PONTIFICIA
UNIVERSIDAD
CATÓLICA
DE CHILE

Centro de Políticas Públicas UC

El valor de la privacidad en el combate al COVID-19 en Chile: análisis de las tecnologías de trazabilidad

FERNANDO ARANCIBIA-COLLAO
Facultad de Filosofía

ERNESTO SAN MARTÍN
Facultad de Matemáticas






TEMAS DE LA AGENDA PÚBLICA

Año **16** / Nº **143** / **Julio 2021**
ISSN 0718-9745

El valor de la privacidad en el combate al COVID-19 en Chile: análisis de las tecnologías de trazabilidad

FERNANDO ARANCIBIA-COLLAO
Facultad de Filosofía

ERNESTO SAN MARTÍN
Facultad de Matemáticas

1. Introducción

La discusión sobre la aplicación de las tecnologías de trazabilidad para combatir la pandemia no es nueva. Surgió a propósito de la influenza H1N1 y el uso de las búsquedas de internet para prevenir la propagación de la gripe (Ginsberg et al., 2009; Mayer-Schönberger y Cukier, 2013, p. 11). Con ocasión de la pandemia por COVID-19, este debate se ha reavivado.

Aun cuando ya haya una pluralidad de vacunas siendo fabricadas, la pandemia está lejos de estar bajo control. Cuando escribimos estas líneas (junio de 2021), Chile lleva más de 11 millones de vacunados, pero ha alcanzado casi 9.000 contagiados diarios, superando las cifras del peor periodo de la primera ola. Por ello, la discusión sobre las tecnologías de trazabilidad seguirá teniendo vigencia a la hora de planificar estrategias de combate a la expansión del COVID-19. Pero, además, porque "es casi seguro que estas y otras tecnologías relacionadas se convertirán […] en la caja de herramientas más amplia para la prevención y el control de enfermedades transmisibles de salud pública en el futuro" (Kahn et al., 2020, p. 1).

En el contexto del COVID-19 se han intentado una serie de tecnologías de trazabilidad, fundamentalmente asociadas a los teléfonos móviles. Existen varios ejemplos: las aplicaciones WeChat y Alipay, que son originalmente plataformas de pago, están siendo usadas para el combate de esta pandemia (Gan y Culver, 2020; Kahn et al., 2020, p. 40), o bien las aplicaciones Trace Together, de Singapur; Aarogya Setu, de India; NHSX, de Oxford; o CovidSafe, de la Universidad de Washington (Kahn et al., 2020, p. 40). En general, el desarrollo de estas tecnologías posee varias particularidades, según (i) si almacena o no cierta información, como la localización; (ii) si la información que se guarda es centralizada o descentralizada; (iii) si su uso es voluntario u obligatorio; y (iv) la tecnología usada, entre otros (Kahn et al., 2020, p. 40).

En este artículo, se presentarán estas tecnologías y los riesgos a la privacidad asociados a su uso e implementación. Específicamente, queremos realizar un análisis ético, haciendo referencia a los desafíos relevantes que plantean, con énfasis en la privacidad.

En el apartado 2 presentaremos estas tecnologías, la regulación aplicable, y las implicancias para las metodologías de tratamiento de datos. En el apartado 3 detallaremos el marco ético de referencia, a saber: los principios morales aplicables, los modelos de deliberación moral, y la cuestión sobre el consentimiento informado. Veremos, también, la naturaleza moral de la privacidad, y los riesgos que estas tecnologías implican para este valor. Finalmente, en el apartado 4, daremos algunas recomendaciones para autoridades y científicos, con base en el análisis anterior.

2. Tecnologías de trazabilidad y su aplicabilidad en Chile

2.1. Descripción de las tecnologías de trazabilidad aplicables en Chile

Uno de los mandatos que tiene toda autoridad sanitaria es velar por la salud pública. En el contexto del COVID-19, esta se ve afectada por la rápida propagación del virus, pues no se trata solo de una propagación por medio de contacto físico persona a persona, sino también de contacto con objetos inanimados contaminados con el virus (Van Doremalen et al., 2020), además de contagio persona a persona por medio del aire (Zhang et al., 2020) Esto, sumado a los problemas respiratorios que causa el virus, ha producido y continúa produciendo colapsos en los sistemas sanitarios de cada país, lo que pone en riesgo la vida de los contagiados, pues las capacidades hospitalarias se ven limitadas, teniendo que llegar incluso a tomar decisiones éticamente complejas con relación a qué tipo de paciente atender por sobre otros (Neves, Bitencourt y Bitencourt, 2020; Robert et al., 2020).

Este panorama ha llevado a los países a recolectar información que permita desacelerar los contagios y así dar cierto respiro a la capacidad sanitaria: típicamente estos datos se recogen por medio de la aplicación de tests PCR para identificar a las personas que están probablemente contagiadas y así privilegiar el aislamiento social, de modo de desacelerar la expansión del contagio.

Esta información, junto a la rapidez de propagación del virus (parámetro R0), se ha utilizado para realizar predicciones de contagio por medio de modelos SIR y variantes (REFS), modelos matemático-epidemiológicos que permiten calcular la proporción de infectados y recuperados a partir de la cantidad inicial de susceptibles de ser contagiados. Sin embargo, el mayor número de infectados son identificados por medio de tests PCR, cuya certeza para identificar reales contagiados depende del ciclo de la enfermedad (Sethuraman, Jeremiah y Ryo, 2020), lo que en principio podría debilitar su uso como herramienta para la toma de decisiones de políticas sanitarias. Por otro lado, y lo que parece más inconveniente para dicho propósito, es que este tipo de aproximación se basa en la idea de que el contagio es persona a persona, lo que nuevamente resulta poco convincente con relación al comportamiento dinámico del contagio (González y San Martín, 2020). En este contexto, y dada la rápida velocidad de contagio y la emergencia sanitaria que esto implica, resulta adecuado aplicar tecnologías de trazabilidad que aseguren un seguimiento "casi continuo", es decir, una toma de información permanente, de modo de asegurar un mejor confinamiento de personas contagiadas cuando sea necesario.

Un ejemplo de esto es Coronavirus Pandemic Epidemiology (COPE) Consortium desarrollado en Reino Unido, que reúne esfuerzos científicos tanto de expertos en big data como en epidemiología: se creó una aplicación de trazabilidad utilizable en los teléfonos celulares. Esta aplicación permite recolectar datos sobre factores de riesgo, síntomas predictivos, resultados clínicos y puntos geográficos críticos. Fue lanzada en el Reino Unido el 24 de marzo de 2020 y cinco días después en Estados Unidos, logrando reunir hasta el 2 de mayo de 2020 información de más de 2,8 millones de usuarios. El interés de política sanitaria de esta aplicación fue "ofrecer una prueba de concepto para el replanteamiento de los enfoques existentes, a fin de permitir la recopilación y el análisis de datos epidemiológicos rápidamente escalables, lo que es fundamental para una respuesta basada en datos a este reto de salud pública" (Drew et al., 2020).

Una iniciativa como esta se basa en el paradigma de Políticas Públicas Basadas en Evidencia, cuyo *motto* reza así: "las políticas públicas deben basarse en la mejor evidencia disponible" (Davies y Boruch, 2001). En el caso de la actual pandemia, parece adecuado aplicar este paradigma y así unir las mejores capacidades que permitan tomar buenas decisiones de salud pública, como son la reorganización de los establecimientos hospitalarios (lo que significa, por ejemplo, posponer la atención de otras enfermedades REFS), la adecuación de residencias sanitarias, decidir cuarentenas totales, etc.

En Chile, el Ministerio de Salud implementó una tecnología de seguimiento a través de una nube virtual. Esta innovación "permitirá que todos los sectores involucrados en el rastreo de un caso conozcan simultáneamente la condición del paciente y de sus contactos estrechos" (Cooperativa.cl, 2020).

En lo que sigue, caracterizaremos las diversas tecnologías de trazabilidad según la tecnología utilizada, el manejo que realizan de los datos de las personas, el carácter obligatorio o voluntario de su uso y su objetivo como política pública para enfrentar el COVID-19. Las tecnologías que describiremos más abajo pueden potencialmente ser aplicables en Chile, dado que varias de ellas satisfacen los requerimientos de nuestra legislación vigente.

Las diversas tecnologías de trazabilidad existentes se caracterizan por tomar posición respecto de una serie de aspectos, varios de los cuales poseen implicancias éticas directas. En primer lugar, acerca de los datos que se registrarán y el modo de almacenarlos. En este punto es necesario distinguir entre sistemas centralizados y sistemas descentralizados de almacenamiento de datos. Un sistema centralizado registra los datos en una nube, de modo que la autoridad pueda acceder a ellos con mayor facilidad. Un sistema descentralizado, por el contrario, almacena los datos directamente en el dispositivo (Arriagada Bruneau et al., 2020, pp. 17-18).

Los sistemas centralizados permiten recoger datos de una pluralidad de fuentes, como los celulares, códigos QR, cámaras de reconocimiento facial, tarjetas de crédito e interacciones de redes sociales (Kahn et al., 2020, p. 37). Como veremos, son los que más desafíos a la privacidad suponen.

