COVID-19:
Las tecnologías de rastreo de contactos en dispositivos móviles y el derecho a la privacidad

Regulación nacional, derecho internacional y comparado

Autores

Christine Weidenslaufer
Email: cweidenslaufer@bcn.cl
Tel.: (56) 2 2270 1892

Matías Meza-Lopehandía
Email: mmezalopehandia@bcn.cl
Tel.: (56) 32 226 3965

Carlos Medel
Email: cmedel@bcn.cl
Tel.: (56) 32 226 3160

Nº SUP: 125043

Resumen

El Informe analiza el funcionamiento de las principales aplicaciones con rastreo de contactos diseñadas para enfrentar el COVID-19, con el objetivo de indagar sus oportunidades y riesgos asociados. Se pone especial énfasis en el marco normativo aplicable a este tipo de dispositivos, abordando el derecho internacional de los DDHH, la normativa supranacional de la Unión Europea, las modificaciones a la normativa nacional de dos casos (Australia y Colombia) y la situación normativa chilena.

La decisión, por parte de los gobiernos nacionales, de desarrollar una aplicación de este tipo implica entrelazar aspectos técnicos (efectividad), con aspectos normativos (respecto de privacidad) y sociales (evitar exclusión). La Unión Europea ha hecho recomendaciones acerca de qué tecnologías compatibilizarían mejor con el respeto a la privacidad y la inclusión social, inclinándose, por ejemplo, por un sistema descentralizado de almacenamiento de datos privados y por utilizar Bluetooth en lugar de G.P.S como tecnología base, buscando maximizar la efectividad y minimizar la cantidad de información procesada. Sin embargo, el análisis de trece aplicaciones actualmente en funcionamiento mostró que, en la práctica, predominan sistemas tecnológicos híbridos, por lo que este informe evalúa la relación entre tecnología, normativa e inclusión social, siguiendo las combinaciones tecnológicas más frecuentes.

En términos del derecho a la privacidad y el uso de estos dispositivos, los organismos competentes en DDHH han señalado que, en el contexto del COVID-19, el derecho a la vida privada, bajo circunstancias excepcionales, que sean oficialmente proclamadas (estados de excepción constitucional), puede ser suspendido, y que dicha suspensión queda sujeta al principio de proporcionalidad y de mínima intervención, la que, conforme al derecho internacional de los derechos humanos, debería ser legal, necesaria y proporcional.

Finalmente, respecto a la normativa a nivel nacional, Australia acaba de promulgar una ley *ad hoc* para su aplicación, COVIDSafe, especificando los protocolos a seguir en orden a cumplir su normativa vigente.

Tabla de contenidos

Introducción

En el ámbito de la salud, así como en el resto de la sociedad, las tecnologías de la información están redefiniendo las interacciones sociales, modificando desde la manera en que los pacientes acceden a la información sanitaria hasta los procedimientos con los que se les diagnostica y trata[1].

En relación con el COVID-19, diversos países están utilizado aplicaciones (*apps*) que rastrean, a través del teléfono móvil, los movimientos de las personas para identificar y entregar recomendaciones sanitarias a quienes, incluso sin saberlo, hayan estado en contacto con un caso de COVID-19 positivo (eHealth Network, 2020).

En la elaboración de estas aplicaciones concurren factores de diversa índole, como los aspectos técnicos y su eficacia para enfrentar el COVID-19 o su capacidad de cumplir con el marco normativo

[1] Respecto a las transformaciones de las tecnologías de la información en el sector salud, ver Davis, *et. al.*, 2020 y WHO, 2019. Sobre un análisis general de las tecnologías de la información, ver Castells, 2005.

aplicable, como también variables sociales, ya que la efectividad de dichas aplicaciones depende de su uso masivo por parte de la población. Esto abre diversas interrogantes, que van desde las condiciones que facilitan su uso por la población (por ejemplo, confianza en la autoridad, o en la tecnología propuesta), hasta el problema de las brechas de acceso que afectan a determinados grupos (por ejemplo, personas con baja alfabetización digital o sin acceso a equipos móviles).

El presente Informe aborda el funcionamiento de las principales aplicaciones con 'rastreo de contactos' (*contact tracing*) diseñadas para enfrentar el COVID-19, con el objetivo de indagar las oportunidades y riesgos asociados, analizando el marco normativo aplicable a este tipo de dispositivos según el derecho internacional de los DDHH, las normativas supranacionales y las normativas nacionales de algunos casos específicos, y en particular, el caso chileno.

Para esto, la primera parte de este informe analiza el funcionamiento de las aplicaciones con rastreo de contactos, así como los principales protocolos desarrollados hasta el momento. Luego, se analizan las características técnicas de trece aplicaciones actualmente en funcionamiento para enfrentar el COVID-19.

Un aspecto central, como se verá, son las decisiones técnicas que se adopten para almacenar y compartir la información sanitaria que recoge la aplicación, así como la tecnología base utilizada. La mayoría de las aplicaciones con rastreo de contactos utiliza un sistema de almacenamiento de los datos ‘centralizado’ o ‘descentralizado’, lo que define ciertas funcionalidades y determinada manera de tratar los datos de sus usuarios. Además, cada una de ellas debe adoptar una tecnología de base, que, en general, son Bluetooth o G.P.S, las cuales también permiten algunas funcionalidades y restringe otras, dependiendo de la tecnología base adoptada.

La segunda parte de este Informe analiza las implicancias normativas del uso de aplicaciones con rastreo de contactos. Si bien el uso de esta tecnología puede traer beneficios a la sociedad en general, la construcción de un dispositivo también implica gestionar los riesgos asociados a su uso. En ese sentido, los aspectos más sensibles son el respeto de la normativa vigente, especialmente la referida a la privacidad de las personas, y el evitar la exclusión de grupos de población que pueden estar en desventaja al usar la aplicación, como, por ejemplo, los adultos mayores, las personas con baja alfabetización digital y los inmigrantes (de Montjoye, *et. al.*, 2020).

Al respecto, esta segunda parte empieza analizando la normativa internacional sobre derechos humanos, indagando en la manera en que se interpreta el respeto a los derechos fundamentales (especialmente el de privacidad y protección de datos personales) en el contexto de la emergencia sanitaria actual. Luego, analiza la normativa supranacional, específicamente las recomendaciones que la Unión Europea hizo a sus Estados Parte para que las aplicaciones con rastreo de contactos, usadas para enfrentar el COVID-19, cumplan con la normativa vigente.

Finalmente, el Informe analiza el problema normativo a nivel nacional, en donde el uso de la mencionada tecnología puede implicar la modificación de la normativa vigente (como ocurre en varios países de la Unión Europea) o la creación de una normativa nueva, referida específicamente al uso de

tales dispositivos (como es el caso de Australia y Colombia). Para el caso de Chile, se considera su legislación vigente, la nueva aplicación recién lanzada, y los proyectos de ley relativos al tema.

Atendido el rápido desarrollo de la contingencia, las materias tratadas en el presente Informe son esencialmente dinámicas. En consecuencia, su contenido corresponde a información disponible y vigente al momento de su elaboración (26.05.2020).

El documento cita las fuentes originales (en inglés), traducidas al castellano por los propios autores de este trabajo. No fue posible utilizar traducciones oficiales porque se trata, en su mayoría, de documentos elaborados recientemente (abril/mayo del 2020), respecto de los cuales no hay dicho tipo de traducciones.

I. Rastreo de contactos del COVID-19. Funcionamiento, protocolos y aplicaciones desarrolladas.

1. Funcionamiento del rastreo de contactos para enfrentar el COVID-19.

La digitalización de las interacciones sociales también ha alcanzado el campo de la salud, haciendo emerger nuevas maneras de enfrentar los desafíos sanitarios y ofreciendo la posibilidad de aumentar su cobertura y calidad. Así, la OMS define ‘salud digital’ (*digital health*) como el “uso de las tecnologías de la información y comunicación en apoyo a la salud y los campos relacionados con ella”, lo que incluye la ‘salud móvil’, esto es, el uso de tecnologías inalámbricas en la salud pública, así como la incorporación de “áreas emergentes, como el uso de ciencias informáticas avanzadas en 'big data', la genómica y la inteligencia artificial” (WHO, 2019:1).

De manera general, una 'intervención digital en salud' (*digital health intervention*) es cualquier funcionalidad específica de una determinada tecnología digital que sea utilizada para alcanzar un objetivo sanitario. Respecto a la emergencia sanitaria del COVID-19, resulta particularmente interesante la 'intervención digital' denominada 'seguimiento digital' (*digital tracking*) y su rol en la provisión de servicios sanitarios. Esta es definida por la OMS como el “uso de un registro digitalizado para capturar y almacenar información de salud de los clientes con el fin de hacer un seguimiento de su estado de salud y los servicios recibidos” (WHO, 2019: 64).

El 'seguimiento digital' ayuda a que los trabajadores de la salud puedan garantizar que las personas reciban los servicios adecuados, pudiendo incluir, por ejemplo, formularios digitales de registros en papel, registros de gestión de casos en poblaciones objetivo específicas, así como registros electrónicos de pacientes identificados de forma única (ID) (WHO, 2019: xvi).

La OMS recomienda a los Estados el uso del ‘seguimiento digital’ para mejorar la cobertura y calidad de la salud, pero sólo en los casos en que el sistema de salud pueda apoyar la implementación de estos componentes de intervención de manera integrada; para tareas que ya estén definidas dentro del alcance de los trabajadores de la salud; y abordando adecuadamente las preocupaciones sobre la privacidad de los datos y la transmisión de contenido confidencial a los clientes (pacientes) (WHO, 2019: xxi).

Además, en el uso de ‘seguimiento digital’, la OMS recomienda prestar especial atención a las

> necesidades, preferencias y circunstancias de grupos particularmente desfavorecidos o difíciles de alcanzar, incluidas las personas con baja alfabetización digital, personas que hablan idiomas minoritarios, poblaciones migrantes en nuevos entornos, personas afectadas por situaciones de emergencia, o personas con discapacidades, como discapacidad visual o auditiva (WHO, 2019: 84).

Finalmente, respecto a las recomendaciones técnicas, la OMS propone seguir los Principios para el Desarrollo Digital, que incluyen el uso de estándares abiertos, de datos abiertos, de códigos abiertos y de innovación abierta (*open innovation*) (WHO, 2019: 85).

Una forma particular de 'seguimiento digital' lo constituye el 'rastreo de contactos' (*contact tracing*), que ha cobrado relevancia en la emergencia sanitaria del COVID-19. Este es entendido como el proceso de identificar a todos quienes hayan entrado en contacto físico con una persona contagiada, de manera de advertirles que pueden estar en riesgo de enfermarse. Así, basándose en la cercanía y tiempo de duración del contacto con el infectado, la autoridad sanitaria puede orientar el comportamiento de quienes estén, sin saberlo, en riesgo de contagio (POST, 2020).

Ese procedimiento, tradicionalmente realizado de manera manual por el personal de salud (registro escrito), es automatizado por dichas aplicaciones, lo que trae aparejado ventajas y riesgos. Su principal ventaja radica en que, al tratarse de un método automatizado, no depende ni de la memoria de la persona infectada ni de que la persona infectada conozca o no a quienes hayan estado cerca suyo (WHO, 2019).

El dispositivo rastrea automáticamente a todos quienes, consciente o inconscientemente, tuvieron un contacto con un infectado, pudiendo ser efectivo, por ejemplo, para rastrear los contactos de los infectados asintomáticos. Lo central acá es la definición de qué constituye un 'contacto' y de qué tipo de contacto se trata ('estrecho' o 'de bajo riesgo'). Según el protocolo de la Unión Europea (UE), un ‘contacto’, es cualquier persona que haya tenido cercanía física con un caso COVID-19 en un período de tiempo que va desde las 48 horas antes del inicio de los síntomas hasta 14 días después de iniciados, según el Centro Europeo para la Prevención y el Control de Enfermedades de la UE (*European Centre for Disease Prevention and Control*, ECDC, 2020a: 2). En tanto, un ‘contacto estrecho’, según la UE, lo constituye cualquier contacto físico con un infectado de al menos 15 minutos de duración y a menos de 1,5 metros de distancia (eHealth Network, 2020).

