Desafíos de seguridad y privacidad en el diseño e implementación de soluciones de rastreo de proximidad

Gustavo Betarte*§, Juan Diego Campo*§, Andrea Delgado*§, Pablo Ezzatti*§, Álvaro Forteza†, Laura González*§, Álvaro Martín*§, Bárbara Muracciole‡, Raúl Ruggia*§
*Instituto de Computación, Facultad de Ingeniería, Universidad de la República
†Departamento de Economía, Facultad de Ciencias Sociales, Universidad de la República
‡Centro de Derecho Informático, Facultad de Derecho, Universidad de la República
§Área Informática, PEDECIBA

5 de mayo de 2020

***Resumen*—El impacto social y sanitario del COVID-19 es claro. El enfoque utilizado mayoritariamente para detener la epidemia es la aplicación de controles de una epidemia clásica, como son el aislamiento de casos, el monitoreo de contactos y la cuarentena, así como el distanciamiento físico y las medidas de higiene. La identificación de contactos asociados a un caso positivo es un proceso artesanal y proclive a errores y omisiones, dependiente principalmente de la memoria de la persona, que debe ser realizado por personal especializado. Estas limitaciones son particularmente graves en el caso de la pandemia actual, dado el elevado factor de contagio que presenta el COVID-19.**

En el entendido de que para el combate de esta, y otras epidemias futuras, es estratégico avanzar en el conocimiento y uso de las tecnologías digitales como herramientas de ayuda a los sistemas científicos biológicos, así como a las instituciones de salud, este documento presenta la posición que un equipo multi-disciplinario de docentes de la Universidad de la República toma ante la problemática del uso de tecnologías digitales para implementar rastreo de proximidad que mejoren la eficacia del proceso de detección de contagios.

El objetivo principal del presente esfuerzo es desarrollar un estudio profundo de las soluciones tecnológicas ya disponibles y sus impactos en los derechos y libertades, para entender su aplicación y posible adaptación a la realidad socio-económica y jurídica uruguaya.

***Index Terms*—COVID-19, rastreo de proximidad, soluciones tecnológicas, protección de datos personales, seguridad informática.**

I. Introducción

El impacto social y sanitario del COVID-19 es claro. Al día 4 de mayo de 2020 las infecciones mundiales por COVID-19 superan los 3.595.000 casos confirmados en 212 países, con 249.225 muertes. También hay aproximadamente 1.166.000 personas que se han recuperado completamente de esta enfermedad.

Actualmente no se cuenta con un tratamiento médico específico y no hay una estimación precisa del tiempo requerido para producir una vacuna, pero difícilmente esté disponible este año. El enfoque utilizado para detener el COVID-19 en Uruguay es la aplicación de controles de una epidemia clásica, como son el aislamiento de casos, el monitoreo de contactos y la cuarentena, así como el distanciamiento físico y las medidas de higiene.

La identificación no digital de contactos asociados a un caso positivo es un proceso artesanal y proclive a errores y omisiones, dependiente principalmente de la memoria de la persona. Además, requiere ser realizado por personal especialmente capacitado y no es eficaz para identificar contactos con desconocidos (por ejemplo en medios de transporte públicos, supermercados, etc). Estas limitaciones son particularmente graves en el caso de la pandemia actual, dado el elevado factor de contagio informado en la literatura ([1], [2] y, para una lista de 11 trabajos con estimaciones de los parámetros básicos, ver [3]). Por esta razón, en las últimas semanas han surgido múltiples iniciativas para el desarrollo de soluciones tecnológicas que mejoren la eficacia del proceso.

En la sección II se relevan brevemente las estrategias que se han seguido en el mundo para lidiar con esta situación, y el contexto en el cual, durante los meses de marzo y abril, ha tomado fuerza la idea de que las Tecnologías de la Información y la Comunicación (TIC) pueden ser utilizadas para complementar las medidas clásicas. En este sentido, a fines de abril ya están disponibles soluciones digitales de distinta naturaleza para el monitoreo, rastreo, prevención, diagnóstico y tratamiento de las infecciones [4, 5, 6, 7, 8, 9]. Algunas de estas soluciones están siendo usadas, con resultados prometedores, y si bien cuentan con funcionalidades que se podrían utilizar en Uruguay (para el COVID-19), no todas parecen ser *compatibles* con la realidad del país, por ejemplo, debido a sus implicancias en relación con la normativa nacional aplicable, especialmente en materia de protección de datos personales (Leyes Nº 18.331 de 11 de agosto de 2008 y Nº 19.670 de 15 de octubre de 2018, Decretos Nº 414/009 de 31 de agosto de 2009 y 64/020 de 17 de febrero de 2020). Notar que la implementación masiva de una solución digital vulnerable o invasiva puede poner en riesgo toda la estrategia de contención de la enfermedad con la ayuda de este tipo de aplicaciones [10, 11].

En el entendido de que para el combate de esta, y otras epidemias futuras, es estratégico avanzar en el conocimiento y uso de las tecnologías digitales como herramientas de ayuda a los sistemas científicos biológicos, así como a las instituciones de salud, hemos nucleado en torno a un proyecto de investigación, sometido al llamado CSIC COVID-19 [12], un equipo multi-disciplinario de docentes de la Universidad de la República con el objetivo de desarrollar un estudio profundo de las soluciones tecnológicas ya disponibles y sus impactos en los derechos y libertades, para entender su aplicación y posible adaptación a la realidad socio-económica y jurídica uruguaya.

En una primera fase el foco del trabajo es el estudio de aplicaciones para *rastreo de contactos/proximidad* (proximity/contact tracing), las cuales se describen en la sección III. Algunos de los desafíos más importantes en relación a este tipo de aplicaciones se detallan en la sección IV, seguidos de algunas consideraciones finales sobre la importancia de un análisis minucioso y una discusión profunda sobre estos aspectos.