Respecto de los sistemas descentralizados, estos consisten en un seguimiento por proximidad que protege la privacidad (*privacy-preserving proximity tracking*) que opera a través de un sistema de Bluetooth de baja energía (Bluetooth Low Energy, en adelante: BLE), que registra la proximidad en el dispositivo móvil de los usuarios a través de *beacons* anonimizados. Si una de las personas tiene la aplicación, da positivo por COVID-19 y lo registra en su aplicación, quienes hayan tenido contacto con ella recibirán una notificación. Un ejemplo de estas aplicaciones son las de Exposure Notification, desarrolladas por Apple y Google (Kahn et al., 2020).

Junto con los modelos centralizados y descentralizados, hay modelos intermedios que, por una parte, poseen un sistema centralizado para recibir información sin identificación personal, y un sistema descentralizado para el almacenamiento de datos personales. Los usuarios de estas aplicaciones tienen la opción de compartir la información a la autoridad sanitaria, como por ejemplo, la aplicación COVID SafePaths, desarrollada por el MIT (Kahn et al., 2020, p. 39).

A partir de estas distinciones, se puede afirmar que los sistemas descentralizados son los que garantizan en mayor medida la privacidad, dado que un sistema centralizado promueve la reutilización de los datos (Arriagada Bruneau et al., 2020, p. 18; Steinmann, Matei y Collmann, 2016, pp. 14-15), pues estos son guardados directamente en una nube.

En segundo lugar, las aplicaciones de trazabilidad deben definir el carácter voluntario, incentivado u obligatorio de su uso. En países como Corea del Sur, Polonia e Israel, el uso de estas aplicaciones es obligatorio. Esta dimensión de las aplicaciones de trazabilidad va normalmente de la mano de un tipo especial de almacenamiento de los datos. Los sistemas obligatorios son centralizados.

En el caso de Polonia, por ejemplo, "las autoridades sanitarias han establecido *check-ins* obligatorios que incluyen una captura de puntos de referencia con GPS y *selfies* enviadas a la agencia de monitoreo para garantizar que las personas no estén rompiendo la cuarentena" (Kahn et al., 2020, p. 37).

En tercer lugar, estas aplicaciones deben definir su objetivo. En este sentido, podemos hablar de tecnologías que establecen la trazabilidad de una persona infectada con COVID-19, mientras otras tienen un propósito más limitado, a saber, notificar la proximidad o contacto con una persona COVID positiva (Kahn et al., 2020, p. 40). Finalmente, respecto de la tecnología, las aplicaciones pueden integrar el ya mencionado BLE, GPS o bien SMS. Lo usual es que las aplicaciones usen una combinación de BLE y GPS, como, por ejemplo, WeChat/Alipay, COVID SafePaths o Care19 (Kahn et al., 2020, p. 40).

Respecto de las tecnologías de trazabilidad aplicadas a telefonía móvil, existen varias aplicaciones, algunas de ellas ya han sido adoptadas, mientras que otras han sido abandonadas. Dentro de las primeras tenemos al Corona-Warn-App, desarrollado en Alemania, el Inmuni, de Italia, y el SwissCovid, de Suiza. Dentro de los segundos, encontramos al Isle of Wight, del Reino Unido. La diferencia entre las aplicaciones exitosas y aquellas no existosas radica en el modo en que han integrado los problemas de privacidad.

A partir de lo anterior, podemos clasificar estas tecnologías según la siguiente tabla[1]:

1 Esta tabla se guía por la propuesta de Kahn et al. (2020, p. 40), con algunas diferencias respecto de la original.

Tabla 1. **Aplicaciones de trazabilidad**

Aplicación, país y/o desarrollador	Tecnología utilizada	Acceso de la autoridad gubernamental	Centralizada, intermedia, descentralizada	Obligatoria o voluntaria	Objetivo
WeChat/Alipay (China)	BLE, GPS	Los datos provienen de fuentes de gobierno	Centralizada	Obligatoria	Notificar proximidad y exposición a un caso positivo
Trace Together (Singapur)	BLE	Posee acceso a los datos si se registra un caso positivo	Descentralizada	Voluntaria	Rastreo digital
NHSX (Reino Unido, Universidad de Oxford)	BLE	Posee acceso a los datos	Centralizada	Voluntaria	Rastreo digital
Covid SafePaths (EE.UU., MIT)	BLE, GPS	El usuario puede compartir sus datos si sale positivo	Intermedia	Voluntaria	Rastreo digital
Aarogya Setu (India)	BLE, GPS	Acceso anonimizado a los datos agregados	Intermedia	Voluntaria	Rastreo digital
Care19 (EE.UU., Dakota del Norte)	BLE, GPS	Posee acceso a los datos agregados, aunque puede acceder a datos del usuario si sale positivo	Intermedia	Voluntaria	Rastreo digital y notificar proximidad y exposición a un caso positivo

En cuanto al éxito de estas tecnologías, hay datos acerca de la aceptación de su uso por parte de la ciudadanía, como así también datos sobre su uso efectivo. En general, se encontró "un fuerte apoyo a la aplicación" tanto bajo un régimen voluntario como obligatorio, "en todos los países, en todos los subgrupos de población, e independientemente de las tasas de mortalidad por COVID-19 a nivel regional" (Altmann et al., 2020).

En cuanto al uso de estas aplicaciones, se plantea que, para ser efectivas, debe haber un umbral de 50% a 70% de usuarios activos. Sin embargo, se ha reportado, a febrero de 2021, que solo un 20% de la población de Singapur ha descargado la aplicación Trace Together, con un 16% de población que lo usa activamente, junto con un 4% de australianos que ha descargado CovidSafe de Play Store (Akinbi, Forshaw y Blinkhorn, 2021). Esto contrasta con los datos de la aplicación NHSX del Reino Unido, que ha demostrado ser eficaz al disminuir contagios (Lewis, 2021; Wymant et al., 2021).

2.2. Legislación en Chile

La protección a la privacidad está regulada en varios instrumentos normativos, siendo el más importante de ellos la Constitución Política. En su artículo 19 Nº 4 consigna como derecho fundamental "el respeto y la protección a la vida privada y a la honra de la persona y su familia, y asimismo, la protección de sus datos personales", indicando que "el tratamiento y la proteccion de estos datos se efectuará en la forma y condiciones que determine la ley". Dentro de esta determinación está la Ley Nº 19.628 sobre Protección de la Vida Privada, y, además, los instrumentos jurídicos internacionales, que en nuestro ordenamiento tienen jerarquía de ley, como el Pacto Internacional de Derechos Civiles y Políticos (art. 17), y la Convención Americana sobre Derechos Humanos (art. 11), que, en términos generales, poseen fórmulas semejantes a la Constitución en la relación entre protección de la vida privada y la honra de la persona y la exigencia de que la ley las proteja.

La Ley Nº 19.268 define los datos personales y los datos sensibles. Los datos personales son aquellos "relativos a cualquier información concerniente a personas naturales, identificadas o identificables" (art. 2°, literal f), mientras que los datos sensibles son "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 racional, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos y la vida sexual" (art. 2, letra g). Por lo tanto, todo dato que sea recopilado para rastrear y/o registrar personas con diagnóstico PCR positivo por COVID-19 será dato personal y sensible, al referirse a los "estados de salud físicos" de "personas identificadas o identificables". Las tecnologías discutidas, entonces, tienen efectos sobre la privacidad de ambos tipos de datos.

Otro de los instrumentos normativos relevantes para el caso que estamos analizando es la Ley Nº 20.584, sobre los derechos y deberes que tienen las personas en relación con acciones vinculadas a su atención en salud. Esta ley tiene algunas disposiciones relacionadas con el uso de datos personales y sensibles (según la Ley Nº 19.268), como con el consentimiento informado en prestaciones de salud.

En el artículo 5°, literal c se dice que las personas tienen derecho al respeto y la protección de la vida privada en su atención en salud, particularmente respecto de toma de fotografías, grabaciones y filmaciones, con independencia de su uso. En el inciso 5º se regula la reserva de la información de la ficha clínica, considerada dato sensible (art. 12). La información de esa ficha no podrá ser accedida por terceros no relacionados a la atención de la persona, salvo cuando existan condiciones particulares para entregar la información total o parcial, como cuando la persona autoriza expresamente a un tercero para el acceso a esa información, o bien lo soliciten los tribunales, el Ministerio Público o el ISP (art. 13).

Respecto del consentimiento informado, la ley plantea que la persona debe expresar su voluntad para someterse o no a cualquier procedimiento vinculado a su atención en salud, y que el profesional tratante deberá proveer información "adecuada, suficiente y comprensible" (art. 14). En esta misma línea se pronuncia la ley cuando exige el respeto a la autonomía en la participación en una investigación. La expresión de voluntad de la persona "deberá ser previa, expresa, libre, informada, personal y constar por escrito" (art. 21).

Esta última exigencia nos lleva a la Ley Nº 20.120 sobre investigación científica en el ser humano. A este respecto, la ley plantea, en el art. 11, inc. 2°:

> "Para los efectos de esta ley, existe consentimiento informado cuando la persona que debe prestarlo conoce los aspectos esenciales de la investigación, en especial su finalidad, beneficios, riesgos y los procedimientos o tratamientos alternativos. Para ello deberá habérsele proporcionado información adecuada, suficiente y comprensible sobre ella. Asimismo, deberá hacerse especial mención del derecho que tiene de no autorizar la investigación o de revocar su consentimiento en cualquier momento y por cualquier medio, sin que ello importe responsabilidad, sanción o pérdida de beneficio alguno".

En síntesis: los datos recopilados, registrados y utilizados por las tecnologías de trazabilidad son datos personales y sensibles, y están protegidos por la ley. Por otra parte, se puede interpretar que el uso de estas tecnologías implica atención en salud. Bajo esa perspectiva, existe una protección de los datos personales y sensibles, como así también del consentimiento informado.