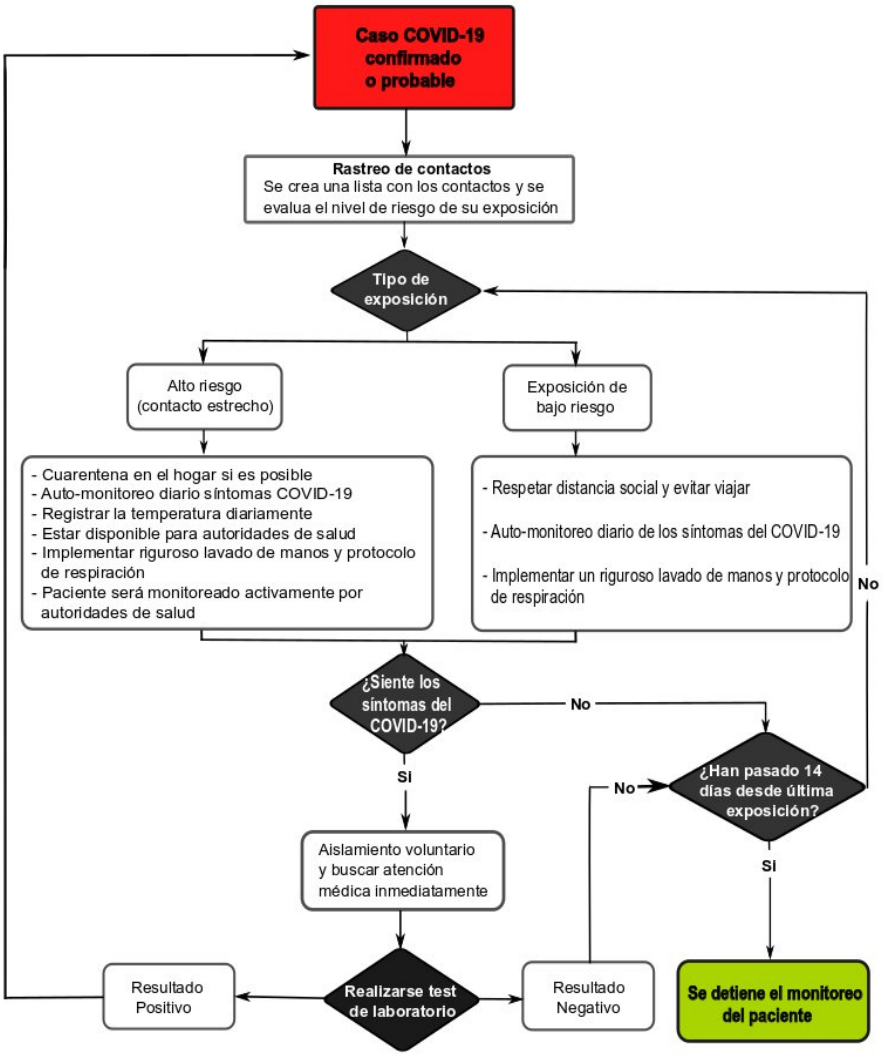
Para el mencionado Centro de la UE, el rastreo de contactos constituye una medida esencial para combatir la emergencia sanitaria del COVID-19, en sinergia con otras, como el distanciamiento social y la aplicación masiva de test (ECDC, 2020a:2). Según el protocolo de este organismo, una vez confirmado un caso positivo de COVID-19 el rastreo de contactos realiza las siguientes acciones:

- Se entrevista el caso para recopilar información sobre los posibles contactos que ocurrieron desde 48 horas antes del inicio de los síntomas hasta su aislamiento. Esto se realiza telefónicamente;
- Se rastrean los contactos y se clasifican según su nivel de exposición: de alto riesgo ('contacto estrecho') o de bajo riesgo;

- Se coordina la realización del test para los contactos sintomáticos; y
- Se rastrean y se entabla comunicación con los contactos identificados y se les proporciona información sobre las medidas adecuadas de control de infecciones, monitoreo de síntomas y otras medidas de precaución, como la necesidad de cuarentena (ECDC, 2020a:2).

El riesgo asociado de infección depende del nivel de exposición que se tuvo ante un caso COVID-19, por lo que el tipo de seguimiento y monitoreo dependerá de si se tuvo un 'contacto estrecho' o un 'contacto de bajo riesgo'. En caso de que haya sido un 'contacto estrecho', como muestra la Figura 1, la persona debe guardar cuarentena, auto monitorear los síntomas del COVID-19 diariamente, registrar su temperatura también a diario, implementar el protocolo de lavado de manos y respiración, y estar disponible para las autoridades de salud, quienes monitorearán a dicha persona hasta 14 días después de haber dejado de sentir síntomas. Si, por el contrario, se trató de un 'contacto de bajo riesgo', la persona debe respetar la distancia social y evitar viajar, auto monitorearse diariamente los síntomas del COVID-19, e implementar el protocolo de lavado de manos y respiración (ECDC, 2020a: 2).

Figura 1. Algoritmo para el manejo de contactos de casos de COVID-19, protocolo de la Unión Europea.



Fuente: ECDC, 2020, p. 7. Traducción propia.

La evidencia empírica sobre la efectividad del rastreo de contactos analizada por el Centro de la Unión Europea, sugiere que éste fue efectivo en varios países, sin embargo, su efecto real resulta difícil de cuantificar ya que siempre estuvo acompañado por otras medidas de control adoptadas en paralelo, como, por ejemplo, la prohibición de reuniones y cuarentenas (ECDC, 2020a:2). Además, la evidencia empírica de la efectividad del rastreo de contacto, así como de cualquier medida para enfrentar el COVID-19, se sistematiza en un contexto en el que no se tiene información certera acerca de las características de un virus, que, además, ha mostrado una alta velocidad de expansión y una dinámica evolutiva no lineal.

Por otra parte, algunos especialistas han puesto en duda la efectividad de ciertas tecnologías de rastreo. En particular, Susan Landau (2020), profesora en ciberseguridad de la Universidad Tufts, cuestiona la utilidad de la georeferenciación a través de las antenas de telefonía y aquella basadas en GPS[2] o en Wifi. Estas no proveerían información suficientemente precisa como para determinar si una persona estuvo en contacto peligroso con otra infectada, entre otros problemas. En el mismo sentido, el grupo de académicos firmantes del *Contact Tracing Joint Statement s*eñalaron que "las soluciones basadas en el uso compartido de geolocalización para rastrear contactos carecen de suficiente precisión y también conllevan riesgos de privacidad porque los datos del GPS se envían a una ubicación centralizada. Por esta razón, resulta altamente preferible el uso de soluciones basadas en Bluetooth, cuando estén disponibles" (KU Leuven, 2020b). Por otra parte, el análisis técnico desarrollado por Meckelburg concluyó que, considerando los modelos de *smart phones* disponibles en el mercado, Bluetooth BLE correspondería a la tecnología más eficaz para medir proximidad física en la actualidad (Meckelburg, 2020:15).

Frente a esto, la ONG basada en Nueva York Human Rights Watch (HRW), ha señalado que aunque el uso de la tecnología Bluetooth para el rastreo de interacciones ha sido presentada como más efectiva y menos invasiva, esto aun no habría sido probado, y podría ser particularmente sensible cuando la información se almacena en forma centralizada (HRW, 2020). En el mismo sentido apunta la ONG dedicada a la defensa de derechos digitales, Electronic Frontier Foundation, al evaluar la API de exposición desarrollada por Apple y Google con tecnología Bluetooth (Cypers y Gebhart, 2020).

A pesar de lo anterior, el Centro Europeo para la Prevención y el Control de Enfermedades (ECDC, 2020a: 2) valoró positivamente la evidencia empírica del uso del rastreo de contactos en diversos países asiáticos, al señalar que:

- Singapur y varias provincias en China pudieron limitar la cantidad de brotes iniciales a través de test generalizados, rastreo de contactos y cuarentena, y estos esfuerzos siguen siendo claves para la contención actual del virus;
- El rastreo de contactos resultó en la identificación de muchos casos nuevos, a menudo antes del inicio de los síntomas, y redujo sustancialmente el tiempo desde el inicio de los síntomas hasta el aislamiento, disminuyendo así la probabilidad de transmisión;
- La evidencia de Singapur ha resaltado el papel de la transmisión presintomática en la dinámica general del brote, lo que sugiere que el control de la pandemia requiere una cuarentena rápida de los ‘contactos estrechos’ para prevenir la transmisión posterior;

[2] Ver en: https://www.gps.gov/ (marzo, 2020)

- En Vietnam, donde se están realizando grandes esfuerzos para aislar casos y rastrear y poner en cuarentena sus contactos, se está considerando el uso de inteligencia artificial para potenciar aún más el rastreo de contactos y el manejo de pacientes potencialmente infectados.

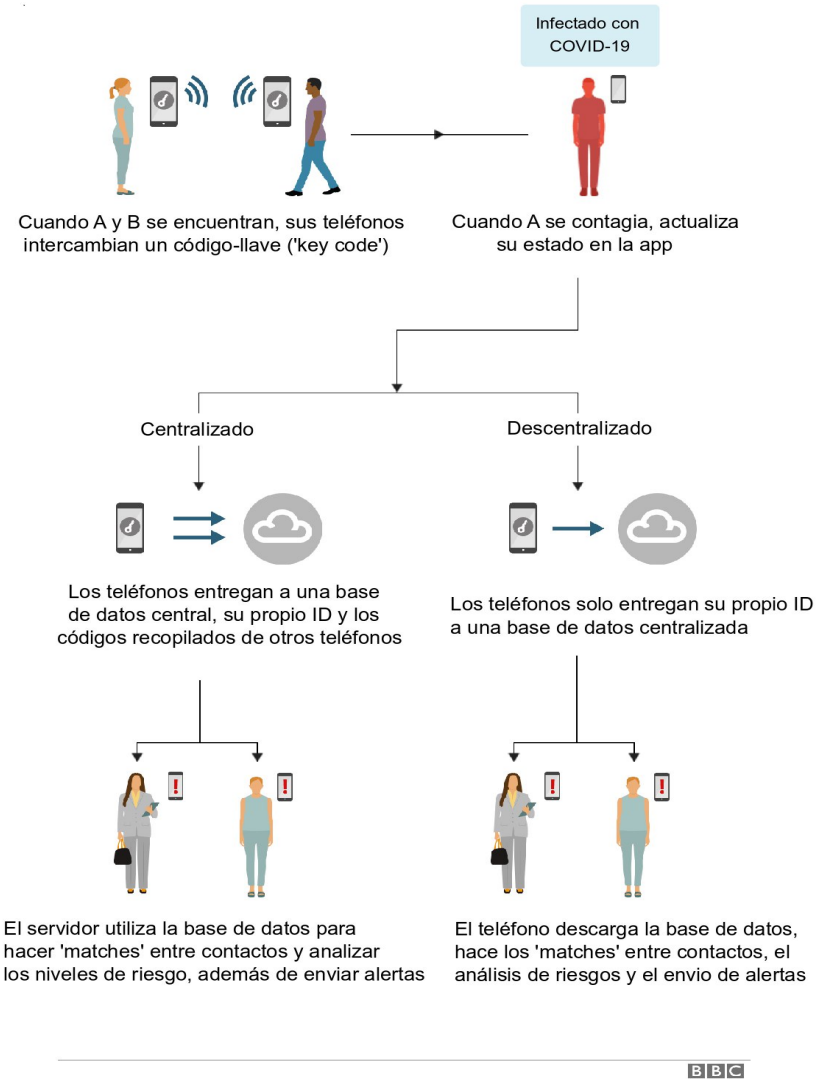
De esta forma, diversos gobiernos han ido adoptado medidas técnicas, como por ejemplo el rastreo de contactos, casi al mismo tiempo en que han ido conociendo el comportamiento del COVID-19 en la población. Lo anterior exige a los Estados equilibrar al mismo tiempo aspectos de diversa índole, siendo especialmente relevantes, por una parte, la efectividad concreta de dichas herramientas digitales para el control del COVID-19, y, por otra, el respeto de dichas aplicaciones del derecho a la privacidad de las personas y la protección de sus datos personales. Las alternativas tecnológicas de funcionamiento del rastreo de contactos disponibles permiten compatibilizar exigencias técnicas (efectividad de la herramienta) con exigencias normativas (respeto a los derechos fundamentales) si ambas exigencias son consideradas desde la concepción y el diseño de dichas aplicaciones.

2. Los principales protocolos y modelos de almacenamiento de 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 un sistema 'descentralizado' o 'centralizado' de almacenamiento de la información de sus usuarios (Figura 2). En los sistemas centralizados, una vez anonimizados los datos de las personas, estos son almacenados a un servidor central gestionado por la autoridad a cargo de la aplicación. En los modelos descentralizados, en cambio, la información se almacena localmente, usando el teléfono móvil de cada persona, compartiéndose con la autoridad sanitaria la menor cantidad de información privada posible (Hidalgo, 2020).

Así, al momento de decidir el tipo de almacenamiento de los datos de los usuarios, paralelamente están en juego factores de efectividad y otros de índole normativos y sociales: un almacenamiento centralizado permite recopilar mayor cantidad de información, aunque también presenta mayores riesgos para la privacidad de las personas. Al respecto, por ejemplo, si bien las directrices de la Unión Europea recomiendan fuertemente el uso de una gestión de datos descentralizada (EDPB, 2020), el Reino Unido está desarrollando una aplicación con gestión centralizada, la cual, según informa la prensa británica, estaría sufriendo importantes problemas de seguridad en el almacenamiento de los datos de sus usuarios (BBC, 2020b). Es decir, este tipo de decisiones no son meramente técnicas, sino que técnico-normativas: tienen como trasfondo la búsqueda del equilibrio entre la efectividad técnica y el respeto de la normativa, para lo cual no existe una ‘receta única’ sino que las aplicaciones desarrollan su manera particular de equilibrar dicha ecuación, considerando las alternativas técnicas disponibles y la normativa vigente en su territorio.

Figura 2. Sistemas de almacenamiento de los datos personales en las apps para rastrear COVID-19.



Fuente: BBC (2020a). Traducción propia.

