 European Centre for Disease Prevention and Control (ECDC). 2020. Op cit

18 Hidalgo, Cesar. 2020. Op cit.

19 European Data Protection Board (EDPB). 2020. Op. cit.

20 Parliamentary Office of Science and Technology, POST. 2020. Contact tracing apps for COVID-19. Disponible en: http://bcn.cl/2e56t (junio, 2020).

21 O'Neill, Patrick Howell; Tate Ryan-Mosley y Bobbie Johnson. 2020. Covid Tracing Tracker. MIT Technology Review, May 7, 2020. Disponible en: http://bcn.cl/2e56q (junio, 2020).

22 Ferrer, Eduardo y Alfonso Herrera. 2017. La suspensión de derechos humanos y garantías. Una perspectiva de derecho comparad y desde la Convención Americana sobre Derechos Humanos. En Gerardo Esquivel, Francisco Ibarra y Pedro Salazar. Cien ensayos para el centenario. Constitución Política de los Estados Unidos Mexicanos, tomo 2: Estudios jurídicos. Ciudad de México: UNAM.

23 HRW. 2020. Mobile Location Data and Covid-19: Q&A. 13/05/2020. Disponible en: http://bcn.cl/2e574 (junio, 2020).

24 AGNU, 2020. Las pandemias y la libertad de opinión y de expresión. Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y expresión. A/HRC/44/49. Disponible en: https://cutt.ly/byDQnPX (junio, 2020).

25 Cooper, Dan y Lynn, Miles. 2020. EU Commission Releases Guidance on COVID-19 Apps. Inside Privacy, de Covington & Burling LLP. 20 abril, 2020. Disponible en: http://bcn.cl/2e58m (junio, 2020).

26 European Data Protection Board (EDPB). 2020. Op. cit.

27 Privacy Amendment (Public Health Contact Information) Bill 2020. Explanatory Memorandum, 2019. Disponible en: http://bcn.cl/2e58f (junio, 2020).

28 The Guardian. 2020. How did the Covidsafe app go from being vital to almost irrelevant? Disponible en: http://bcn.cl/2e5hd (junio, 2020).

29 Los casos fueron seleccionados considerándose exclusivamente su funcionalidad de rastreo de contactos, y no otras relacionadas con la pandemia (aunque puedan estar incorporadas en las mismas), tales como herramientas de autodiagnóstico, provisión de información y cumplimiento de cuarentenas, registro de aislamiento, entrega de reportes médicos, atención médica telemática, recordatorio de medidas de prevención; entre otras.

30 Parte de la información contenida en la Tabla ha sido recogida por el proyecto Contract Tracing Tracker, publicado por el MIT Technology Review; otra fue obtenida de los sitios web de cada una de las aplicaciones o consorcios específicos y la restante de artículos web especializados en tecnología.

31 Disponible en: http://bcn.cl/2e586 (junio, 2020).

32 Disponible en: https://stop.koronavirus.gov.mk/en (junio, 2020).

33 Disponible en: https://participate.roteskreuz.at/stopp-corona/ (junio, 2020).

34 Disponible en: http://covidradar.mx/ (junio, 2020).

35 Disponible en: https://virusafe.info/ (junio, 2020).

36 Disponible en: https://helsenorge.no/coronavirus/smittestopp?redirect=false/ (junio, 2020).

37 Disponible en: https://www.ins.gov.co/Terminos_y_condiciones_CoronApp.pdf y http://bcn.cl/2e588 (junio, 2020).

38 Disponible en: https://govtech.gov.pl/protegosafe/ (junio, 2020).

39 Disponible en: https://asistencia.covid19.gob.es/ (junio, 2020).

40 Disponible en: https://erouska.cz/ (junio, 2020).

41 Disponible en: https://www.covid.is/app/en (junio, 2020).

42 Disponible en: https://www.tracetogether.gov.sg/ (junio, 2020).

43 Disponible en: https://govextra.gov.il/ministry-of-health/hamagen-app/download-en/ (junio, 2020).

44 Latour, Bruno. 1987. Science in action: how to follow scientists and engineers through society. Cambridge, Massachusetts: Harvard University Press.

45 “CoronApp: La nueva aplicación de Chile para combatir la pandemia", Gobdigital, 16 de abril, 2020. Información disponible en: http://bcn.cl/2ejdu (junio, 2020).

46 Sitio web de la aplicación CoronApp, gobierno de Chile. Información disponible en: https://coronapp.gob.cl/ (junio, 2020).

47 Términos y condiciones. CoronApp. Disponible en: https://coronapp.gob.cl/terminos.html (junio, 2020).

48 Política de Privacidad. CoronApp Disponible en: https://coronapp.gob.cl/politicas.html (junio, 2020).

49 Oficio N° 675 del 7 de mayo, Del Consejo para la Transparencia a ministros de Segpres y Minsal. CPLT. Disponible en: http://bcn.cl/2ejdw (junio, 2020).