Sin embargo, esta legislación es insuficiente para brindar una protección robusta a la privacidad. Se han planteado los siguientes problemas:

> "Primero, la ausencia de una obligación que requiera establecer medidas concretas y precisas de seguridad por parte del responsable (del tratamiento de los datos), que atiendan a criterios mínimos como el estado de arte, los costos de implementar medidas, la naturaleza de los datos personales, el tipo de tratamiento o los posibles riesgos que este conlleva. Segundo, la ausencia de obligaciones asociadas al reporte de vulneraciones que afecten medidas de seguridad a una autoridad o a los titulares de datos afectados, de forma que puedan tomar aquellos resguardos que permitan atenuar los efectos adversos derivados de la vulneración. (…) Tercero, la ausencia de la posibilidad de que los titulares exijan a los responsables la aplicación de medidas de seguridad específicas para garantizar la seguridad de los datos tratados. (…) Cuarto, la ausencia de obligaciones de seguridad particulares para el mandatario o encargado que trata los datos personales en lugar y nombre del responsable del banco de datos. (…) Quinto, la ausencia de un principio de seguridad que inspire el tratamiento de los datos personales por los responsables del banco de datos y los mandatarios (Benussi Díaz, 2020, pp. 243-44).

Todo lo anterior afecta a los datos personales y sensibles que manejan las aplicaciones de trazabilidad. Además, la legislación no contempla instrumentos de fiscalización sobre el modo en que las aplicaciones de trazabilidad

procesarán el consentimiento informado. En este sentido, no hay posibilidad de que dicho consentimiento sea solicitado por un profesional, como lo exige el art. 14 de la Ley Nº 20.584.

En resumen, de acuerdo con esta aproximación general, la legislación vigente no permite establecer un marco regulatorio claro para estas tecnologías ni una protección jurídica relevante para la privacidad.

3. Privacidad y uso ético de datos

3.1. Principios éticos

La consideración de principios de acción es el primer paso a la hora de considerar las nuevas tecnologías aplicadas al combate del COVID-19 y los riesgos que implican. Estos principios precisan los alcances de esta tecnología en el modo en que limitan los derechos fundamentales de las personas y, en particular, el derecho a la privacidad. En lo que sigue, analizaremos las tecnologías de trazabilidad a la luz de los principios de beneficencia, no maleficencia, autonomía, justicia, confianza y precaución.

Uno de los principales objetivos de las tecnologías utilizadas para el trazado de los pacientes contagiados es disminuir la tasa de contagio. En esta línea va la política general del Ministerio de Salud de desarrollar una estrategia de trazado (El Mercurio, 2020). El objetivo es, sin duda, realizar un bien, a partir del principio de beneficencia. Sin embargo, debe establecerse con claridad de qué manera se concibe el hacer el bien. En este sentido, la aplicación del principio de beneficencia (hacer el bien) no basta por sí solo, sino que debe estar sometido a ciertas restricciones que limiten el uso de los medios. La primera restricción es el principio de no maleficencia (evitar el mal). Sin embargo, una concepción utilitarista de ambos principios haría un cálculo entre los bienes a alcanzar versus los males a evitar. Si una aplicación de rastreo lesiona la privacidad de las personas, causando daño, habrá que considerar cuánto más bien podría hacerse por esta vía y, de este modo, la lesión a la privacidad quedaría justificada.

Los principios de beneficencia y no maleficencia deben ser complementados por el principio de autonomía. Este plantea la necesidad de respetar la libertad de las personas y su capacidad de decisión (Steinmann et al., 2016, pp. 19-20). En el contexto de las aplicaciones de rastreo, es necesario que la persona consienta en su uso, y que su registro no implique otras restricciones a sus derechos. Esto supone una limitación a los principios anteriores dado que toda búsqueda del bien total, a partir del principio de beneficencia, deberá someterse a la decisión libre de quien es objeto del rastreo.

Por su parte, el principio de justicia está vinculado a otros temas más generales sobre la justicia a nivel socioeconómico en general, y a nivel de la atención sanitaria en particular (Hortal, 2002, pp. 79-80). En primer lugar, este principio complementa a los anteriores, en el sentido de que el uso de estos mecanismos de rastreo no debe implicar una desventaja comparativa para quien es objeto de esta tecnología. En segundo lugar, el registro de las personas rastreadas podría implicar injusticias posteriores que podrían manifestarse en un acceso desigual a ciertos bienes sociales para quienes han sido rastreados, como también que este hecho implique, para ellos, que los recursos sociales no les sean adecuadamente distribuidos (Steinmann et al., 2016, p. 19), por ejemplo, para el acceso a seguros o planes de salud.

El principio de confianza se aplica a instituciones y se manifiesta en que la ciudadanía tiene una expectativa razonable de que las instituciones políticas y sociales cumplan adecuadamente sus roles específicos en el contexto de la pandemia (Steinmann et al., 2016, p. 20). La confianza presupone los demás principios: la ciudadanía debe confiar en que las instituciones actuarán para evitar el mal y promover el bien de las personas, respetando su libre decisión y bajo criterios de justicia. La aplicación del principio de confianza en el contexto de las tecnologías de trazabilidad se funda, en una medida importante, en la legislación y en la legitimidad democrática del gobierno. En la medida en que los derechos de las personas estén adecuadamente resguardados por instrumentos normativos que puedan hacer frente a la complejidad que supone el uso de estas tecnologías, y en la medida en que exista un estado de derecho que garantice el respeto por esas normas, las personas podrán utilizar estas tecnologías con la tranquilidad de que sus datos no serán utilizados para otros fines.

A este respecto es importante mencionar que la trazabilidad, así como otras medidas, pueden ser obligatorias dado un contexto de emergencia, así como ocurre en Polonia, Corea del Sur e Israel: es el contexto de emergencia el que permite una excepción al respeto de derechos individuales y civiles, como la confidencialidad de los datos privados. Resulta importante que, ante esta medi-

da de excepción, se asegure que, una vez terminada la misma, se restauren dichos derechos[2], garantizándose ya sea la destrucción total de la información recolectada durante el período de emergencia, o se prometa que la misma no será utilizada con otros fines[3]. Esto último es parte de los protocolos estadísticos que salvaguardan la confidencialidad de los datos, que significa que la parte que tiene acceso a la información personal está limitada por una promesa explícita o implícita en relación con que protegerá dicha información de accesos y de usos no autorizados. La confidencialidad hace así referencia a "una cualidad o condición acordada a la información en tanto una obligación de no transmitir dicha información a terceros no autorizados" (Fienberg, 2005)[4].

El principio de precaución, por su parte, plantea la necesidad de evaluar global y prudencialmente los riesgos de toda nueva innovación tecnológica. La evaluación de dichos riesgos tiene una dimensión científica, que identifica riesgos mensurables, pero también tiene una dimensión prudencial, vinculada a riesgos no mensurables, y que pueden poner en peligro bienes morales importantes para las personas y comunidades. Este principio tiene dos interpretaciones viables. En ambas interpretaciones se requerirá que los riesgos sean analizados con total seriedad antes de dar luz verde a cualquier innovación tecnológica que pueda afectar los derechos fundamentales de las personas. La primera interpretación, de carácter flexible, plantea que debe darse un tiempo de moratoria para el análisis de los riesgos antes de poner en funcionamiento cualquier innovación tecnológica. La segunda, una interpretación estricta, plantea que debe tenerse total seguridad de que las innovaciones tecnológicas no afecten derechos fundamentales de las personas (Eizagirre, 2011). Uno de los criterios que se ha planteado a propósito del principio de precaución en el contexto de las tecnologías de trazabilidad es la reversibilidad. Puesto que existe una gran incertidumbre epistémica respecto de los efectos de estas tecnologías, y puesto que estas tecnologías, a su vez, podrían evitar gran daño, la reversibilidad de las limitaciones y de las acciones adoptadas en pro de una mayor presencia de estas tecnologías es fundamental, tanto para el respeto de la privacidad y de los valores que esta protege, como de la utilidad de estas tecnologías para evitar mayores contagios y pérdidas de vidas (Nijsingh, Van Bergen y Wild, 2020).

Los principios listados y explicados en este apartado permiten tener una perspectiva global de evaluación de la viabilidad moral de las tecnologías que se están planteando para combatir el COVID-19. Cada uno de estos principios plantea exigencias especificables en el contexto de la evaluación. También, estos principios deben considerarse en su conjunto, y en cierto modo, bajo un cierto orden de aplicación.

La primera limitación a toda acción tecnológica que afecte a las personas debe pasar por el filtro de los principios de beneficencia y no maleficencia; es decir, deben ser acciones e innovaciones dirigidas hacia la promoción de un bien o hacia la evitación de un mal. Estos dos principios, sin otros límites, puede dar lugar a aplicaciones utilitaristas que pasen a llevar derechos individuales importantes. Por ello, requiere ser complementado con los principios siguientes.

En segundo lugar, el principio de autonomía exige el consentimiento del sujeto, mientras que el principio de justicia requiere que la aplicación de estas tecnologías no tenga impacto en el acceso de las personas a los bienes sociales.

En tercer lugar, el principio de confianza regula las relaciones de la ciudadanía con las instituciones sociales encargadas de aplicar estas nuevas tecnologías y monitorear su uso. El principio de confianza, en el contexto de un reciente estallido social, se vuelve fundamental para la viabilidad de estas tecnologías, y, sobre todo, para su legitimidad social.