Ya sea se trate de sistemas de almacenamiento 'centralizados' o 'descentralizados', los expertos recomiendan que los datos se eliminen una vez el riesgo de infección haya pasado. La UE recomienda que se borren los datos entre 14 y 16 días después del contacto y que se publique tanto el código fuente como el protocolo de la aplicación para entender cabalmente la manera en que los datos fueron usados y recopilados (POST, 2020).

El 19 de abril de 2020, 304 académicos de todo el mundo firmaron una carta (*Contact Tracing Joint Statement*) advirtiendo contra la adopción de modelos centralizados ya que, incluso con fichas anónimas, los datos centralizados podrían ser desanonimizados y utilizados para fines de vigilancia.[3]

[3] A la fecha, de acuerdo al propio documento electrónico de la carta, el número total actual de firmas es 636,

Asimismo, una base de datos centralizada podría ser un objetivo atractivo para terceros, aumentando el riesgo de violaciones a la seguridad de este tipo de modelos (POST, 2020).

Por otra parte, optar por un sistema descentralizado[4] supone renunciar a una instancia centralizada de almacenamiento, no pudiéndose utilizar los datos recopilados para otros fines sanitarios complementarios, como, por ejemplo, investigar la eficacia de la aplicación o comprender la evolución general del virus. En un modelo descentralizado, se requeriría que los usuarios entreguen voluntariamente sus datos para este fin (POST, 2020 y KU Leuven, 2020a).

De esta forma, diferentes consorcios en el mundo, que reúnen principalmente a académicos y entidades privadas, han estado desarrollando protocolos para aplicaciones digitales de rastreo de contactos. Muchos de estos protocolos son iniciativas abiertas, esto es, su código fuente puede ser auditado libremente (eHealth Network, 2020: 10). Mientras el Parlamento Europeo ha votado a favor de la adopción de aplicaciones descentralizadas, un consorcio internacional de investigadores dirigido desde Suiza, llamado DP-3T, ha desarrollado un enfoque descentralizado, al igual que Apple y Google, entidades que en abril anunciaron su trabajo conjunto para desarrollar aplicaciones de rastreo descentralizadas en sus teléfonos (POST, 2020).

El 18 de abril de 2020 se publicaron los detalles de un protocolo de rastreo alemán que utiliza un modelo centralizado, pero el ministro de salud alemán ha anunciado desde entonces que adoptarán un enfoque descentralizado. La aplicación australiana (CovidSafe) ha sido descrita como un modelo "híbrido-centralizado", ya que los datos se almacenan en el teléfono del usuario a menos que éste haya estado en contacto con una persona infectada, en cuyo caso su identidad se revela al Ministerio de Salud (POST, 2020).

Por tanto, la tecnología básica subyacente a las aplicaciones actualmente en uso puede ser alguna de las siguientes o una combinación de ellas (O'Neill, Ryan-Mosley y Johnson, 2020):

- Localización: algunas aplicaciones identifican los contactos de una persona al rastrear los movimientos del teléfono (por ejemplo, usando GPS o triangulación desde torres de celulares cercanas) y buscando otros teléfonos que hayan pasado tiempo en la misma ubicación.
- Bluetooth: algunos sistemas utilizan el 'seguimiento de proximidad', en el cual los teléfonos intercambian *tokens* cifrados con cualquier otro teléfono cercano a través de Bluetooth. Es más fácil anonimizar y generalmente se considera mejor para la privacidad que el seguimiento de localización.

---

pues además de los 304 firmantes originales, otras 332 personas la han firmado electrónicamente. Este documento se encuentra alojado en el sitio web del departamento de Ingeniería Eléctrica (también conocido como ESAT), de la Universidad belga KU Leuven. En particular, debe señalarse que el Grupo de Seguridad Informática y Criptografía Industrial (COSIC), perteneciente al ESAT, está trabajando en el equipo del DP-3T (KU Leuven, 2020b).

[4] Los modelos descentralizados mencionados por los señalados académicos incluyen los protocolos DP-3T (https://github.com/DP-3T), TCN Coalition (https://tcn-coalition.org/), PACT (MIT) (https://pact.mit.edu/), PACT (UW) (https://covidsafe.cs.washington.edu/). Las siglas PACT corresponden a *Private Automated Contact Tracing.*

- DP-3T (*Decentralized Privacy-Preserving Proximity Tracing*): significa 'seguimiento de proximidad descentralizado que preserva la privacidad'. Es un protocolo de código abierto para el seguimiento basado en Bluetooth, en el que los registros de contactos de un teléfono individual solo se almacenan localmente, por lo que ninguna autoridad central puede saber quién ha estado expuesto al virus.
- Google-Apple: probablemente muchas aplicaciones se basarán en la API[5] conjunta que Apple y Google están desarrollando. Esta permite que los teléfonos iOS y Android se comuniquen entre sí a través de Bluetooth, lo que permite a los desarrolladores crear una aplicación de seguimiento de contactos que funcione para ambos. Más tarde, las dos compañías planean incorporar esto directamente en sus sistemas operativos. Google ha señalado que se basaron en el protocolo DP-3T para su desarrollo. Sin embargo, la UE cuestionó que el código Apple-Google no fuera público, ya que hace menos transparente el uso de la información (eHealth Network, 2020: 24). Por su probable nivel de uso a nivel internacional, este protocolo es explicado en mayor detalle en Anexo 2 al final de este documento.

3. Análisis de trece aplicaciones 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) 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 3[6][7]. En el Anexo 1, dos tablas resumen la información disponible de cada aplicación, de acuerdo a los criterios ya indicados.

[5] *Application Programming Interface*

[6] 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.

[7] 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.

Figura 3. Nombre y país donde son usadas las trece aplicaciones seleccionadas.

País	Nombre de la aplicación	País	Nombre de la aplicación
Australia	COVIDSafe[8]	Macedonia	StopKorona![9]
Austria	Stopp Corona[10]	México	CovidRadar[11]
Bulgaria	ViruSafe[12]	Noruega	Smittestopp[13]
Colombia	CoronApp[14]	Polonia	ProteGO Safe[15]
España	Asistencia COVID-19[16]	República Checa	eRouška[17]
Islandia	Rakning C-19[18]	Singapur	Tracetogether[19]
Israel	HaMagen[20]		

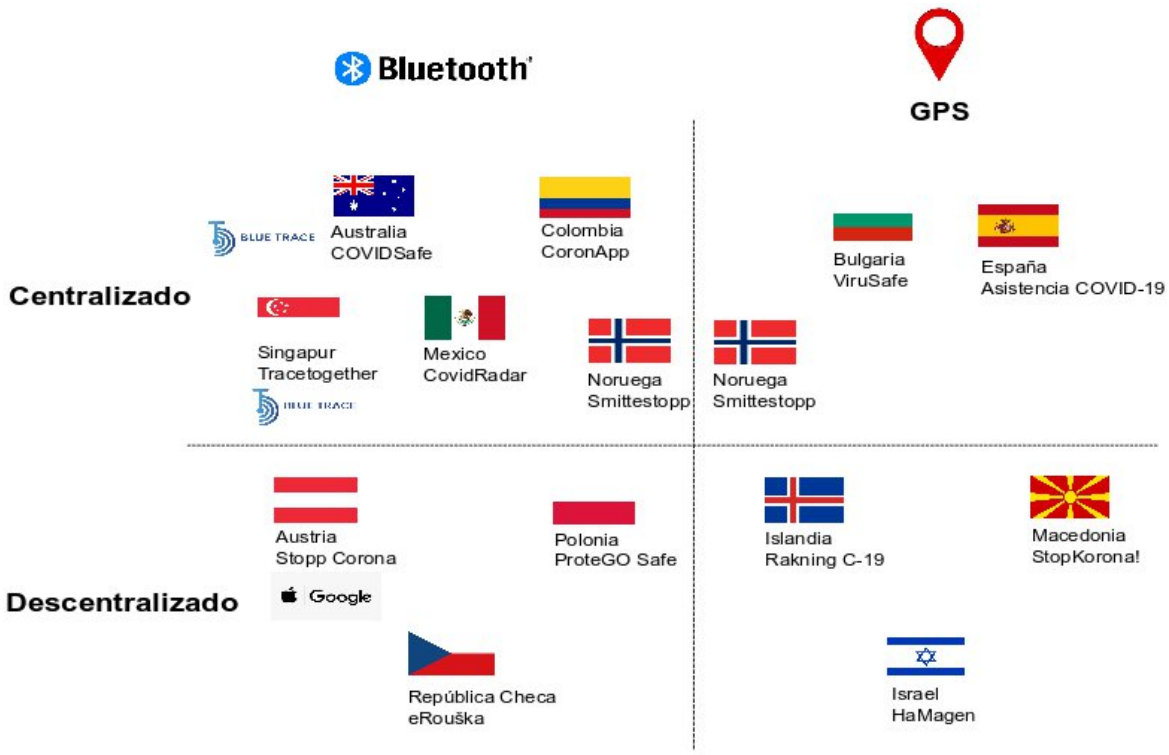
Fuente: La que se indica en la nota al pie de cada caso.

Considerando la velocidad con la que se desarrollan estas aplicaciones en la actualidad, la sistematización que presenta la Figura 3 no es exhaustiva ni definitiva.

Respecto al análisis de las características de las aplicaciones, al distribuir las trece aplicaciones seleccionadas según el soporte tecnológico base que utilizan (fundamentalmente Bluetooth o GPS) y según su sistema de almacenamiento de datos (centralizado o descentralizado), se obtuvieron los cuatro grupos de aplicaciones que muestra la Figura 4.

[8] Disponible en: http://bcn.cl/2e586 (mayo, 2020)
[9] Disponible en: https://stop.koronavirus.gov.mk/en (mayo, 2020)
[10] Disponible en: https://participate.roteskreuz.at/stopp-corona/ (mayo, 2020)
[11] Disponible en: http://covidradar.mx/ (mayo, 2020)
[12] Disponible en: https://virusafe.info/ (mayo, 2020)
[13] Disponible en: https://helsenorge.no/coronavirus/smittestopp?redirect=false/ (mayo, 2020)
[14] Disponible en: https://www.ins.gov.co/Terminos_y_condiciones_CoronApp.pdf y http://bcn.cl/2e588 (mayo, 2020)
15 Disponible en: https://govtech.gov.pl/protegosafe/ (mayo, 2020)
[16] Disponible en: https://asistencia.covid19.gob.es/ (mayo, 2020)
[17] Disponible en: https://erouska.cz/ (mayo, 2020)
[18] Disponible en: https://www.covid.is/app/en (mayo, 2020)
[19] Disponible en: https://www.tracetogether.gov.sg/ (mayo, 2020)
[20] Disponible en: https://govextra.gov.il/ministry-of-health/hamagen-app/download-en/ (mayo, 2020)

Figura 4. 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.

En los casos de las aplicaciones COVIDSafe (Australia) y Tracetogether (Singapur), ademas 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.

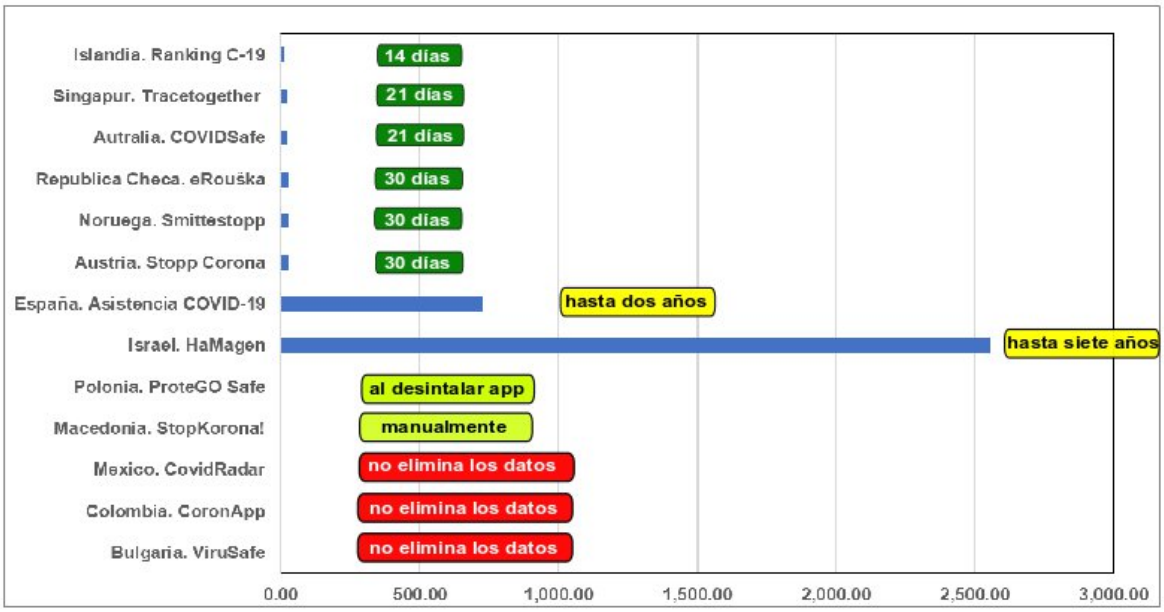
Cada una de las subdivisiones de la Figura 14 muestra un ensamblaje técnico-normativo específico, que permite funcionalidades particulares y resguarda, con mayor o menor celo, determinados derechos. Así, el grupo del cuadrante inferior izquierdo, formado por Stopp Corona (Austria), eRouška (República Checa) y ProteGO Safe (Polonia), por una parte, utiliza Bluetooh (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 los datos, por lo 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), está formado por Asistencia COVID-19 (España), ViruSafe (Bulgaria) y Smittestopp (Noruega), aplicaciones que procesan los datos georreferenciados de sus usuarios, al tiempo que almacenan la información utilizando un sistema centralizado. Como se ha señalado, el almacenamiento centralizado de los datos entrega información que el órgano (central) responsable de la aplicación puede utilizar para fines sanitarios, pero, en el mismo acto, 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, para el objetivo de este Informe resulta especialmente relevante indagar, además, en el tratamiento de los datos personales de sus usuarios, específicamente en: qué tipo de datos recopilan, si los eliminan o no, y, de hacerlo, cuánto tiempo le toma a cada aplicación borrarlos (Figura 5).