2 En Francia, como consecuencia de los atentados terroristas de los últimos años, se implantó la llamada Ley de Seguridad Global, que impone sistemas de vigilancia continuos, involucrando a los ciudadanos como colaboradores en la vigilancia de toda actitud sospechosa que podría conllevar acciones terroristas: esto implica –en palabras del presidente Macron– la construcción de "una sociedad de vigilancia". Ante esto, ciertos derechos civiles de respeto de la privacidad se ven debilitados: la paradoja ética de esta situación radica en el hecho de que el Estado francés no ha definido operacionalmente cuándo el estado de emergencia llega a su fin (Codaccioni, 2021).

3 La Ley Dicom o Ley Nº 20.575 estableció los datos financieros que se puede informar a terceros no titulares, las condiciones que una persona debe cumplir para ser borrado del registro Dicom y los usos no autorizados de dichos datos (como, por ejemplo, la admisión a atención médica de urgencia o la postulación a un cargo público). A pesar de esto, es posible hallar testimonios aislados de un uso indebido de esta información personal.

4 La promesa de no permitir un uso no autorizado de los datos es un acto performativo de lenguaje: el acto de prometer por un otro que tiene la potestad de hacerlo realiza la confidencialidad de la información.

Finalmente, la precaución como principio integrativo permite evaluar íntegramente los riesgos que presentan estas tecnologías a la luz de los principios anteriores. El principio de precaución se aplica, sobre todo, en la evaluación del riesgo, no solo en su gestión (Eizagirre, 2011). Es un principio que permite integrar la evaluación de una innovación tecnológica en un contexto político y moral más amplio.

3.2. Modelos de deliberación moral

Una aproximación meramente principalista al problema de la privacidad deja una serie de interrogantes abiertas. En primer lugar, la aplicación del principio de beneficencia requiere una definición previa acerca del bien que se busca realizar. Por otra parte, cabe preguntarse si las consideraciones de beneficencia son prioritarias a otras relativas a la justicia o a la autonomía. Tanto la determinación de la naturaleza de ese bien como la prioridad de lo justo sobre lo bueno (o viceversa) es rol de los modelos de deliberación moral.

Un modelo de deliberación moral (o marco ético de referencia, modelo ético, entre otras denominaciones) define, por una parte, las interrelaciones entre lo bueno y lo justo, y por otra establece criterios para definir lo bueno y/o lo justo, según corresponda[5].

3.2.1. Utilitarismo

Uno de los modelos éticos más relevantes en la historia de la ética y las ciencias sociales es el utilitarismo. El utilitarismo tiene diversas versiones, dentro de las cuales la más difundida tanto en filosofía como en economía[6] es el utilitarismo clásico, desarrollado por Jeremy Bentham y J. S. Mill (Bentham, 1780; Mill, 1863). Este modelo plantea la obligatoriedad de la maximización de la utilidad. La utilidad se entiende en términos de felicidad, y la felicidad, en términos hedonistas (predominio del placer por sobre el dolor). Para el utilitarismo lo bueno es la felicidad[7] en sentido hedonista. A su vez, para esta teoría, lo bueno define lo justo, en la medida en que la obligación de justicia dice relación con la maximización de la utilidad para todos[8].

La acción, de acuerdo con esta perspectiva, se evalúa por sus consecuencias. Si las consecuencias son la mayor felicidad neta frente a otras posibilidades de acción, entonces la acción es correcta. En ese sentido, el utilitarismo es una forma específica de razonamiento consecuencialista, que pone énfasis en las consecuencias de la acción para evaluarla. La diferencia del utilitarismo respecto de otras formas de consecuencialismo no utilitarista radica en el modo en que se evalúan las consecuencias; pero comparte con estas teorías la preeminencia de las consecuencias en la evaluación moral.

Existen varias formas recientes de utilitarismo (Brandt, 1979; Hardin, 1988; Lyons, 1965; Smart y Williams, 1973) y otras cuantas de consecuencialismos no utilitaristas (Griffin, 1986; Mulgan, 2001). Una forma reciente y destacada es el utilitarismo de la preferencia, del filósofo Peter Singer. Esta forma de utilitarismo mantiene la dimensión consecuencialista del utilitarismo clásico, pero prescinde de su fundación eudaimonista, al basar la consideración de consecuencias en la satisfacción de las preferencias de los agentes moralmente relevantes (Singer, 1979).

3.2.2. Deontología

Otro modelo ético relevante es el deontológico. Su formulación clásica se debe a Immanuel Kant. A diferencia del utilitarismo, plantea que lo justo tiene prioridad por sobre lo bueno, en la medida en que lo bueno es una consideración secundaria del acto. El acto correcto no necesariamente implica promover o maximizar un valor, sino actuar conforme a ciertos principios básicos de la moralidad. Kant habla del "imperativo categórico", el cual es un principio que define ciertas normas morales mínimas y absolutas de respeto por el otro (Kant, 2012). La consideración del otro como un "fin en sí mismo" lleva a reconocer a la autonomía como un principio prioritario entre los listados en el apartado anterior, junto con el de justicia.

La teoría de la justicia de John Rawls es una teoría deontológica aplicada a las instituciones sociales. Para este

5 La explicación de los modelos éticos que sigue es extremadamente resumida y toma en consideración solo algunos de los enfoques que existen en filosofía moral.

6 El utilitarismo ha sido fundamental en la caracterización de la economía del bienestar, que tradicionalmente ha utilizado un criterio utilitarista para la determinación del óptimo social (Hausman, McPherson y Satz, 2017; Sen, 1991).

7 De ahí que a las éticas de la felicidad se les llame "eudaimonistas" (por el término griego eudaimonía, que significa "felicidad").

8 Existen otros aspectos estructurales del utilitarismo, a saber: si la maximización de la utilidad se exige respecto de cada acto, o bien, se espera establecer un corpus de reglas que, en términos generales, tiendan a maximizar la utilidad. Es la conocida oposición entre utilitarismo del acto versus utilitarismo de la regla (Gensler, 1998, pp. 171-194; Vardy y Grosch, 1997, pp. 81-83).

autor, las exigencias de justicia son el mínimo común a las que deben someterse todas las concepciones del bien substantivas. Estas exigencias de justicia se establecen a través de un consenso entrecruzado entre estas diversas doctrinas del bien (Rawls, 1995).

Para la ética deontológica, las consideraciones de autonomía y justicia son prioritarias respecto de las relativas a la beneficencia.

3.2.3. Ética de la virtud y de bienes

La ética de la virtud es otra de las teorías relevantes en la literatura reciente (Battaly, 2015; Hursthouse, 1999; McKinnon, 1999; Russell, 2009; Swanton, 2003). Tiene su formulación clásica en la filosofía de Aristóteles, y actualmente se ha desarrollado profusamente. Una teoría emparentada con la ética de la virtud es la ética de bienes, cuya formulación clásica se encuentra también en Aristóteles, y en la teoría de la ley natural de Tomás de Aquino, y por esto se justifica tratarlas de manera conjunta (Aquino, 2007; Aristóteles, 1998). Estas dos teorías son, al igual que el utilitarismo, éticas de la felicidad, y por ello lo justo es dependiente de lo bueno. Sin embargo, comparte con la ética deontológica la existencia de deberes morales mínimos e incondicionados que no están sujetos a consideraciones de utilidad.

La ética de la virtud pone énfasis en los aspectos del carácter que constituyen disposiciones valiosas. Se enfoca no tanto en el valor moral de las acciones (deontología), o en sus consecuencias (utilitarismo), sino en el agente moral, que desarrolla disposiciones valiosas a manera de una "segunda naturaleza". Estas disposiciones serán virtudes si son valiosas y vicios si son moralmente indeseables. De ahí que toda atribución que hacemos del carácter de una persona (si es honesta, trabajadora, justa, o bien, mentirosa, envidiosa, etc.) corresponde a esta "segunda naturaleza", que se adquiere a través del hábito en la realización de ciertas elecciones.

La ética de bienes (también llamada "ética de la ley natural") plantea la existencia de bienes humanos básicos que constituyen el florecimiento y la realización humana (Chappell, 1998; Finnis, 1980; Gómez-Lobo, 2002; Murphy, 2001; Oderberg, 2000). Junto con la ética de la virtud, y en cuanto ética eudaimonista, plantea que la realización humana es la meta última de toda acción y decisión y, por lo tanto, de la moralidad. Mientras que para la ética de la virtud la felicidad se alcanza en el desarrollo y cultivo de virtudes, para la ética de bienes, el florecimiento humano se logra en el desarrollo de ciertos proyectos de vida que se fundan en estos bienes humanos básicos, tales como la vida, el conocimiento, la experiencia estética, la familia, la amistad, entre otros.

Finalmente, ambos modelos éticos consideran que la autonomía es un principio secundario frente al bien, implicando esto que la autonomía debe ser correctamente ejercida con base en las virtudes (ética de la virtud) o en los bienes humanos básicos (ética de bienes). El ejercicio de la autonomía implica ciertas restricciones deontológicas basadas en estas virtudes o en estos bienes humanos básicos.

3.2.4. Análisis principalista y modelos éticos

Los modelos éticos antes explicados permiten complementar el análisis principalista del apartado anterior a través de la precisión sobre (i) la naturaleza del bien moral y (ii) la correlación entre este bien y otros aspectos, como el de la justicia. De modo preliminar, podemos indicar que un modelo deontológico dará prioridad al principio de justicia, mientras que un modelo eudaimonista (a saber, el utilitarismo, la ética de la virtud y la ética de bienes) darán énfasis al principio de beneficencia. La diferencia entre los modelos eudaimonistas radicará fundamentalmente (aunque no únicamente) en el modo de interpretar la beneficencia.

Respecto de las tecnologías de trazabilidad, los principios y los modelos éticos, podemos pensar que una aplicación no restringida de estas tecnologías debe tener como objeto la realización de un bien y el evitar un mal (en aplicación de los principios de beneficencia y no maleficencia). Desde la perspectiva de un utilitarismo clásico, la aplicación de estas tecnologías será legítima si promueve la felicidad del mayor número. Esta felicidad debe entenderse siempre como un cálculo que integre placeres y dolores (según la concepción hedonista de esta teoría) o satisfacción de preferencias del mayor número (de acuerdo con el utilitarismo de la preferencia). De este modo, es natural concluir que, en aplicación del modelo utilitarista, no habría mayores restricciones al principio de beneficencia, mientras el uso de estas tecnologías genere como consecuencia un estado de cosas en el cual se promueve el bienestar del mayor número. A su vez, las consideraciones de justicia se subordinarán a este cálculo, de modo que la aplicación del principio de justicia será un mero correlato de la aplicación del principio de beneficencia.

Sin embargo, la consideración de los principios de autonomía, confianza y precaución establecen restriccio-

nes a la mera consideración de las consecuencias. Por una parte, la autonomía sería una clara restricción de la maximización de la utilidad del utilitarismo clásico. Por otra, si bien el principio de autonomía es claramente deontológico, es posible articular una concepción consecuencialista de la autonomía, en la cual lo moralmente obligatorio sería maximización en la realización de este valor (Farrell, 2003, pp. 89-99). Respecto del principio de confianza, su correcta atribución a las instituciones requiere ciertas restricciones al cálculo de consecuencias: no vale cualquier tipo de medio para alcanzar la mayor utilidad total. La confianza de las personas en las instituciones se vería afectada si no existen restricciones respecto de los medios utilizados para la protección de la salud de las personas. Finalmente, el principio de precaución cumple un rol integrador de los principios anteriores a través de una evaluación integral del riesgo. De este modo, toma en consideración eventuales riesgos, no solo aquellos asociados a la salud y la vida de las personas, sino también riesgos a sus libertades y a sus posibilidades de realización en otros ámbitos.

Un razonamiento consecuencialista podría integrar las consideraciones anteriores en términos de utilidad (a saber, que la autonomía de las personas contribuye a la felicidad total o que la confianza en las instituciones redunda en la felicidad total). Pero, aún en este caso, las restricciones emanadas del contenido de estos principios permanecerían y, por lo tanto, no es posible plantear que un razonamiento utilitarista interpretaría la felicidad total como la maximización de la vida y la salud de las personas, aún a costa de un riesgo claro a su privacidad o a otras libertades relevantes. De este modo, aún un razonamiento utilitarista flexible propondría restricciones al uso de las tecnologías de trazabilidad, tomando en consideración otros valores.

Por parte de la deontología, las restricciones a los usos de estas tecnologías son más claras. Los principios antes listados se entienden como exigencias categóricas de respeto por el otro. Así, antes de promover el bien, lo que se busca es el respeto a la autonomía de las personas y otras consideraciones de justicia relevantes. Así, la aplicación de las tecnologías de trazabilidad no sería, en ningún caso, permisiva desde el punto de vista de las medidas que podría adoptar la autoridad (como ya vimos a propósito del utilitarismo, ni siquiera un análisis utilitarista flexible permitiría una aplicación de este tipo). Las restricciones más relevantes dicen relación con la autonomía y las consideraciones de justicia que deben cumplir la autoridad en la aplicación de estas tecnologías. Consideraciones de utilidad que, por muy robustas que sean (en el sentido de que se evalúe que una aplicación permisiva de estas tecnologías conllevaría un gran bien en términos de la salud y la vida de las personas), no podrían pasar a llevar aspectos relevantes de la autodeterminación de la persona ni afectar sus posibilidades de realización en otros ámbitos.

Finalmente, respecto de las éticas de bienes y de la virtud, al ser estas modelos de naturaleza eudaimonista, el principio de beneficencia posee prioridad respecto de los demás, que se entienden en función de la concepción de bien que plantean estas teorías. De este modo, la evaluación moral de la aplicación de las tecnologías de trazabilidad debe considerar, en el caso de la ética de la virtud, (i) si está realizada por motivos valiosos, (ii) si promueve ciertas disposiciones valiosas en las personas y, finalmente, (iii) si promueve las posibilidades de realización de las personas, en virtud de una concepción de felicidad integral. De manera similar, la ética de bienes evaluaría la aplicación de las tecnologías de trazabilidad desde la perspectiva de los bienes humanos básicos que promueven o afectan.

Estas dos teorías deben identificar, en primer lugar, una concepción de felicidad que dé contenido a la aplicación del principio de beneficencia. Por otra parte, deben considerar ciertas restricciones deontológicas que van de la mano de los principios de no-maleficencia, autonomía y justicia. De este modo, desde estos modelos éticos, no sería permisible moralmente promover por cualquier medio las virtudes o los bienes humanos básicos, sino, por el contrario, lo correcto será integrar las restricciones de los principios antedichos de manera estricta. Ahora bien, de la misma manera en que estos principios limitan la promoción de la concepción de felicidad de estas teorías por cualquier medio, también esta concepción de felicidad, basada en las virtudes y en los bienes humanos básicos, limita los alcances de la autonomía y la justicia, en el sentido de que la autonomía, por ejemplo, no podría tener como objetivo la disolución de alguna virtud o la transgresión de un bien humano básico.

3.3. La privacidad

La evaluación principalista propuesta en el apartado 3.1 constituye una aproximación general y minimalista, dirigida a orientar la acción relativa a las posibles tecnologías que puedan afectar los derechos de las personas. Los principios establecen criterios de corrección generales y mínimos respecto de estas tecnologías, pero, por sí mismos, no nos hablan sobre las concepciones de bien y

otros valores substantivos que pudieran ser relevantes. Por ello, es necesario tomar en cuenta los modelos de deliberación moral estudiados en el apartado 3.2, para entender cómo evaluar las situaciones y aplicar los principios, estableciendo sus contenidos normativos precisos y el modo en que ellos se interrelacionarán. Hemos planteado, de modo provisional, la forma en que estos principios, de acuerdo con cada modelo ético, evaluarían en términos generales las tecnologías de trazabilidad. En este apartado quisiéramos desarrollar sus implicancias para la privacidad en específico.

3.3.1. Naturaleza moral de la privacidad

La privacidad tiene una pluralidad de sentidos diversos. Para el problema que nos presentan estas tecnologías, son importantes dos concepciones sobre la privacidad: la informacional, es decir, "confidencialidad, anonimidad, protección de datos, y secreto respecto de los hechos de una persona"; y la privacidad física, a saber, el hecho de poder estar tranquilo, solo, sin la observación de otros (Allen, 2003, p. 485). Ambos tipos de privacidad están estrechamente vinculados, puesto que la concepción física implica, en algún sentido, la informacional. Con relación a las tecnologías de seguimiento, la posibilidad de la autoridad de rastrear la ubicación de una persona supone una invasión tanto de la privacidad informacional como de la física.

La naturaleza moral de la privacidad es la de un valor instrumental o valor-medio (Baron, 2007, pp. 49 y 150). En efecto, la privacidad por sí misma no tiene valor moral, sino en cuanto resguarda otros valores más importantes. En primer lugar, podemos afirmar que la privacidad protege la autonomía y la capacidad de tomar decisiones libres o, en otras palabras, nuestra capacidad de agencia moral (Allen, 2003, pp. 492). Pero también puede ser condición de posibilidad de otros bienes, como todos los bienes relacionales (como la amistad o el amor) que requieren de cierta intimidad (Tollefsen, 2007, pp. 23-26). Además, estos bienes relacionales pueden ser comprendidos como bienes esenciales para una vida auténticamente plena (Murphy, 2001, pp. 126-131; Tollefsen, 2007, p. 26).

3.3.2. Riesgos a la privacidad

Los riesgos a la privacidad relacionados con las tecnologías de trazabilidad pueden considerarse en el contexto más amplio de los peligros relativos al uso de datos, los cuales, a su vez, poseen implicancias éticas y políticas relevantes. Podemos clasificar estos riesgos entre directos e indirectos. Los directos dicen relación con aquellos riesgos que implican directamente el uso de estas tecnologías. Los riesgos a la privacidad son, esencialmente, directos. Los riesgos indirectos son aquellos que dicen relación con los bienes que protege la privacidad. Puesto que no es posible disociar los riesgos indirectos de la privacidad de los directos, consideramos que son igualmente relevantes, y deben ser tenidos en cuenta a la hora de desarrollar y adoptar cualquier tecnología de trazabilidad para combatir al COVID-19.