Figura 5. Eliminación de los datos personales almacenados por la aplicación.



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

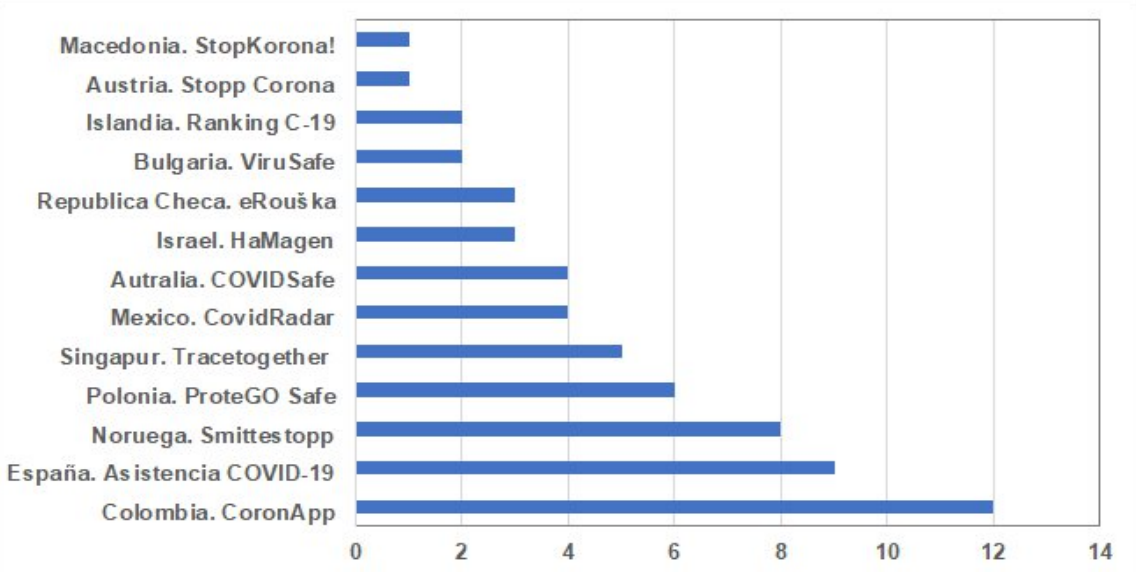
Las tres aplicaciones del cuadrante inferior izquierdo (Bluetooth - almacenamiento descentralizado) eliminan los datos almacenados y para ello Stopp Corona (Austria) y eRouška (República Checa) se toman 30 días, en tanto que ProteGO Safe (Polonia) los elimina cuando el usuario desinstala la aplicación.

Respecto de las aplicaciones del cuadrante superior derecho (GPS - almacenamiento centralizado), 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 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 sus usuarios. En un sentido similar, la aplicación española también mezcla un sistema de almacenamiento centralizado con registro de GPS y un periodo extenso para eliminar los datos de sus usuarios.

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 eliminarlos.

Otra característica importante para analizar el tratamiento de los datos personales, por parte de las aplicaciones con rastreo de contactos, es la cantidad de tipos de datos de sus usuarios que éstas declaran almacenar. Al respecto, como muestra la Figura 6, las aplicaciones 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[21] y Asistencia COVID-19 (España) señala que almacena 9[22], las aplicaciones Stopp Corona (Austria) y StopKorona! (Macedonia) declaran almacenar solamente el número de teléfono.

Figura 6. 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, otros dos aspectos relevantes en el manejo de la información son la organización u ente que desarrolla la aplicación y aquél encargado de administrar los datos recopilados. Respecto al primer aspecto, casi la mitad (6 de las 13 aplicaciones analizadas) fueron desarrolladas por organismos estatales[23]; cuatro fueron desarrolladas en un trabajo conjunto entre organismos públicos

[21] Estos son: Nombre y apellido, tipo y número de documento, número de teléfono, sexo, fecha de nacimiento, país, departamento, ciudad de residencia, correo electrónico, contraseña, origen étnico, e información médica (reporte de salud: estoy bien / estoy mal, síntomas, contacto con personas con síntomas, atención médica recibida, viaje a otros países).

[22] Estos datos son: Nombre y apellidos, número de teléfono móvil, DNI / NIE, dirección completa y código postal, fecha de nacimiento, geolocalización, género (opcional) y diversos datos de salud relacionados con los síntomas.

[23] **Australia**, el Departamento de Salud y la Agencia de Transformación Digital; **Islandia**, la Oficina del Director de Salud Pública; **Noruega**, el Instituto noruego de salud pública y Simula (organización académica); **Polonia**, el Ministerio de Asuntos Digitales; **República Checa**, el Ministerio de salud y voluntarios de la plataforma COVID19CZ; y **Singapur**, el Ministerio de Salud y la Agencia gubernamental de tecnología (GovTech).

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 aplicación 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, como se verá en la segunda parte.

Se hace la prevención que las comparaciones anteriores son el reflejo de la información provista por los sitios web respectivos a cada aplicación, pudiendo estar ella incompleta, lo que afectaría el análisis expuesto.

II. Regulación de las aplicaciones con rastreo de contactos y derechos humanos.

1. Derecho internacional de los derechos humanos.

El manejo de la pandemia del COVID-19, por sus especiales características, requiere que se tomen una serie de medidas que impactan seriamente en la vida cotidiana de las personas. De hecho, parecen poner en jaque el ejercicio de sus derechos más elementales: la libertad de tránsito, el derecho al trabajo, al salario justo, a reunión, a la salud, a la alimentación, a la educación, o el derecho a una vida libre de violencia de género, por mencionar algunos de los más evidentes (OACNUDH, 2020b). En este sentido, la Alta Comisionada de Naciones Unidas para los Derechos Humanos ha señalado que:

> Los confinamientos, las cuarentenas y otras medidas de esa índole orientadas a combatir la expansión del COVID-19 deben aplicarse siempre en la más estricta observación de las normas de derechos humanos y de manera proporcional y ponderada al riesgo en que se incurre, pero aún así pueden repercutir gravemente sobre la vida de las personas (OACNUDH, 2020a).

Por otra parte, las condiciones generadas por la crisis pueden derivar en la agudización de la discriminación y estigmatización de poblaciones e individuos pertenecientes a minorías. En efecto, los diferentes expertos del sistema universal de derechos humanos, han urgido a los gobiernos para que utilicen las medidas de emergencia en concordancia con el derecho internacional, esto es, que sean necesarias, proporcionales y no discriminatorias, y en general, que aquellas no sean usadas como excusas para suprimir la vigencia de los derechos humanos.[24]

[24] Los expertos de Naciones Unidas son parte de los mecanismos de protección de los derechos humanos, y dependen del Consejo de Derechos Humanos. Están compuestos por expertos independientes que reciben un mandato para la promoción, difusión y protección de derechos específicos alrededor del mundo (OHCHRa, 2020). En un sentido similar, la Alta Comisionada señaló recientemente que la "situación de emergencia no es un cheque en blanco para hacer caso omiso de las obligaciones en materia de derechos humanos" (OACNUDH, 2020b)

Por lo anterior, la Alta Comisionada ha llamado a "crear una estrategia mundial de mayor colaboración, basada en los derechos humanos, para hacer frente a la crisis", particularmente en relación con la posible agudización de las desigualdades y del sufrimiento humano (OACNUDH, 2020b).

Esto se relaciona con cierto tipo de medidas asociadas al distanciamiento social, en particular, la cuarentena o confinamiento y los cordones sanitarios, en tanto limitan la libertad ambulatoria. Sin embargo, como se ha señalado más arriba en este trabajo, existen otro tipo de medidas que permiten registrar los movimientos de una persona a través de una aplicación instalada en sus dispositivos móviles. Aunque estas no han sido el foco inicial de preocupación de las agencias de Naciones Unidas para la protección de derechos humanos, su utilización también genera preocupación, tanto por la agudización de las desigualdades implícita en soluciones basadas en tecnología, como por un eventual uso abusivo de la información recopilada que vulnere el derecho a la privacidad.[25] Esta última cuestión es abordada en profundidad a continuación.

1.2. El derecho a la privacidad.

El derecho a la protección de la vida privada está consagrado en el Pacto Internacional de Derechos Civiles y Políticos (PIDCP) en los siguientes términos:

> Artículo 17
> 1. Nadie será objeto de *injerencias arbitrarias o ilegales en su vida privada*, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación.
> 2. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques.[26]

En el ámbito interamericano, la Convención Americana de Derechos Humanos (CADH) reconoce el derecho a la privacidad en términos análogos al del PICDC, el que está reconocido en distintos instrumentos internacionales de derechos humanos.[27] Aunque su formulación literal no incluye limitaciones permisibles expresas -como sí se hace con otros derechos- se ha entendido que la referencia a la arbitrariedad y legalidad autorizan tales limitaciones (AGNU, 2013).

En este sentido, el Comité de Derechos Humanos (CCPR, por sus siglas en inglés), organismo de Naciones Unidas que vigila el cumplimiento del PIDCP, ha aclarado que si bien la ley puede autorizar intrusiones en la privacidad -que debe garantizase frente a todas las injerencias, sean provenientes de

---

[25] HRW ha señalado que el uso de este tipo de tecnología es foco de preocupación, tanto porque la información de localización móvil suele contener información sensible relativa a la identidad, localización, comportamiento, relaciones sociales y actividades de los usuarios, como por la brecha digital, que afecta especialmente a las poblaciones más vulnerables frente al COVID-19, como los pobres y los ancianos (HRW, 2020). Por su parte, el Relator Especial sobre el derecho a la salud ha manifestado su preocupación porque las nuevas facultades de vigilancia expongan a los drogadictos y a otras poblaciones criminalizadas a la represión policial y al encarcelamiento (OHCHR, 2020b).

[26] Énfasis añadido. El PIDCP es un tratado internacional multilateral actualmente vigente. Fue ratificado por Chile en 1972 (Decreto N° 778 de 1989 del Ministerio de Relaciones Exteriores)

[27] A nivel universal están también la Declaración Universal de Derechos Humanos (art. 12), la Convención sobre los Derechos del Niño (art. 16), y la Convención Internacional sobre la Protección de los Derechos de Todos los Trabajadores Migratorios y de sus Familiares (art. 14). A nivel regional está protegido por el Convenio Europeo de Derechos Humanos (art. 8) y la Convención Americana sobre Derechos Humanos (art. 11).

las propias autoridades como de organismos privados-[28] estas deben ajustarse a las disposiciones, propósitos y objetivos del Pacto, no ser arbitrarias y la legislación respectiva debe "especificar con detalle las circunstancias precisas en que podrán autorizarse esas injerencias" (CCPR, 1988:párr.8). Además, exige que la autorización para la intercepción se haga por la autoridad competente evaluando su pertinencia caso a caso. Consecuentemente, prohíbe la vigilancia por medios electrónicos o de otra índole.[29]

El cambio tecnológico en esta época es tan rápido, que "las consecuencias sociales de una tecnología son raramente comprendidas antes de que se difunda y adopte" (CIDH, 2017:92). Por lo mismo, no es raro enfrentar cierto retraso en los documentos internacionales de derechos humanos en estas materias. En efecto, el Relator de Naciones Unidas para la Libertad de Expresión ha señalado que los mecanismos internacionales de protección de derechos humanos no han desarrollado plenamente el contenido del derecho a la privacidad, particularmente frente al desarrollo tecnológico (AGNU, 2013).

Sin embargo, a pesar de haber sido adoptado hace más de treinta años, la Observación General n° 16 del CCPR se refiere a la cuestión de los bancos de datos. Al respecto señala que "[l]a recopilación y el registro de información personal en computadoras, bancos de datos y otros dispositivos, tanto por las autoridades públicas como por las particulares o entidades privadas, *deben estar reglamentados por la ley*". Además, reconoce tres derechos específicos en esta materia: (i) el derecho a verificar los datos propios; (ii) el derecho a saber quién los controla; y (iii) el derecho a la rectificación o eliminación de datos incorrectos o compilados ilegalmente (CCPR, 1998: párr. 10).