El riesgo más claro y directo de estas tecnologías es la reidentificación del usuario que proporciona los datos. El principio fundamental de estas tecnologías es la anonimización de los datos que recopila. La anonimización "consiste en despojar los conjuntos de datos de todos los rasgos identificadores personales, como pueden ser nombre, dirección, número de tarjeta de crédito, fecha de nacimiento o número de la seguridad social. Los datos resultantes pueden ser analizados y compartidos sin poner en peligro la privacidad de nadie. Pero esto solo funciona en un mundo escaso en información. Los datos masivos, al incrementar la cantidad y diversidad de la información, facilitan la reidentificación" (Mayer-Schönberger y Cukier, 2013, p. 192). Si bien existen mecanismos técnicos de anonimización (Gkoulalas-Divanis y Loukides, 2015) es posible, también, elaborar modelos que reidentifiquen a las personas usando 15 atributos demográficos y con un 99,98% de eficacia (Arriagada Bruneau et al., 2020, p. 15; Rocher, Hendrickx y De Montjoye, 2019). La reidentificación de los datos plantea riesgos evidentes a la privacidad, particularmente en sistemas de trazabilidad centralizados.

En cuanto a los riesgos indirectos, el primero de ellos es hacia la igualdad de oportunidades. Ella se puede ver afectada, toda vez que el uso de datos personales y sensibles podría tener efectos en personas afectadas con alguna condición de salud para contratar un plan de protección de la salud, postular a un trabajo, obtener un crédito, incluso su seguridad y libertad (Mayer-Schönberger y Cukier, 2013, pp. 196-202). Esto, desde el punto de vista de una ética deontológica, afecta la autonomía de la persona, y desde el de una ética de la virtud o de bienes, disminuye las posibilidades de realización de esa persona.

El segundo riesgo indirecto es la 'dictadura de los datos'. El uso de datos por parte de quienes toman decisiones de política pública podría llevar a decisiones incorrectas, sin un marco analítico que permita interpretar los datos

con los que cuentan (Mayer-Schönberger y Cukier 2013, pp. 203-210). En particular, las decisiones incorrectas se deben al hecho de que los datos de trazabilidad dependen del consentimiento de los usuarios y, por tanto, están afectos a sesgos de autoselección.

Finalmente, existen desafíos más amplios a la democracia. El uso de los datos por parte de gobiernos podría implicar mayores riesgos a los derechos fundamentales de los habitantes de esos países. En virtud de la pandemia, se pueden expandir los estados de excepción (Nay, 2020), y el uso de tecnologías de trazabilidad de tipo centralizado podría dar información valiosa para la persecución de opositores. "El tipo de países en los cuales las aplicaciones de trazabilidad centralizada han sido aplicadas, son generalmente 'estados de vigilancia', esto es, países que tienen una gran dosis de poder sobre los ciudadanos y conocimiento sobre ellos" (Codaccioni, 2021; Sweeney, 2020, p. 303). Finalmente, la privacidad se convierte en una condición necesaria para la participación política democrática, "ya que permite a los individuos y grupos para elegir aspectos de sus vidas que permanecerán privados o que se divulgarán a medida que participen en la participación política y obtengan información sobre candidatos y temas" (Francis y Francis, 2017, p. 278).

4. Recomendaciones

En lo que sigue quisiéramos recoger las consideraciones anteriores para brindar algunas recomendaciones que orienten los procesos de deliberación sobre política pública, a propósito del riesgo a la privacidad que podría suponer el uso e implementación de las tecnologías de trazabilidad.

4.1. Las condiciones para un uso responsable de datos personales en el combate a la pandemia

En primer lugar, existe una discusión clara y abundante en el mundo desarrollado sobre la importancia de la privacidad y, en virtud de ello, se han elaborado técnicas de anonimización de datos para proteger la privacidad de las personas sin una pérdida substantiva de la utilidad de los datos. En el caso de las tecnologías de trazabilidad, la utilidad de los datos puede llevar a evitar contagios y, por lo tanto, a salvar vidas.

Sin embargo, un enfoque utilitarista, tal como fue discutido, implica riesgos para bienes morales relevantes. En una era digital, en la cual la posesión y uso de los datos adquiere cada vez mayor relevancia, no podemos descartar que los riesgos a la privacidad impliquen, también, riesgos ciertos a los bienes que la privacidad protege.

A propósito de la privacidad informacional, un uso desregulado de los datos provistos por las personas infectadas por COVID-19 puede implicar un riesgo a la privacidad física, en lugares donde no hay un marco jurídico robusto que regule el uso de estos datos. Esto no es solo un riesgo para países autoritarios, sino también para democracias, como demuestra el caso francés (Codaccioni, 2021).

En este sentido, creemos que el resguardo de la democracia, de la separación de poderes y de la sujeción de los actos de gobierno al imperio del derecho son fundamentales a la hora de establecer las condiciones apropiadas para un uso respetuoso de la privacidad y de los bienes morales que ella protege. Todo lo que implique un menoscabo de estas condiciones políticas y morales puede conllevar a, en un mediano o largo plazo, un riesgo para la privacidad. Por ello, el uso de mecanismos de almacenamiento descentralizado resulta coherente con esta exigencia, requiriéndose además la promesa explícita por parte del Estado de salvaguardar la confidencialidad de los datos.

4.2. Un uso éticamente responsable de los datos personales

El uso de datos personales a propósito del COVID-19 representa un desafío tanto para los organismos públicos como para las universidades y empresas privadas que colaboran con ellos. El uso que se les dé a los datos tiene una motivación y, cualquiera que ella sea, requiere de una reflexión ética, que es la que se ha intentado aportar en este artículo. Junto con las recomendaciones del apartado siguiente, es necesario que quienes toman decisiones de política pública sobre estos temas reconozcan los valores involucrados y las posibles consecuencias de esas políticas públicas para valores morales relevantes. Muchos de esos valores no son cuantificables, y de este modo, no pueden ser fácilmente objeto de la consideración técnica y científica. Sin embargo, en su consideración efectiva radica la protección de la privacidad y de los valores asociados a ella.

4.3. Recomendaciones para autoridades y cientificos

4.3.1. Autoridades

Las autoridades deberán establecer objetivos claros para estas tecnologías, en línea con la legislación vigente y el respeto por los derechos humanos, los que se fundan en los principios éticos (apartado 3.1) y los modelos de deliberación moral (apartado 3.2) que dotan de contenido a estos últimos. Deberán, asimismo, tener una adecuada visión de los riesgos a la privacidad (apartado 3.3.2), tanto para las personas como para las instituciones democráticas, que son la condición necesaria de un uso éticamente responsable de los datos en un contexto de pandemia. Para ello se sugiere el siguiente esquema de deliberación[9], basado en un triple análisis. El primer nivel del análisis versa sobre la utilidad de las aplicaciones de trazabilidad; el segundo, acerca de la viabilidad política de su uso; y el tercero, sobre las restricciones deontológicas en el uso de la aplicación.

Primer nivel de análisis: utilidad de la aplicación

1) ¿Es una solución necesaria?
   a. Sí, es necesaria para evitar contagios (y, consecuentemente, para evitar una sobrecarga del sistema sanitario y, en último término, salvar vidas).
   b. No es necesaria, dado que, o bien hay otras soluciones accesibles, o bien no aporta substantivamente a evitar contagios.
2) ¿Es una solución proporcionada?
   a. Sí, es una solución proporcional en cuanto a su utilidad para evitar contagios.
   b. En relación con los riesgos a la privacidad, no parece que sea proporcionada dado su efecto limitado para evitar contagios.

Segundo nivel de análisis: viabilidad política

3) ¿Existe una legislación robusta, completa y adecuada, aplicable a estas tecnologías?
   a. Sí, existe.
   b. No hay una legislación completa, pero sí hay un marco regulatorio general que puede adaptarse.
   c. No existe, y por tanto hay un riesgo de que haya muchas situaciones que no entren dentro de alguna regulación aplicable de manera clara.
4) ¿Existe un estado de derecho funcional?
   a. Sí, existe separación de poderes, y todas las acciones de los poderes públicos se encuentran sometidas al derecho y al control de las instancias respectivas.
   b. No, hay una débil separación de poderes, existe arbitrariedad en algunas actuaciones de los poderes públicos y no hay instancias de control definidas.
5) ¿Hay estabilidad política?
   a. Sí, hay un marco institucional que funciona y que regula la vida social de manera óptima.
   b. No, existe riesgo de cambio institucional por vías no establecidas.

Tercer nivel de análisis: restricciones deontológicas

6) ¿Es una aplicación voluntaria?
   a. Sí, es voluntario bajar la aplicación y utilizarla.
   b. No, es obligatoria y su no uso o uso inadecuado implica sanción.
7) ¿Es una aplicación transitoria?
   a. Sí, se establecen las condiciones en virtud de las cuales dejará de usarse o bien un periodo de término específico.
   b. No, su desarrollo no tiene fecha de término.
8) ¿Su uso requiere consentimiento?
   a. Sí, es necesario expresar consentimiento.
   b. No, no es necesario.
9) ¿Los datos del usuario son almacenados anónimamente?
   a. Sí, son resguardados anónimamente.
   b. No, la anonimidad de los datos no está garantizada.
10) ¿Puede el usuario disponer de sus datos?
   a. Sí, puede eliminarlos o compartirlos.
   b. No, no puede disponer de ellos.
11) ¿Tiene un propósito definido?
   a. Sí, tiene un propósito definido (notificar proximidad con un contacto positivo, monitorear el comportamiento de un caso positivo, verificar el cumplimiento de la cuarentena, etc.).
   b. No hay propósito definido.
12) ¿Monitorea otros comportamientos del usuario?
   a. Sí, monitorea otros comportamientos.
   b. No, posee un propósito específico y se limita a él.
13) ¿Es accesible para todos en igualdad de condiciones?
   a. Sí, está pensada para personas de todas las condiciones sociales, en un lenguaje accesible y bajo términos y condiciones comprensibles y aceptables para todos.
   b. No está disponible ni es accesible para todos los grupos de personas

9 El esquema elaborado toma como base el de Morley, Cowl, Taddeo y Floridi (Morley et al., 2020). El análisis nuestro difiere del anterior en cuanto plantea tres niveles a diferencia de los dos originales, los cuales están enfocados esencialmente en la aplicación de trazabilidad más que en las condiciones que la hacen necesaria epidemiológicamente (es decir, útil) y viable políticamente (es decir, desde el punto de vista del respeto a la privacidad y los bienes morales vinculados a ella).

El análisis propuesto parte desde el cuestionamiento a la necesidad de plantear, por motivos de utilidad en el combate a la pandemia, tecnologías de trazabilidad. Si la evaluación indica que no son necesarias en términos de utilidad, su implementación y desarrollo no estarán justificadas. Si lo estuvieran, es necesario resguardar la privacidad, de modo que el segundo nivel de análisis dice relación con las condiciones políticas que la hacen viable para este efecto. En tercer lugar, una vez que están dadas las condiciones políticas, es necesario plantearse las restricciones deontológicas que debería imponerse al desarrollo e implementación de estas tecnologías. Las condiciones de viabilidad política son relevantes para el juicio prudencial acerca de estas tecnologías, ya que, a falta de un marco político adecuado, el uso de los datos por parte de las autoridades, sin un control efectivo, puede llevar a los riesgos indirectos identificados más arriba. Las restricciones deontológicas, finalmente, garantizan que la aplicación que se elabore cumpla con los estándares mínimos planteados por los principios y los modelos de deliberación moral planteados en los apartados 3.1 y 3.2.

4.3.2. Científicos

Los científicos deberán tener una clara visión de las limitaciones a la investigación que impone la legislación vigente a propósito del uso de datos personales y sensibles (apartado 2.2), y de los límites que el consentimiento informado impone a los datos recolectados y, en consecuencia, a las conclusiones y recomendaciones que de ellos se derivan.

Como ha sido desarrollado en el apartado anterior, la aplicación de tecnologías de trazabilidad exige un esquema de deliberación. Si dicho procedimiento llega al tercer nivel, necesariamente la información que se recolectará estará afecta a lo que técnicamente se llama sesgo por consentimiento, que es un ejemplo de los sesgos de autoselección, lo que técnicamente implica la presencia de datos faltantes no-aleatorios. Esto trae como consecuencia que las recomendaciones de políticas sanitarias se basen en información sesgada, esto es, que solo es posible hacer recomendaciones con relación a la población que consintió en participar de la trazabilidad.

En la mayoría de las aplicaciones de trazabilidad que hemos tenido en cuenta en este análisis, el registro de los datos depende exclusivamente del usuario y del tiempo que consagra en enviar los reportes[10], lo cual tiene implicancias metodológicas: basta pensar que la configuración que los datos permiten construir puede cambiar de un momento a otro, lo que cuestiona la eficacia de una trazabilidad "en tiempo real". Sin embargo, la intención de la política sanitaria es salvaguardar la salud pública de toda una población. Por lo tanto, el objetivo de la trazabilidad se debilita precisamente por salvaguardar el consentimiento de los participantes. Es cierto, como lo sugieren Rothstein y Shoben (2013), que este problema puede ser solucionado usando las metodologías estadísticas de imputación de datos; pero las mismas requieren información adicional de los usuarios que no participaron: el hecho es que, al rehusar participar, dicha información no está disponible; y si lo estuviese, no puede ser utilizada porque los usuarios no consintieron en que se use parte o toda su información. Por tanto, el requerimiento ético impone reales limitaciones al análisis estadístico sobre el cual se construirán las recomendaciones de política sanitaria. Este es un problema que requiere nuevos desarrollos.

Lo anterior invita a los científicos a sistematizar una reflexión sobre el rol de la ciencia y su función propia en el contexto pandémico cuando ella se ve limitada por requerimientos éticos. Para esto, es necesario reflexionar sobre cómo la ciencia puede ser, por ejemplo, un medio para la realización de la plenitud social, en línea con los modelos de deliberación moral revisados.

Dos principios relevantes en el quehacer científico son el de confianza y el de precaución. En un contexto cada vez más escéptico del rol de la ciencia, es necesario que la actividad científica genere confianza en la ciudadanía (véase el principio de confianza). Una manera de realizar esto es integrar la evaluación científica del riesgo (véase el principio de precaución) con una concepción ética que complemente a la evaluación científica. Estos riesgos no son solamente aquellos mensurables, sino que son, también, aquellos que afectan bienes humanos básicos, sus posibilidades de realización, la igualdad de oportunidades y las instituciones democráticas. Otra

10 Técnicamente, esto corresponde al "cumplimiento del individuo en seguir el tratamiento" (compliance). Es sabido que la falta de compliance induce problemas de identificación, lo que al menos implica debilitar la calidad de los datos recolectados; ver Manski (2007).

manera es enfrentar el desafío que las limitaciones éticas imponen, generando agendas de investigación que superen las metodologías de análisis de datos que no suponen restricciones éticas.

Finalmente, y en particular respecto del uso de datos, recogemos la posibilidad de maximizar la utilidad de los datos, minimizando los riesgos a la privacidad, buscando cada vez mejores estrategias metodológicas y técnicas, que impidan el registro centralizado y la reutilización de los datos para otros fines. Esta maximización debe tener en cuenta las limitaciones deontológicas de los principios éticos y de los modelos de deliberación moral.

5. Conclusiones

En este artículo hemos presentado las tecnologías de trazabilidad para el combate al COVID-19 en Chile y, en particular, los desafíos éticos que supone su uso. Hemos descrito brevemente estas tecnologías y sus implicancias metodológicas en el tratamiento de datos y, en particular, para el consentimiento informado, que es una dimensión ética indispensable de cualquier uso ético de los datos (2.1). Hemos presentado la legislación nacional que regularía su uso (2.2). Vimos los principios éticos aplicables al análisis de estas tecnologías y el modo de operarlos integralmente en el análisis ético (3.1) y los modelos de deliberación moral que le dan contenido a estos principios (3.2). Finalmente, estudiamos la naturaleza moral de la privacidad y los riesgos para ella (3.3). El artículo termina con recomendaciones generales y específicas, tanto para autoridades como para científicos (apartado 4).

Si bien este artículo se ha focalizado en analizar éticamente el impacto de la trazabilidad de infectados por COVID-19 sobre la privacidad, presenta un esquema de deliberación que, combinado con los modelos éticos, resulta una herramienta eficaz para ser usada tanto por científicos como por hacedores de políticas públicas. Por otro lado, este trabajo ha enfatizado los impactos que tienen las consideraciones éticas sobre la metodología de análisis estadístico de los datos recolectados. Concretamente, si se recolectan datos de participantes que consientan en aquello, entonces nos encontramos ante un dilema: por un lado, se tienen datos afectados por el sesgo de selección y, por otro lado, las metodologías estadísticas que se puedan utilizar para "controlar" dicho sesgo no son factibles, pues el usarlas implica una violación a los participantes que no consintieron en participar. En cualquier caso, se requiere que la autoridad satisfaga dos requerimientos éticos: en primer lugar, la promesa de mantener la confidencialidad de los datos; y, por otro lado, asegurar que los derechos puestos bajo excepción se restaurarán una vez que finalice el estado de emergencia. No está de más insistir que aquí está en juego la confianza que los ciudadanos tienen en las instituciones públicas.

Referencias

Akinbi, A., Forshaw, M. y Blinkhorn, V., 2021. Contact Tracing Apps for the COVID-19 Pandemic: A Systematic Literature Review of Challenges and Future Directions for Neo-Liberal Societies. *Health Information Science and Systems,* 9(1), pp. 1-15.

Allen, A.L., 2003. Privacy. En H. LaFollette (editor). T*he Oxford Handbook of Practical Ethics.* Oxford: Oxford University Press.

Altmann, S., Milsom, L., Zillessen, H., Blasone, R., Gerdon, F., Bach, R., Kreuter, F., Nosenzo, D., Toussaert, S. y Abeler, J., 2020. Acceptability of App-Based Contact Tracing for COVID-19: Cross-Country Survey Evidence. *MedRxiv,* pp. 1-52.

Aquino, Santo Tomás, 2007. *Suma de Teologia I-II.* Madrid: Biblioteca de Autores Cristianos.

Aristóteles, 1998. *Ética A Nicómaco.* Madrid: Gredos.

Arriagada Bruneau, G., Gilthorpe, M. y Müller, V.C., 2020. Los imperativos éticos de la pandemia de COVID-19: un análisis desde la ética de los datos. *Veritas*, (46), pp. 13-35.

Baron, J., 2007. *Against Bioethics.* Cambridge: MIT Press.

Battaly, H., 2015. *Virtue.* Oxford: Polity.

Bentham, J., 1780. *An Introduction to the Principles of Morals and Legislation.* Nueva York: Dover Publications.

Benussi Díaz, C., 2020. Security Obligations on the Personal Data Processing in Chile: Current Regulatory Landscape and Pending Regulatory Challenges. *Revista Chilena de Derecho y Tecnología,* 9(1), 227-279.

Brandt, R.B., 1979. *A Theory of the Good and the Right.* Oxford: Prometheus Books.