Por otro lado, la noción de inviolabilidad de la correspondencia consagrada en los tratados citados, ha sido entendida tanto en el ámbito interamericano como en el europeo, como inviolabilidad de las comunicaciones, abarcando así la telefonía, el Internet e incluso los metadatos generados en el tráfico en línea (CIDH, 2017).[30]

La elaboración de la cuestión de la privacidad y protección de datos personales se ha hecho en general bajo el alero de los mecanismos de protección de la libertad de expresión, en tanto presupuesto del ejercicio de tal derecho.[31] En efecto, en un informe relativamente reciente, la Relatoría para la Libertad de Expresión de la CIDH identificó el incremento en las capacidades del Estado y de particulares para monitorear e interceptar comunicaciones y para vigilar, como un serio riesgo para el

---

[28] En el mismo sentido, en el sistema interamericano de derechos humanos, la CIDH (2017:76) ha señalado que "el ámbito de la privacidad se caracteriza por quedar exento o inmune a las invasiones o agresiones abusivas o arbitrarias por p*arte de terceros o de la autoridad pública*" (énfasis añadido).

[29] Más recientemente, la Relatoría de Libertad de Expresión de la Comisión Interamericana de Derechos Humanos (CIDH, 2017:84) ha señalado que "[l]a vigilancia en todas sus modalidades constituye una injerencia en la vida privada".

[30] En este sentido, la Corte Interamericana de Derechos Humanos ha señalado que los tratados de derechos humanos son "instrumentos vivos" que deben adaptarse a las condiciones de vida actuales (CtIDH, 2001: párr. 146). Por su parte, el Tribunal Europeo de Derechos Humanos ha desarrollado la noción de "interpretación evolutiva" de los tratados, conforme a la cual, estos se adaptan interpretándolos "de conformidad con la práctica y las convicciones generalmente reconocidas por sus Estados partes" (Pascual, 2014:127).

[31] "La intimidad y la libertad de expresión se relacionan entre sí y son mutuamente dependientes; la vulneración de una de estas puede ser tanto la causa como la consecuencia de la vulneración de la otra" (AGNU, 2013: 20). En el mismo sentido, CIDH, 2017.

derecho a la vida privada en línea, pues esta "requiere que se garantice la confidencialidad de los datos personales en línea" (CIDH, 2017:81).[32]

Como se ha señalado más arriba, el derecho internacional admite la posibilidad de restringir el alcance del derecho a la privacidad, pero toda limitación debería ser proporcional, esto es, debe tener una finalidad legitima en una sociedad democrática, ser adecuada, necesaria y proporcional. Además, deberían estar establecidas por ley,[33] y esta debe contemplar la exigencia de una orden judicial previa. En palabras de la Relatoría interamericana:

> El sistema interamericano, en consonancia con el europeo y el universal, estableció un test tripartito para verificar la legitimidad de una injerencia estatal o no estatal en la vida privada como es la vigilancia electrónica. Conforme dicho test, la medida de vigilancia ha de ser legal, en sentido formal y material, necesaria y proporcionada [...] Los objetivos conforme a los cuales se habilite el monitoreo [...] deben constar expresamente en la ley y en todos los casos las leyes deberán establecer la necesidad de una orden judicial previa (CIDH, 2017:85s).

Por su parte, el Relator de Naciones Unidas ha señalado que "[l]a legislación debe estipular que la vigilancia de las comunicaciones por el Estado solo se realice en las situaciones más excepcionales y únicamente con la supervisión de una autoridad judicial independiente" (AGNU, 2013:22).

Además, la Relatoría le asigna un valor especial a la privacidad en línea, exigiendo que la justificación de la vigilancia responda "a una necesidad cierta e imperiosa para el logro de los objetivos legítimos que persiguen", lo que excluiría *a priori* la vigilancia masiva, pues ésta "en ningún caso puede ser proporcionada" (CIDH, 2017:87s). En el mismo sentido, las relatorías de libertad de expresión del sistema universal, el africano, el europeo y el interamericano, señalaron en una declaración conjunta que "la vigilancia indirecta o masiva, es inherentemente desproporcionada y constituye una violación de los derechos de privacidad y libertad de expresión" y por lo mismo, "la vigilancia debería llevarse a cabo solo de forma limitada y selectiva" (OEA, 2015:8a).

Esta exigencia de propocionalidad de la medida restrictiva se vincula estrechamente con la idea de su adecuación. En otras palabras, la medida debe servir para el propósito que la justifica. Esto es relevante en relación con el uso de tecnologías de rastreo de contactos para la contención del COVID-19, pues su utilidad y/o eficacia aún es objeto de debate entre los expertos.

---

[32] "Muchas de las tecnologías que se están utilizando no solo permiten el análisis objetivo de datos y tendencias, sino que inescindiblemente permiten la identificación de los usuarios que conforman la masa crítica analizada. Los Estados deben procurar que se utilice tanto en el ámbito público como en el privado la tecnología adecuada para utilizar los datos masivos garantizando la protección debida a los derechos humanos en internet (CIDH, 2017:91).

[33] En esta materia, el Relator de Naciones Unidas señaló en su informe de 2013 que proteger la seguridad nacional y perseguir la actividad delictiva "podrían justificar el uso excepcional de tecnologías de vigilancia de las comunicaciones" pero identificó que "las leyes nacionales que reglamentan qué constituiría la participación necesaria, legítima y proporcional del Estado en la vigilancia de las comunicaciones suelen ser insuficientes o inexistentes" (AGNU, 2013:3).

1.3. Privacidad y control de la pandemia COVID-19.

Como se desprende de lo señalado en el apartado anterior, bajo determinadas circunstancias, la privacidad puede ser intervenida. Es más, el derecho a la vida privada es parte del catálogo de derechos que, bajo circunstancias excepcionales que sean oficialmente proclamadas (estados de excepción constitucional), pueden ser suspendidos (art. 4 PIDCP y art. 27 CADH). Ahora bien, esta suspensión de garantías queda siempre sujeta al principio de proporcionalidad y de mínima intervención (Ferrer y Herrera, 2017) y, conforme al derecho internacional de los derechos humanos, debería ser legal, necesaria y proporcional (HRW, 2020).

En este sentido, la Relatoría sobre la Libertad de Expresión de Naciones Unidas ha reconocido que la expansión del COVID-19 exigirá el uso de herramientas de vigilancia, y que la presión para que se expanda su utilización será cada vez mayor, de manera de rastrear a quienes han tenido contacto con personas contagiadas. Al respecto ha señalado que la recopilación de datos personales con esta finalidad debe hacerse resguardando la protección de los datos personales, por un tiempo limitado e informando a la población de los resultados. En este sentido, señaló que debe hacerse "lo que sea necesario para rastrear el avance de la enfermedad, pero únicamente lo que sea necesario" (AGNU, 2020:21). En el mismo sentido, el Programa Conjunto de las Naciones Unidas sobre el VIH/sida ha recordado que las restricciones que se adopten para proteger la salud pública deben ser de duración limitada, proporcionadas, necesarias, basadas en evidencia y recurribles ante tribunales (UNAIDS, 2020).

Por otra parte, la Relatoría de Naciones Unidas sintetizó los principios internacionales de derechos humanos aplicables a las tecnologías de vigilancia durante la pandemia, los que se reproducen íntegramente a continuación:

> a) Toda autorización de vigilancia debe estar contenida en leyes precisas y públicamente accesibles y ha de aplicarse únicamente cuando sea necesario y de manera proporcionada para lograr un objetivo legítimo (como la protección de la salud pública);
> b) La autorización para vigilar a personas concretas debe basarse en una evaluación independiente, de preferencia por una autoridad judicial, con las limitaciones procedentes en cuanto a su duración, forma, lugar y alcance;
> c) Debería exigirse el mantenimiento riguroso de registros para que las personas y los órganos de supervisión puedan determinar que la vigilancia se llevó a cabo con fines legítimos de salud pública;
> 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. (AGNU, 2020:19)

2. La protección supranacional de la Unión Europea.

El 8 de abril de 2020, la Comisión Europea adoptó una Recomendación destinada a los países de la UE sobre el uso de la tecnología y los datos en el abordaje de la crisis de COVID-19.[34] Esta responde a los llamados para la adopción de un enfoque común de la UE para el uso de aplicaciones móviles en este contexto, que considere tanto la eficacia de la tecnología utilizada, como su respeto de la privacidad individual y la seguridad de los datos, para, de esta forma, evitar la vigilancia y la estigmatización (Cooper y Lynn, 2020). La Recomendación señaló que cualquier aplicación deba:

- 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, este finalice de manera efectiva y los datos personales se destruyan irreversiblemente.

La Comisión complementó la Recomendación con una Comunicación[35] que constituye una guía sobre las aplicaciones COVID-19 y la publicación de un conjunto de instrumentos/herramientas (*Toolbox*) común de la UE para los Estados miembros, elaborada por la Red de Salud en línea (*eHealth Network*) de la UE en conjunto con la Comisión (eHealth Network, 2020). Además, el Comité Europeo de Protección de Datos (*European Data Protection Board, EDPB*) contribuyó a la Comunicación por medio de una Carta de respuesta a la primera, dirigida a la Comisión (EDPB, 2020).

Cada uno de estos instrumentos fue especificando, cada vez más, los tres lineamientos establecidos originalmente por la Recomendación[36]. Así, el último de ellos, la Carta del Comité Europeo de Protección de Datos, especificó las características y recomendaciones que las aplicaciones deben incluir para garantizar el cumplimiento del Reglamento General de Protección de Datos[37] y la Directiva sobre la privacidad y las comunicaciones electrónicas[38], los que se presentan en la Figura 7.

---

[34] Recomendación de la Comisión relativa a un conjunto de instrumentos comunes de la UE para la utilización de la tecnología y los datos para combatir y superar la crisis del COVID-19, en particular por lo que respecta a las aplicaciones móviles y a la utilización de datos de movilidad anonimizados. Recomendación C(2020) 3300 final de 8 de abril de 2020.

[35] Comunicación de la Comisión orientaciones sobre las aplicaciones móviles de apoyo a la lucha contra la pandemia de covid-19 en lo referente a la protección de datos (2020/C 124 I/01).

[36] Para conocer qué aspecto agregó cada organismo se requiere revisar los documentos citados en el párrafo anterior siguiendo su orden de elaboración. Sin embargo, para conocer en detalle las medidas recomendadas por la UE en torno a las aplicaciones con rastreo de contactos, es recomendable centrarse en el último de dichos documentos, la Carta del Comité Europeo de Protección de Datos enviada a la Comisión Europea en respuesta a la Guía de la Comisión.

[37] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos).

[38] Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas

Figura 7. Recomendaciones europeas para las aplicaciones con rastreo de contactos.

Ámbito	Recomendaciones
Identificación de usuarios	La aplicación no debe identificar a la persona infectada ni permitir la reidentificación de ninguna otra persona, ya sea infectada por COVID-19 o no.
Tasa de penetración del usuario	Lograr una tasa de penetración significativa del usuario es fundamental para la eficacia de las aplicaciones, y cualquier heterogeneidad funcional o diferencia en la forma de uso puede crear externalidades negativas.
Voluntariedad	Las aplicaciones deben adoptarse de forma voluntaria. Promocionar adecuadamente el uso de las aplicaciones puede ayudar a evitar una adopción dispersa.
Base legal para consentimiento	Cuando la aplicación se adopta en base a un mandato asignado por ley y en línea con los requisitos establecidos legalmente, la base legal más relevante para el procesamiento del consentimiento es la necesidad de realizar una tarea de interés público.
Seguimiento de ubicación	Las aplicaciones de rastreo de contactos no requieren seguimiento de ubicación, y debido a que hay métodos menos intrusivos de seguimiento de contactos disponibles, su inclusión puede violar el principio de minimización de datos. También existen riesgos relacionados con la seguridad y la privacidad.
Papel de las autoridades sanitarias	Las autoridades sanitarias y la comunidad científica deberían desempeñar un papel en la definición de lo que constituye un 'contacto' (es decir, el encuentro físico con personas infectadas) y respecto de los requisitos funcionales relacionados a las aplicaciones.
Almacenamiento de datos	Si bien el almacenamiento local de datos en los dispositivos individuales y el almacenamiento centralizado (por ejemplo, por una autoridad de salud) pueden cumplir con la ley de protección de datos, el Comité Europeo de Protección de Datos opina que la solución descentralizada está más en línea con el principio de minimización de datos.
Mecanismo de advertencia	Los mecanismos de advertencia solo deben involucrar el procesamiento de seudónimos aleatorios. Además, para evitar que los errores entreguen falsas advertencias, los mecanismos deben garantizar que la información sanitaria ingresada (COVID-positivo) sea correcta.
Positivos falsos	Los algoritmos utilizados en las aplicaciones de rastreo de contactos deben funcionar bajo la estricta supervisión de personal calificado, con el objetivo de limitar la aparición de falsos positivos y negativos.
Aportación humana	El asesoramiento sobre los pasos sanitarios a seguir no debe ser totalmente automatizado, sino que debe prever la interacción humana.

Fuente: European Data Protection Board, EDPB.

3. Incorporación de las aplicaciones a normativas nacionales: Australia y Colombia.

A raíz del COVID-19, durante el primer semestre del presente año y con el fin de permitir el uso de aplicaciones de rastreo de contactos a la luz de las legislación nacionales sobre protección de datos personales, algunos países han dictado nuevas normativas al efecto.