Chappell, T.D.J., 1998. *Understanding Human Goods a Theory of Ethics.* Edimburgo: Edimburgh University Press.

Codaccioni, V., 2021. *La Societé de Vigilance.* Auto-Surveillance, Délation et Haines Sécuritaires. París: Textuel.

Cooperativa.cl., 2020. *Covid-19: MINSAL prepara nueva plataforma de trazabilidad a través de nube de Amazon.*

Davies, P. y Boruch, R., 2001. The Campbell Collaboration. Does for Public Policy What Cochrane Does for Health. *BMJ,* 323(7308), pp. 294-295.

Drew, D.A., Nguyen, L.H., Steves, C.J., Menni, C., Freydin, M., Varsavsky, T., Sudre, C.H., Cardoso, M.J., Ourselin, S., Wolf, J., Spector, T.D., y Chan, A.T., 2020. Rapid Implementation of Mobile Technology for Real-Time Epidemiology of COVID-19. *Science*, 368(6497), 1.362-1.367.

Eizagirre, A., 2011. La Precaución Como Principio de Acción Sostenible. *Isegoría*, (44), 303-324.

Farrell, M.D., 2003. *Ética en las relaciones internas e internacionales.* Barcelona: Gedisa.

Fienberg, S.E., 2005. Confidentiality and Disclosure Limitations. En L. Leonard (editor). *Encyclopedia of Social Measurement.* Nueva York: Elsevier.

Finnis, J., 1980. *Natural Law and Natural Rights.* Oxford: Clarendon Press.

Francis, L.P. y Francis, J.G., 2017. *Privacy. What Everyone Needs to Know.* Oxford: Oxford University Press.

Gan, N. y Culver, D., 2020. China está luchando contra el Coronavirus con un código QR digital. Así funciona. *CNN En Español.*

Gensler, H.J., 1998. *Ethics: A Contemporary Introduction.* Routledge.

Ginsberg, J., Mohebbi, M.H., Patel, R.S., Brammer, L., Smolinski, M.S. y Brilliant, L., 2009. Detecting Influenza Epidemics Using Search Engine Query Data. *Nature,* 457(7232), pp. 1.012-1.014.

Gkoulalas-Divanis, A. y Loukides, G., 2015. A Survey of Anonymization Algorithms for Electronic Health Records. En A. Gkoulalas-Divanis y G. Loukides (editores). *Medical Data Privacy Handbook.* Dordrecht: Springer.

Gómez-Lobo, A., 2002. *Morality and the Human Goods: An Introduction to Natural Law Ethics.* Washington, D. C.: Georgetown University Press.

González, J. y San Martín, E., 2020. Muchas curvas, misma información: sobre la indeterminación del modelo SIR y su uso en el contexto de la pandemia del COVID-19. *Laboratorio Interdisciplinario de Estadística Social.*

Griffin, J., 1986. *Well-Being: Its Meaning, Measurement and Moral Importance.* Oxford: Clarendon Press.

Hardin, R., 1988. *Morality Within the Limits of Reason.* Chicago: University of Chicago Press.

Hausman, D., McPherson, M. y Satz, D., 2017. Economic Analysis, Moral Philosophy, and Public Policy. 3rd ed. Cambridge: Cambridge University Press.

Hortal, A., 2002. *Ética general de las profesiones.* Bilbao: Descleé de Brower.

Hursthouse, R., 1999. *On Virtue Ethics.* Oxford: Oxford University Press.

Kahn, J.P., Ali, J., Barnhill, A., Cicero, A., Esmonde, K., Hood, A., Hutler, B., Regenberg, A., Watson, C. y Watson, M., 2020. *Digital Contact Tracing for Pandemic Response. Ethics and Governance Guidance.* J. P. Kahn (editor). Baltimore: Johns Hopkins University Press.

Kant, I., 2012. *Fundamentación para una metafísica de las costumbres.* Madrid: Alianza.

Lewis, D., 2021. Contact-Tracing Apps Help Reduce COVID Infections, Data Suggest. *Nature,* 591, pp. 18-19.

Lyons, D., 1965. *Forms and Limits of Utilitarianism.* Oxford: Clarendon Press.

Manski, C., 2007. *Identification for Prediction and Decision.* Cambridge: Harvard University Press.

Mayer-Schönberger, V. y Cukier, K., 2013. *Big Data. La revolución de los datos masivos.* Madrid: Turner.

McKinnon, C., 1999. *Character, Virtue Theories, and the Vices.* Toronto: Broadview Press.

El Mercurio, 2020. *Trazabilidad: la intrincada estrategia del MINSAL para detectar contagios que busca un nuevo impulso.*

Mill, J.S., 1863. *Utilitarianism.* Cambridge: Cambridge University Press.

Morley, J., Cowl, J., Taddeo, M. y Floridi, L., 2020. *Ethical Guidelines for SARS-CoV-2 Digital Tracking and Tracing Systems.*

Mulgan, T., 2001. *The Demands of Consequentialism.* Oxford: Oxford University Press.

Murphy, M.C., 2001. *Natural Law and Practical Rationality.* Cambridge: Cambridge University Press.

Nay, O., 2020. Can a Virus Undermine Human Rights? *The Lancet Public Health,* 5(5), e238-239.

Neves, N., Bitencourt, F. y Bitencourt, A., 2020. Ethical Dilemmas in COVID-19 Times: How to Decide Who Lives and Who Dies? *Revista da Associação Médica Brasileira* 66(11), pp. 106-111.

Nijsingh, N., Van Bergen, A. y Wild, V., 2020. Applying a Precautionary Approach to Mobile Contact Tracing for COVID-19: The Value of Reversibility. *Journal of Bioethical Inquiry.*

Oderberg, D.S., 2000. *Moral Theory: A Non-Consequentialist Approach.* Oxford: Wiley-Blackwell.

Rawls, J., 1995. *Teoría de la justicia.* México: Fondo de Cultura Económica.

Robert, R., Kentish-Barnes, N., Boyer, A., Laurent, A., Azoulay, E. y Reignier, J., 2020. Ethical Dilemmas Due to the Covid-19 Pandemic. *Annals of Intensive Care,* 10(1).

Rocher, L., Hendrickx, J.M. y De Montjoye, Y.A., 2019. Estimating the Success of Re-Identifications in Incomplete Datasets Using Generative Models. *Nature Communications,* 10(1), p. 3.069.

Rothstein, M.A. y Shoben, A.B., 2013. Does consent bias research? *The American Journal of Bioethics,* 13(4), pp. 27-37.

Russell, D.C., 2009. *Practical Intelligence and the Virtues.* Oxford: Oxford University Press.

Sen, A.K., 1991. *On Ethics and Economics.* Oxford: Wiley-Blackwell.

Sethuraman, N., Stanleyraj Jeremiah, S. y Ryo, A., 2020. Interpreting Diagnostic Tests for SARS-CoV-2. JAMA - *Journal of the American Medical Association,* 323(22), pp. 2.249-2.251.

Singer, P., 1979. *Practical Ethics.* Cambridge: Cambridge University Press.

Smart, J.J.C. y Williams, B., 1973. *Utilitarianism: For and Against.* Cambridge: Cambridge University Press.

Steinmann, M., Matei, S. y Collmann, J., 2016. A Theoretical Framework for Ethical Reflection in Big Data Research. En J. Collmann and S. A. Matei (Editores). *Ethical Reasoning in Big Data: An Exploratory Analysis.* Dordrecht: Springer.

Swanton, C., 2003. *Virtue Ethics: A Pluralistic View.* Oxford: Clarendon Press.

Sweeney, Y., 2020. Tracking the Debate on COVID-19 Surveillance Tools. *Nature Machine Intelligence,* 2(6), pp. 301-304.

Tollefsen, C.O., 2007. *Biomedical Research and Beyond: Expanding the Ethics of Inquiry.* Nueva York: Routledge.

Van Doremalen, N., Bushmaker, T., Morris, D.H., Holbrook, M.G., Gamble, A., Williamson, B.N., Tamin, A., Harcourt, J.L., Thornburg, N.J., Gerber, S.I., Lloyd-Smith, J.O., De Wit, E. y Munster, V.J., 2020. Aerosol and Surface Stability of SARS-CoV-2 as Compared with SARS-CoV-1. *New England Journal of Medicine,* 382(16), pp. 1.564-1.567.

Vardy, P. y Grosch, P., 1997. *The Puzzle of Ethics.* Londres: M.E. Sharpe.

Wymant, C., Ferretti, L., Tsallis, D., Charalambides, M., Abeler-Dörner, L., Bonsall, D., Hinch, R., Kendall, M., Milsom, L., Ayres, M., Holmes, C., Briers, M. y Fraser, C., 2021. The Epidemiological Impact of the NHS COVID-19 App. (septiembre 2020).

Zhang, R., Li, Y., Zhang, A.L., Wang, Y. y Molina, M.J., 2020. Identifying Airborne Transmission as the Dominant Route for the Spread of COVID-19. *Proceedings of the National Academy of Sciences of the United States of America,* 117(26), 14.857-14.863.

CÓMO CITAR ESTA PUBLICACIÓN:
Arancibia-Collao, F., y San Martín, E., 2021. El valor de la privacidad en el combate al COVID-19 en Chile: análisis de las tecnologías de trazabilidad. *Temas de la Agenda Pública,* 16(143), 1-17. Centro de Políticas Públicas UC.

PONTIFICIA
UNIVERSIDAD
CATÓLICA
DE CHILE