3.1. Australia.

A modo de ejemplo, la reforma a la normativa australiana de protección de datos personales se realizó en un cortísimo plazo, con una actividad legislativa de 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 original que autorizó la recopilación de datos personales por razón de salud pública en el contexto de la emergencia por el COVID-19, e introdujo medidas adicionales para reforzar la protección de la privacidad (Explanatory Memorandum, 2020:2).[39]

Entre las principales modificaciones está la creación de nuevos tipos penales por uso no autorizado de los datos personales recopilados por dicha aplicación; cargar los datos sin consentimiento; retener o divulgar los datos cargados fuera de Australia; 'desencriptar' (*unencrypt*) los datos cifrados de la aplicación COVIDSafe; 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 deba entregar, en el plazo 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, casi a un mes de su lanzamiento, COVIDSafe apenas había sido utilizada, "pasando de vital a irrelevante" (The Guardian, 2020).

3.2. Colombia.

Otro caso de modificación normativa se llevó a cabo en Colombia, aunque de manera diferente a la reforma australiana. En Colombia, la modificación normativa fue causada por el uso de CoronApp-Colombia, la aplicación móvil del Gobierno nacional de Colombia lanzada el 7 de marzo de 2020 (Ministerio de Salud y Protección Social, 2020). Según el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), el tratamiento de los datos personales y el análisis de la información recopilada por dicha aplicación se realizaría de forma completamente anónima, en cumplimiento con la Ley de Habeas Data, esta es, la Ley 1581 de 2012 sobre protección de datos personales (MinTIC,

[39] Biosecurity (Human Biosecurity Emergency) (Human Coronavirus with Pandemic Potential) (Emergency Requirements—Public Health Contact Information) Determination 2020.

2020). Como una excepción al tratamiento anónimo de los datos, el documento de Términos y Condiciones de uso de CoronApp Colombia, del Instituto Nacional de Salud, señala que:

> Excepcionalmente se tratará la información de forma no anonimizada cuando es rigurosamente necesario conocer la identidad del titular del dato y conforme a lo dispuesto en la Ley 1581 de 2012 y sus decretos reglamentarios.

Asimismo, en su Política de tratamiento de información, el Instituto Nacional de Salud afirmó -respecto de los datos entregados voluntariamente- que no sería necesario solicitar el consentimiento del titular de los datos, por cuanto el artículo 10 de la Ley 1581 de 2012 así lo permite cuando se trata de: "a) Información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial;" y en "c) Casos de urgencia médica o sanitaria;". Pero, señala el artículo, quien acceda a los datos personales debe igualmente cumplir con las disposiciones de dicha ley.

La Fundación Karisma y su laboratorio de seguridad digital K+Lab declararon que los términos y condiciones serían insuficientes, por cuanto "no se ofrece información sobre la forma como gestiona de manera segura y respetuosa la privacidad de los datos, no explica cómo es la temporalidad de su naturaleza, ni lo que sucederá con los datos al finalizar esta emergencia". Asimismo, se harían "referencias generales a que cumplen la ley, que toman medidas seguras o indican que la información de salud quedará alojada en una infraestructura dedicada" (Fundación Karisma, 2020).

Transcurridos casi dos meses desde el lanzamiento de la aplicación, el 30 de abril se reformó el Decreto 1078 de 2015 del Sector de Tecnologías de la Información y las Comunicaciones.[40] Se le incorporó un nuevo título que señala que los canales oficiales de reporte de información durante la emergencia sanitaria serán CoronApp Colombia, la aplicación tecnológica oficial en el territorio nacional (art. 2.2.18.2.), y la línea oficial de atención telefónica 192 (art. 2.2.18.3.). Asimismo, como ya hacía previamente, reiteró que tales medidas "se aplicarán bajo la plena observancia de la normativa que rige la protección de datos personales, contenida en la Ley Estatutaria 1581 de 2012 y sus normas reglamentarias" (art. 2.2.18.4.). Sin embargo, dicho decreto no se refirió a los aspectos planteados por la Fundación Karisma antes citados.

Por tanto, a diferencia del caso australiano, en Colombia no hubo reforma alguna a la normativa sobre privacidad de datos, elevándose la respectiva aplicación de rastreo de contactos a herramienta de carácter permanente.

[40] Decreto 614 de 2020 (Abril 30) Por el cual se adiciona el título 18 a la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, para establecer los canales oficiales de reporte de información durante las emergencias sanitarias.

III. Protección de los datos personales en Chile y la nueva aplicación CoronApp.

1. La aplicación oficial chilena.

El pasado 16 de marzo fue lanzada la primera versión de la aplicación nacional CoronApp (Chile). Como se verá, es escasa la información oficial respecto de esta aplicación, por lo que, en lo que sigue, se le analizará considerando los tres documentos públicos disponibles: los Términos y Condiciones[41] y las Políticas de Privacidad[42] de la propia aplicación, ambos publicados en su sitio web, y una nota informativa de la Agencia de Gobierno Digital, entidad desarrolladora de la aplicación, que describe sus funciones generales (División de Gobierno Digital, 2020)

Los objetivos declarados de CoronApp (Chile) son: i) permitir a los usuarios reportar y controlar sus síntomas relacionados con el COVID-19, así como también, monitorear los síntomas de hasta 8 personas (familiares, convivientes u otros que no puedan acceder a la aplicación); ii) obtener información oficial sobre la pandemia, recibiendo notificaciones del Gobierno e información a través del WhatsApp informativo del MINSAL; iv) indagar el lugar donde una persona residirá durante la cuarentena; y v) colaborar con la prevención de contagios, informando sobre situaciones que pongan en riesgo a más personas (CoronApp (Chile), página de inicio).

Al utilizar las mismas categorías con las que se analizaron las aplicaciones extranjeras, se tiene que el órgano desarrollador de CoronApp (Chile) es una entidad pública: la División de Gobierno Digital de la Secretaria General de la Presidencia. Sin embargo, no se establece el órgano responsable de administrar los datos recopilados. Al respecto, como se verá, un Oficio del Consejo para la Transparencia solicitó identificar al órgano responsable de los datos.

Respecto a la tecnología base utilizada, tampoco hay información concluyente, sino solo parcial. Por un lado, se informa que CoronApp (Chile) adoptó el protocolo Google-Apple, el cual utiliza Bluetooth como tecnología base. Sin embargo, sus Términos y Condiciones señalan que “algunas funciones de los Servicios hacen uso de información detallada de ubicación, por ejemplo, en forma de señales GPS”. De modo que, al igual que en el caso de Noruega, la aplicación CoronApp (Chile) utilizaría un híbrido Bluetooth-GPS como tecnología base. Lo anterior, no obstante, constituye solo una hipótesis debido a la falta de información oficial al respecto.

Con relación al sistema de almacenamiento de datos de CoronApp (Chile), la Política de Privacidad (numeral 5) señala que "la información registrada en la aplicación será almacenada y replicada en una nube privada bajo la completa administración del MINSAL [...]". Por tanto, podría tratarse de un sistema de almacenamiento de datos centralizado, al igual que la mayoría de las aplicaciones analizadas (7 de 13), o, considerando que también utiliza Bluetooth, podría tratarse de un sistema de almacenamiento "híbrido-centralizado", como el caso australiano. Estas son, nuevamente, sólo hipótesis.

[41] Disponible en: https://coronapp.gob.cl/terminos.html (mayo, 2020)
[42] Disponible en: https://coronapp.gob.cl/politicas.html (mayo, 2020)

Ahora, respecto a la cantidad de tipos de datos que CoronApp (Chile) solicita a sus usuarios, las Políticas de Privacidad especifican que la aplicación solicita y almacena 10 tipos de datos a sus usuarios[43]. Al compararlo con las 13 aplicaciones analizadas previamente en términos de la cantidad de datos solicitados a sus usuarios, CoronApp (Chile) se sitúa solo bajo CoronApp Colombia (que solicita 12 tipos de datos) y por sobre del resto de las otras 12 aplicaciones revisadas.

Finalmente, respecto a si CoronApp (Chile) elimina o no los datos de sus usuarios y, de hacerlo, cuánto tiempo se toma, el numeral 5 de las Políticas de Privacidad de CoronApp (Chile) señala que:

> Los datos serán almacenados y tratados durante el tiempo que sea necesario para la protección de la salud pública, en el contexto de la emergencia sanitaria. Para fines históricos, estadísticos, científicos y de estudios o investigaciones, se podrán almacenar y utilizar los datos por un período de 15 años, con las debidas medidas de seguridad y garantías de anonimización (CoronApp Chile, Politicas de Privacidad, numeral 5).

De esta forma, comparada con las aplicaciones extranjeras analizadas, CoronApp (Chile) se sitúa entre las aplicaciones que declara que podrá eliminar los datos de sus usuarios, aunque en un periodo tiempo extenso (hasta 15 años). Le siguen, la aplicación israelí (hasta 7 años) y la española (hasta 2 años), en tanto las restantes se toman 30 días o menos.

2. Normativa aplicable a los datos personales.

En forma resumida, se puede señalar que la legislación que regula desde 1999 la protección y tratamiento de los datos personales es la Ley N° 19.628 sobre Protección de la Vida Privada.

En la definición de su artículo 2°, letra f), establece que son datos personales "los relativos a cualquier información concerniente a personas naturales, identificadas o identificables." Luego, en la letra g) del mismo artículo, dispone que son datos sensibles, "aquellos datos personales que se refieren a las características físicas o morales de las personas o a hechos o circunstancias de su vida privada o intimidad, tales como los hábitos personales, el origen racial, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual".

El tratamiento de los datos sensibles está regulado en forma particular en el artículo 10, que lo restringe en los siguientes términos:

> Artículo 10.- No pueden ser objeto de tratamiento los datos sensibles, salvo cuando la ley lo autorice, exista consentimiento del titular o sean datos necesarios para la determinación u otorgamiento de beneficios de salud que correspondan a sus titulares.

[43] Estos son: RUN o Pasaporte del usuario, correo electrónico, número telefónico, nombre y apellido, edad, comuna y ciudad de residencia, geolocalización, medicamentos que toma o han sido prescritos, preexistencia de enfermedades, datos de seguimiento de la enfermedad, tales como síntomas, contacto con personas contagiadas confirmadas y viaje a países de alto riesgo.

Además, de acuerdo al artículo 20:

> El tratamiento de datos personales por parte de un organismo público sólo podrá efectuarse respecto de las materias de su competencia y con sujeción a las reglas precedentes. En esas condiciones, no necesitará el consentimiento del titular[44].

En este mismo sentido, la Ley N° 20.584, que regula los derechos y deberes que tienen las personas en relación con acciones vinculadas a su atención de salud, "buscó garantizar el resguardo de la privacidad y confidencialidad de los datos, así como de las muestras de los pacientes y el reconocimiento de su autonomía, queriendo promover la participación activa en su proceso de atención en salud"[45].

A su vez, en relación a los datos sensibles de salud, el artículo 12 de la Ley N° 20.584 define la ficha clínica:

> Artículo 12.- La ficha clínica es el instrumento obligatorio en el que se registra el conjunto de antecedentes relativos a las diferentes áreas relacionadas con la salud de las personas, que tiene como finalidad la integración de la información necesaria en el proceso asistencial de cada paciente. Podrá configurarse de manera electrónica, en papel o en cualquier otro soporte, siempre que los registros sean completos y se asegure el oportuno acceso, conservación y confidencialidad de los datos, así como la autenticidad de su contenido y de los cambios efectuados en ella.
> *Toda la información* que surja, tanto *de la ficha clínica* como de los estudios y demás documentos donde se registren procedimientos y tratamientos a los que fueron sometidas las personas, será considerada como *dato sensible*, de conformidad con lo dispuesto en la letra g) del artículo 2º de la ley Nº 19.628[46].

Finalmente, el año 2018, se elevó a nivel constitucional el derecho a tal protección, mediante la modificación del artículo 19 Nº 4 de nuestra carta magna[47], como parte del catálogo de derechos fundamentales:

> Artículo 19.- La Constitución asegura a todas las personas:
> 4º.- El respeto y protección a la vida privada y a la honra de la persona y su familia, y asimismo, la protección de sus datos personales. El tratamiento y protección de estos datos se efectuará en la forma y condiciones que determine la ley;

3. Prevenciones y recomendaciones del Consejo para la Transparencia.

En el contexto del COVID-19, el Consejo para la Transparencia, a través del Oficio N° 675, del 7 de mayo del 2020, formuló "algunas prevenciones tendientes a garantizar que las operaciones de tratamientos de datos asociados al funcionamiento de la aplicación CoronApp cumplan estrictamente

---

[44] Énfasis añadido.
[45] Boletín N° 13.452-11.
[46] Énfasis añadido.
[47] Por Ley N° 21.096, Art. único. D.O. 16.06.2018.

con lo dispuesto en el artículo 19 N° 4 de la Constitución Política de la República y las normas pertenecientes a la Ley 19.628, sobre Protección de la Vida Privada" (Consejo para la Transparencia, 2020, n□4).

En el mencionado Oficio, el Consejo para la Transparencia hizo prevenciones respecto a diversas características de la aplicación, entre las que se cuentan:

- **Cantidad de datos que almacena**. El Consejo identificó datos sensibles de salud y datos sensibles relativos a hábitos personales (georreferenciación), por lo que, según dicha entidad, correspondería "evaluar si la recopilación de cada uno de los datos solicitados puede resultar excesiva y desproporcionada de cara al cumplimiento de los fines lícitos que justificarían su procesamiento" (Consejo..., a), iii), al tiempo que recomendó especificar los fines o motivos que persigue el tratamiento de los datos almacenados (Consejo..., a), iv).

- **Identificación del responsable del tratamiento de los datos.** Al respecto, el Consejo señaló que "se debe individualizar con claridad en la Política de Privacidad, en un apartado especial, el organismo público que reviste la calidad de responsable del tratamiento de los datos recopilados a través de la aplicación CoronApp" (Consejo..., b), ii).

- **Agregar otros usuarios dependientes**. Según el numeral 2 de la Política de Privacidad de la aplicación, "los usuarios podrán agregar otros usuarios dependientes, familiares o quienes no tengan acceso a un dispositivo móvil", ante lo cual el Consejo señaló que "no se advierte cómo los usuarios dependientes, quienes no tienen una relación directa con la aplicación, podrán ejercer efectivamente ante el responsable del tratamiento los derechos reconocidos por la Ley 19.628, sobre Protección de la Vida Privada" (Consejo..., e), iv).

- **Almacenamiento de datos**. Respecto a las Políticas de Privacidad de CoronApp (Chile) que permiten almacenar datos, para ciertos fines, hasta por 15 años, el Consejo señala que “debe evaluarse la necesidad de establecer periodos extensos de conservación de los datos, teniendo especialmente presentes los riesgos que trae aparejado el procesamiento de datos sensibles, así como las finalidades extraordinarias que motivaron su recopilación y comunicación” (Consejo…, f), iii)

- **Seguridad de la información**. El numeral 5 de las Políticas de Privacidad señala que la información procesada en la aplicación será “almacenada y replicada en una nube privada bajo la completa administración del MINSAL, en *Amazon Web Services* (AWS) correspondiente a la región ‘*us-east region*’ el cual se encuentra físicamente en Estados Unidos de América en el estado de Virginia”. Al respecto, el Consejo afirmó que “se deben tener presente los riesgos de seguridad que pueden derivarse del hecho que los datos recabados y procesados por CoronApp no sean almacenados en servidores locales propios del MINSAL, sino que en servidores externos, localizados fuera del territorio nacional […]” (Consejo…, f), vi).

4. Proyectos de ley en tramitación.

Previo a la emergencia sanitaria actual, la actualización de la regulación de la vida privada y la protección de datos personales había motivado el ingreso a tramitación de decenas de proyectos de ley en el Congreso Nacional .

Específicamente, durante el periodo entre el 1° de enero y el 25 de mayo de 2020, han sido presentados nuevos proyectos de ley, con diferentes objetivos:

- **Ampliar las excepciones del artículo 10 de la Ley N° 19.628 (autorización por ley, consentimiento del titular, determinación u otorgamiento de beneficios de salud) a casos de pandemias, catástrofes y calamidad pública (Boletín Nº 13.374-07).**

  Presentado por las senadoras Carolina Goic y Ximena Rincón, y los senadores Francisco Chahuán, Guido Girardi y Rabindranath Quinteros. Ingresado el martes 31 de marzo de 2020, actualmente en primer trámite constitucional.

  El PL pretende ampliar los casos de excepción de tratamiento de los datos sensibles, pero limitándola exclusivamente al tiempo que dure la respectiva emergencia.

- **Autorizar el tratamiento de datos sensibles a las autoridades, en el ámbito de la Ley N° 20.584, sobre derechos y deberes del paciente**.

  – El Boletín N° 13.452-11 fue presentado por los senadores Guido Girardi, Carolina Goic, Manuel José Ossandón, Jaime Quintana y David Sandoval. Ingresado el martes 21 de abril de 2020, actualmente en primer trámite constitucional.

    El PL pretende permitir a los alcaldes acceder transitoriamente a la ficha clínica de los pacientes. Se especifica que para el conocimiento de la ficha y la adopción de medidas, el alcalde deba contar con el consentimiento explícito de quien padece COVID-19. El tratamiento de los datos personales por parte del Municipio solo puede hacerse con la finalidades específicas que se establecen, queda sujeto a la Ley N° 19.628, sobre Protección a la Vida Privada, y considera al Alcalde como el responsable del tratamiento de los datos, quien debe responder por los daños y perjuicios provocados a un titular por la pérdida, mal uso y cesión ilícita de los datos de salud contenidos en la ficha clínica.

  – El Boletín N° 13.350-11 fue presentado por la diputada Maya Fernández y los diputados Gabriel Silber, Víctor Torres y Matías Walker. Ingresado el lunes 23 de marzo de 2020, actualmente en primer trámite constitucional.

    El PL, al igual que el anterior, pretende autorizar de manera expresa la transferencia de información entre las autoridades que necesariamente deban conocer de la población afectada de una pandemia o epidemia. Tal autorización solo podrá otorgarse entre el Ministerio de Salud, los Servicios de Salud, las SEREMI de Salud, las Fuerzas de Orden

y Seguridad, y en caso de decretarse un Estado de Excepción Constitucional, las Fuerzas Armadas. El tratamiento también queda sujeto a la Ley N° 19.628 y requiere el paciente deberá ser debidamente informado respecto la finalidad y condiciones del tratamiento de sus datos sensibles.

- **Establecer reglas especiales para el tratamiento de datos personales sensibles de salud, en caso de declaración de una cuarentena sanitaria o un estado de excepción constitucional por calamidad pública**.

  Presentado por el senador Felipe Harboe (Boletín N° 13.497-07). Ingresado el miércoles 13 de mayo de 2020, actualmente en primer trámite constitucional.

  El PL señala que declarada una cuarentena sanitaria o un estado de excepción constitucional por calamidad pública que signifique grave riesgo para la salud o vida de las personas, el tratamiento de datos personales sensibles de salud, incluidos el perfil biológico, datos genéticos, protéomicos o metabólicos y datos biométricos, está sujeto a: la necesidad de consentimiento del titular, salvo se trate de una urgencia sanitaria, para salvaguardar la salud del titular o un tercero, o si el titular no puede otorgar su consentimiento; limitado por la finalidad sanitaria; deber del responsable de garantizar estándares adecuados de seguridad; sanción por mal uso de los datos (multa); responsabilidad de la autoridad sanitaria en las transferencia internacionales de datos sensibles de salud en el marco de la protección o cooperación sanitaria internacional para el combate de la pandemia del covid-19; y posibilidad para los titulares de los datos sensibles de salud de ejercer los derechos del Título II de la Ley Nº 19.628.

Como se observa, ninguno de los anteriores se refiere en forma especial a la aplicación CoronApp (Chile) en forma particular, ni dicen relación con las observaciones y sugerencias realizadas por el Consejo para la Transparencia, en su caso.

Consideraciones finales

El análisis realizado recayó en la manera en que ciertas tecnologías pueden acoplarse a determinadas exigencias normativas y sociales. En términos concretos, lo anterior 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 a las agencias protección de datos personales europeas, aunque no suficiente para lograr que una aplicación de rastreo de contactos tenga éxito en su implementación.

Para cuantificar efectivamente la extensión de posibles contagios y evolución del COVID-19, este tipo de aplicaciones requiere, para ser efectiva, que una porción significativa de la población la utilice. Es decir, no se trata de que por un carril vaya la ‘efectividad técnica’ de la aplicación, y por otro carril independiente, 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, ésta simplemente no puede cumplir de manera efectiva su función sanitaria en relación al 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 que entregue una base de legitimidad social a una aplicación que busca enfrentar la pandemia actual, en particular cuando el uso obligatorio de las aplicaciones sea indeseable y/o impracticable. Además, para la efectividad de la aplicación, se requiere la implementación de otras medidas, entre las que se cuentan una promoción extensiva de la misma, estrategias de inclusión de grupos de población en desventaja digital, además de los aspectos logísticos necesarios para su funcionamiento.

Por último, el cumplimiento de la normativa nacional e internacional de DDHH aplicable en Chile en materia de protección de datos constituye parte del marco normativo aplicable a la implementación de este tipo de herramientas. La construcción de políticas de privacidad detalladas y transparentes para el manejo de los datos recopilados por parte de las autoridades responsables, podría ayudar a generar confianza de la ciudadanía respecto a la aplicación. Esto, sumado a otras medidas, podría terminar en una aplicación legitimada mayoritariamente por la población, lo que, a su vez, constituye un requisito esencial para que la aplicación logre un funcionamiento sanitario efectivo en relación al COVID-19.

Referencias y bibliografía

AGNU. 2013. Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y expresión, Frank La Rue. A /HRC/23/40. Disponible en: http://bcn.cl/2e3pz (mayo, 2020).

-- 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 (mayo, 2020).

Apple/Google, 2020. Exposure Notification Frequently Asked Questions. Disponible en: http://bcn.cl/2e57a (mayo, 2020).

Australian Government. 2020. Nueva herramienta para reducir la propagación del COVID-19. Disponible en: http://bcn.cl/2e579 (mayo, 2020).

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

BBC. 2020b. Coronavirus: Security flaws found in NHS contact-tracing app. May 19, 2020. Disponible en: https://www.bbc.com/news/technology-52725810 (mayo, 2020).

Consejo para la Transparencia. 2020. Oficio 675 del 7 de mayo del 2020. Disponible en: https://cutt.ly/pySamZ6 (mayo, 2020).

CCPR. 1988. Observación general Nº 16. Derecho a la intimidad (artículo 17). Disponible en: http://bcn.cl/2e3ay (mayo, 2019).

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 (mayo, 2020).

CtIDH. 2001. Caso de la Comunidad Mayagna (Sumo) Awas Tingni Vs. Nicaragua. Sentencia de 31 de agosto de 2001 (Fondo, Reparaciones y Costas). Disponible en: http://bcn.cl/2e1m3 (mayo, 2020).

Cypers, Bennet y Gennie Gebhart. (2020). Apple and Google's COVID-19 Exposure Notification API: Questions and Answers. 28/04/2020. Disponible en: http://bcn.cl/2e662 (mayo, 2020).

División de Gobierno Digital, 2020. CoronApp: La nueva aplicación de Chile para combatir la pandemia. Disponible en: https://cutt.ly/hyDvae9 (mayo, 2020)

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 (mayo, 2020).

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 (mayo, 2020).

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

European GNSS Supervisory Authority (GSA), 2020. GNSS for Crisis. Disponible en: https://www.gsa.europa.eu/GNSS4Crisis (mayo, 2020).

Ferrer, Eduardo y Alfonso Herrea. 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.

-- 2020b. El COVID-19 plantea un "reto colosal para el liderazgo" que exige una actuación coordinada, declara la Alta Comisionada ante el Consejo de Derechos Humanos. La pandemia del COVID-19 – Informe oficioso al Consejo de Derechos Humanos. Discurso de Michelle Bachelet, Alta Comisionada de las Naciones Unidas para los Derechos Humanos. 09/04/2020. Disponible en: http://bcn.cl/2e0ry (mayo, 2020).

Government of Singapore. 2020. TraceTogether. Disponible en: http://bcn.cl/2e577 (mayo, 2020).

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

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

Huang, Yasheng; Meicen Sun y Yuze Sui. How Digital Contact Tracing Slowed Covid-19 in East Asia. 2020. Harvard Business Review. April 15, 2020. Disponible en: http://bcn.cl/2e573 (mayo, 2020).

Instituto Nacional de Salud (INS). 2020. Política de tratamiento de información (PTI) relacionada con la Coronapp Colombia. Versión 08/05/2020. Disponible en: http://bcn.cl/2e572 (mayo, 2020).

-- s/f. Términos y Condiciones CoronApp Colombia. Disponible en: http://bcn.cl/2e570 (mayo, 2020).

Joinup. 2020. Digital Response to COVID-19. Disponible en: http://bcn.cl/2e56z (mayo, 2020).

KU Leuven, 2020a. Contact Tracing Joint Statement. Disponible en: http://bcn.cl/2e56y (mayo, 2020).

-- 2020b. COSIC participates in DP-3T (Decentralized Privacy-Preserving Proximity Tracing). Disponible en: http://bcn.cl/2e56x (mayo, 2020).

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

Ministerio de Salud y Protección Social. 2020. CoronApp - Colombia, la aplicación para que conocer la evolución del coronavirus en el país. Disponible en: http://bcn.cl/2e56u (mayo, 2020).

Ministerio de Tecnologías de la Información y las Comunicaciones, MinTIC. 2020. Abecé/ Todo lo que debe saber sobre CoronApp-Colombia y su funcionamiento. 14 abril, 2020. Disponible en: http://bcn.cl/2e56u (mayo, 2020).

Meckelburg, Hans-Juergen. 2020. Contact Tracing Coronavirus COVID-19 -Calibration Method and Proximity Accuracy. Disponible en: https://cutt.ly/FyDQTPs (mayo, 2020).

OACNUDH, 2020a. Coronavirus: La respuesta debe basarse íntegramente en los derechos humanos, afirma Bachelet [nota de prensa].06/03/2020. Disponible en: http://bcn.cl/2e0ba (mayo, 2020).

OEA. 2015. Declaración conjunta sobre libertad de expresión y las respuestas a las situaciones de conflicto. Disponible en: http://bcn.cl/2e3dn (mayo, 2020).

OHCHR. 2020a. COVID-19: States should not abuse emergency measures to suppress human rights - UN experts [nota de prensa]. 16/03/2020. Disponible en: http://bcn.cl/2e0bj (mayo, 2020).

-- 2020b. Statement by the UN expert on the right to health on the protection of people who use drugs during the COVID-19 pandemic. Disponible en: http://bcn.cl/2e165 (mayo, 2020).

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 (mayo, 2020).

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

Pascual, Francisco. 2014. Consenso e interpretación evolutiva de los tratados regionales de derechos humanos. Revista Española de Derechos Internacional, 66(2):113-153.

Pauta. 2020. Hecho en La Moneda: el Gobierno afina el lanzamiento de su app Covid-19. Disponible en: https://cutt.ly/iyAw1WL (mayo, 2020).

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

UNAIDS. 2020. Rights in the time of COVID-19. Lessons from HIV for an effective, community-led response. Disponible en: http://bcn.cl/2e56p (mayo, 2020).

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

Normativa

Unión Europea:

– Comunicación de la Comisión orientaciones sobre las aplicaciones móviles de apoyo a la lucha contra la pandemia de covid-19 en lo referente a la protección de datos (2020/C 124 I/01). Disponible en: http://bcn.cl/2e592 (mayo, 2020).
– Recomendación de la Comisión relativa a un conjunto de instrumentos comunes de la Unión para la utilización de la tecnología y los datos a fin de combatir y superar la crisis de la COVID-19, en particular por lo que respecta a las aplicaciones móviles y a la utilización de datos de movilidad anonimizados. Recomendación C(2020) 3300 final de 8 de abril de 2020. Disponible en: http://bcn.cl/2e593 (mayo, 2020).
– Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos). Disponible en: http://bcn.cl/2e594 (mayo, 2020).
– Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las

comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas). Disponible en: http://bcn.cl/2e595 (mayo, 2020).

Australia:

– Privacy Amendment (Public Health Contact Information) Act 2020, No. 44, 2020. Disponible en: https://www.legislation.gov.au/Details/C2020A00044 (mayo, 2020).
– Privacy Amendment (Public Health Contact Information) Bill 2020. Disponible en: http://bcn.cl/2e58d (mayo, 2020).
– Privacy Amendment (Public Health Contact Information) Bill 2020. Explanatory Memorandum, 2019. Disponible en: http://bcn.cl/2e58f (mayo, 2020).

Chile:

– Constitución Política de la República. Disponible en: http://bcn.cl/24nex (mayo, 2020).
– Ley N° 19.628 sobre protección de la vida privada. Disponible en: http://bcn.cl/25zma (mayo, 2020).
– Ley N° 20.584 que regula los derechos y deberes que tienen las personas en relación con acciones vinculadas a su atención en salud (ley de derechos y deberes de los pacientes). Disponible en: http://bcn.cl/25b3z (mayo, 2020).

Proyectos de ley:

– Proyecto de ley que autoriza efectuar tratamiento de datos sensibles en los casos que indica. Boletín Nº 13.374-07. Disponible en: http://bcn.cl/2e57x (mayo, 2020).
– Proyecto de ley que modifica la ley N° 20.584, sobre derechos y deberes del paciente, para autorizar el tratamiento de datos para el control de pandemia derivada del Covid-19. Boletín N° 13.452-11. Disponible en: http://bcn.cl/2e580 (mayo, 2020).
– Proyecto de ley que modifica la ley N°20.584 que regula los derechos y deberes que tienen las personas en relación con acciones vinculadas a su atención en salud, para permitir el tratamiento de datos sensibles, en casos de epidemias o pandemias, para desarrollar control sanitario, y en las condiciones que indica. Boletín N° 13.350-11. Disponible en: http://bcn.cl/2e581 (mayo, 2020).
– Proyecto de ley que refuerza la protección de los datos sensibles de salud, durante cuarentena sanitaria o estado de excepción de catástrofe declarada por la autoridad. Boletín N° 13.497-07. Disponible en: http://bcn.cl/2e583 (mayo, 2020).

Colombia:

– Ley 1581 de 2012 (Octubre 17) Por la cual se dictan disposiciones generales para la protección de datos personales. Disponible en: http://bcn.cl/2e58g (mayo, 2020).
– Decreto 614 de 2020 (Abril 30) Por el cual se adiciona el título 18 a la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, para establecer los canales oficiales de reporte de información durante las emergencias sanitarias. Disponible en: http://bcn.cl/2e58h (mayo, 2020).
– Decreto 1078 de 2015 Sector de Tecnologías de la Información y las Comunicaciones. Disponible en: http://bcn.cl/2e58l (mayo, 2020).

ANEXO 1: Figura 8. Sistematización información de 13 aplicaciones, de acceso voluntario y con respaldo del respectivo gobierno.

País, aplicación desarrollada, link	Tecnología rastreo contactos / Sistema almacenamiento datos	Datos registrados por la app	Eliminación / tiempo de almacenamiento datos	Desarrollador de app / Administrador datos recopilados
 Australia COVIDSafe cutt.ly/vyO2Ao0	Bluetooth BLUE TRACE / Centralizado	Nombre, número de teléfono, código postal y rango de edad.	Si, 21 días (automático)	Departamento de Salud de Australia / Agencia de Transformación Digital
 Austria Stopp Corona cutt.ly/yyO2Uff	Bluetooth Google / Descentralizado	Número de teléfono.	Si, 30 días.	Cruz Roja austríaca
 Bulgaria ViruSafe virusafe.info/	GPS / Centralizado	Número de teléfono. Historial de ubicación.	No	ScaleFocus / Ministerio de salud y Grupo Nacional sobre Coronavirus
 Colombia CoronApp cutt.ly/OyO2GAO bit.ly/2WUflXz	Bluetooth / Centralizado	Nombre completo, tipo y nº documento, nº teléfono, sexo, fecha de nacimiento, país, departamento, ciudad residencia, e-mail, contraseña, origen étnico y reporte de salud	No. Datos se conservan hasta fin de pandemia, exepto lo que se requiera conservar para fines históricos, científicos o estadísticos.	Instituto Nacional de Salud y HypeLabs / Ministerio de Salud y Protección Social e Instituto Nacional de Salud
 España Asistencia COVID-19 cutt.ly/ayO2XHu	GPS / Centralizado	Nombre completo, nº celular, DNI / NIE, dirección y código postal, fecha de nacimiento, geolocalización, género (opc.) y reporte de salud.	No. Los datos se conservan durante la pandemia, con excepción de las finalidades estadísticas, investigación o interés público, por máximo 2 años	Ministerio de Asuntos Económicos y Transformación Digital y diversas empresas / Ministerio de Sanidad
 Islandia Rakning C-19 www.covid.is/app/en	GPS / Descentralizado	Número de teléfono. Historial de ubicación de los últimos 14 días	Si, 14 días (automático)	Oficina del Director de Salud Pública / Oficina del Director de Salud Pública
 Israel HaMagen cutt.ly/myO2NIm	GPS / Descentralizado	Historial de ubicación de los últimos 14 días (fechas, horas y lugares)	Si, 7 años. La información no utilizada para investigaciones epidemiológicas se eliminará en 30 días	Ministerio de salud, empresas y voluntarios / Ministerio de salud

Fuente: Elaboración propia. La fuente de la información es la que se cita en cada caso.

Figura 8. Sistematización información de 15 aplicaciones, de acceso voluntario y con respaldo del respectivo gobierno (Cont.).

País, aplicación y link	Tecnología rastreo contactos / Sistema almacenamiento datos	Datos registrados por la app	Eliminación / tiempo de almacenamiento datos	Desarrollador de app / Administrador datos recopilados
Macedonia StopKorona! cutt.ly/5yO37se	Bluetooth / Descentralizado	Número de teléfono	Si, pero debe hacerlo el usuario manualmente	NextSense y Ministerio sociedad de la información y administración / Ministerio de salud
Mexico CovidRadar covidradar.mx/	Bluetooth / Centralizado	No recolecta información de datos personales. Del dispositivo recolecta: sistema operativo y tipo, identificador del móvil, dirección IP, entre otros	No	LERTEK S.A. / Gobierno del Estado de Nuevo León
Noruega Smittestopp cutt.ly/gyO9Yaa	Bluetooth GPS / Centralizado	Número de teléfono, edad, posición GPS. Del dispositivo: sistema operativo, número, modelo y tamaño de pantalla, y operador de telefonía.	Si, 30 días (automático). También manualmente. Si se elimina app. datos se eliminan pasada una semana. Todos los datos personales se eliminarán al expirar normativa (1 de diciembre de 2020)	Instituto noruego de salud pública y Simula / Instituto noruego de salud pública
Polonia ProteGO Safe cutt.ly/WyO9M28	Bluetooth / Descentralizado	Nombre, datos de salud, sexo, edad, es fumador de cigarrillos y otros datos que el usuario elija ingresar a la funcionalidad health journal de la app, e identificador del dispositivo móvil.	Si, los datos personales se eliminan junto con la eliminación de la app (cuando deje de usar ProteGO)	Ministerio de asuntos digitales / Inspector sanitario jefe
República Checa eRouška erouska.cz/	Bluetooth / Descentralizado	Número de teléfono. Del dispositivo: modelo del teléfono y sistema operativo.	Si, 30 días (automático). Puede eliminarse manualmente. El nº lo mantiene Ministerio de Salud por 6 meses, o hasta que no sea necesario o hasta solicitud de cancelación, lo que ocurra primero.	Ministerio de salud y voluntarios de la plataforma COVID19CZ / Sin información
Singapur Tracetogether cutt.ly/OyO3LYy	Bluetooth BLUE TRACE / Centralizado	Número de teléfono. Si recolecta del dispositivo: marca, categoría, modelo, sistema operativo, entre otros.	Si, 21 días (automático)	Ministerio de salud y Agencia gubernamental de tecnología (GovTech) / Ministerio de Salud

Fuente: Elaboración propia. La fuente de la información es la que se cita en cada caso.

ANEXO 2: Descripción del protocolo Google-Apple *Privacy-Preserving Contact Tracing Project*

Según su propia descripción, este protocolo de rastreo de contactos digital está basado en una combinación de tecnología inalámbrica *Bluetooth Low Energy* (para la detección de proximidad de teléfonos inteligentes y para el intercambio de datos) y en criptografía que preserva la privacidad (Apple/Google, 2020:3).

En la primera fase del proyecto, una vez habilitados, los dispositivos móviles de los usuarios enviarán regularmente una señal ("baliza") a través de Bluetooth que incluye un identificador aleatorio (una cadena de números aleatorios que no están vinculados a la identidad de un usuario), la que cambia cada 10-20 minutos como protección adicional. Otros teléfonos estarán escuchando estas señales y transmitiendo las suyas también, las que al ser recibidas serán registradas y almacenadas en el dispositivo (Apple/Google, 2020: 3).

Al menos una vez al día, el sistema descargará una lista de las claves de las balizas que se han verificado como pertenecientes a personas confirmadas como positivas para COVID-19. Cada dispositivo verificará la lista de señales que ha registrado contra la lista descargada del servidor. Si hay una coincidencia entre las balizas almacenadas en el dispositivo y la lista de diagnóstico positivo, el usuario puede ser notificado y aconsejado sobre los pasos a seguir a continuación (Apple/Google, 2020: 3).

Para impulsar esta solución en la primera fase, ambas compañías lanzarán interfaces de programación de aplicaciones (API) que permitirán que las apps de rastreo de contactos de las autoridades de salud pública trabajen en dispositivos Android e iOS, al tiempo que mantienen la privacidad del usuario. Estas apps estarán disponibles para que los usuarios las descarguen a través de sus respectivas tiendas de aplicaciones [Apple Store y Google Play]. Una vez que se ingresa a la aplicación, el usuario deberá aceptar los términos y condiciones antes de que el programa esté activo. Las compañías planean hacer disponibles estas API en mayo (Apple/Google, 2020: 3).

En la segunda fase, disponible en los próximos meses, esta capacidad se introducirá en el nivel del sistema operativo para ayudar a garantizar una adopción amplia. Después de que se instale en la actualización del sistema operativo y el usuario haya aceptado, el sistema enviará y escuchará las balizas Bluetooth como en la primera fase, pero sin requerir que se instale una aplicación. Si se detecta una coincidencia, se notificará al usuario, y si el usuario aún no ha descargado una app oficial de la autoridad de salud pública, se le pedirá que la descargue y se le informará sobre los próximos pasos (Apple/Google, 2020: 3).

Solo las autoridades de salud pública tendrán acceso a esta tecnología y sus aplicaciones deben cumplir con criterios específicos de privacidad, seguridad y control de datos. Si en algún momento un usuario es diagnosticado positivamente con COVID-19, él o ella puede trabajar con la autoridad de salud para informar ese diagnóstico dentro de la aplicación, y con su consentimiento sus balizas se agregarán a la lista de diagnóstico positivo. La identidad del usuario no se compartirá con otros usuarios, Apple y Google como parte de este proceso (Apple/Google, 2020:3).

Disclaimer

Asesoría Técnica Parlamentaria, está enfocada en apoyar preferentemente el trabajo de las Comisiones Legislativas de ambas Cámaras, con especial atención al seguimiento de los proyectos de ley. Con lo cual se pretende contribuir a la certeza legislativa y a disminuir la brecha de disponibilidad de información y análisis entre Legislativo y Ejecutivo.