II. Consideraciones preliminares

El rastreo de contactos/proximidad es un método que ha sido extensivamente usado, y su eficacia comprobada, para contener la propagación de enfermedades infecciosas. Con la aplicación de este método se busca informar a personas que han estado en riesgo de contagio lo antes posible para tomar las medidas adecuadas. En esta pandemia, en Uruguay dicha tarea se está realizando de forma artesanal mediante la entrevista y seguimiento de los vectores de contagio. En el caso de COVID-19, la transmisión se produce a través de gotas de saliva. Por lo tanto, los *contactos* a rastrear son personas que han estado a cierta distancia de una persona infectada, en el período de contagio.

La tasa exponencial de propagación del coronavirus y la carencia de mitigaciones confiables y duraderas sugiere que el virus continuará propagándose. Se estipula que las alternativas de freno de la propagación son que la comunidad internacional desarrolle inmunidad de rebaño (aproximadamente 50 % de infección entre la población), o se desarrolle una vacuna viable (a 12 meses de distancia según estimaciones optimistas [13]).

Mientras tanto, países de todo el mundo están luchando para reducir la tasa de infección, principalmente para contener el aumento de pacientes que necesitan atención de emergencia que ha estado abrumando los sistemas médicos. De hecho, proteger la viabilidad del sistema médico es fundamental, tanto para mantener baja la tasa de mortalidad entre los pacientes con COVID-19, como para preservar la capacidad de la sociedad para funcionar como un todo. Se utilizan dos tipos de mecanismos para minimizar las tasas de infección:

1. **Cuarentena general:** instruir a todas las personas de la comunidad a autoaislarse y restringir severamente sus movimientos.
2. **Cuarentena dirigida:** descubrimiento oportuno y aislamiento de individuos infectados y potencialmente infectados.

Hasta el momento la cuarentena general es el enfoque que ha sido más extensivamente adoptado por las autoridades gubernamentales a lo largo de todo el mundo. Sin embargo desde el primer momento se ha alertado sobre, y ya se comienza a hacer notar, los efectos perjudiciales que la cuarentena general tiene tanto para la vida de las personas (especialmente aquellas con antecedentes económicamente vulnerables) como para las economías nacionales en general. Un punto importante a remarcar es que la efectividad de esta medida depende de la cooperación completa de todos los segmentos de la población, algo que ya se está evidenciando se vuelve cada vez más desafiante con el tiempo.

El enfoque de cuarentena dirigido, por otro lado, parece prometedor para mantener la pandemia contenida mientras restringe los efectos más grandes en la población en general. Sin embargo, para ser efectivo este enfoque requiere:

1. Extensas pruebas para descubrir personas contagiosas lo antes posible.
2. Un mecanismo efectivo y oportuno para informar y aislar a las personas que estuvieron cerca de una persona contagiosa. Esto se hace más difícil dada la evidencia de que las personas se vuelven contagiosas por un largo período y en general antes de que sean sintomáticas (y en muchos casos nunca lo son), y que las superficies pueden permanecer contagiosas durante horas después del contacto [14, 15].

Las tasas de infección en los países que han logrado implementar estos dos elementos con éxito, como Corea del Sur, Taiwán o Singapur, se han mantenido relativamente bajas[1], con una perturbación económica y social correspondientemente más leve. Sin embargo, los países que implementaron el mecanismo de aislamiento específico lo hicieron a un alto costo para la privacidad de sus ciudadanos. Sus soluciones requerían referencias cruzadas centrales de historias precisas de ubicación de teléfonos celulares de todos sus ciudadanos contra las identidades de las personas infectadas. Esta información potencialmente personal se ha publicado con medidas parciales de *anonimato* ad hoc que han dejado vulnerable la información privada de individuos infectados y no infectados. Estas características han suscitado inquietudes y objeciones al despliegue en otros países y especialmente en los Estados Unidos (véase, por ejemplo, [16, 17]).

La tecnología, desplegada de manera responsable, puede hacer una contribución decisiva al combate de COVID-19. Los Estados Unidos, varios países europeos, así como empresas multinacionales están impulsando iniciativas con el objetivo de ofrecer una solución técnica que posibilite el rastreo de proximidad a través de teléfonos inteligentes. El foco no es rastrear a las personas, determinando quiénes son y dónde han estado, sino solamente rastrear el virus para informar sobre posibles riesgos de exposición.

Las características del Uruguay en infraestructura tecnológica, por ejemplo Planes Ceibal e Ibirapitá, Sistema Nacional Integrado de Salud (SNIS), Salud.uy, brindan oportunidades para el desarrollo de este tipo de soluciones. Recientemente se ha puesto a disposición la aplicación CoronavirusUY, que permite a una persona registrar indicadores para el monitoreo

[1] En el caso de Corea del Sur, luego de un inicio con crecimiento muy veloz de los casos, se logró revertir la situación.

por parte de personal médico, y así dar lugar a diagnóstico, planificación y monitoreo del tratamiento a distancia. Esta aplicación, al día de hoy (4 de mayo de 2020) ha sido descargada por más de 300 mil usuarios. En este contexto, un sistema diseñado con privacidad y seguridad en mente [18] para el rastreo de proximidad constituiría una herramienta complementaria, para el combate de la presente y futuras epidemias, cuidando los derechos y libertades de las personas.

III. Rastreo de proximidad: el problema y las soluciones tecnológicas

El objetivo principal de nuestro trabajo de investigación es identificar/proponer soluciones tecnológicas de rastreo de proximidad que contribuyan a la gestión de brotes de enfermedades infecciosas (centrados en COVID-19), que sean *compatibles* con la realidad uruguaya, en particular en relación a la infraestructura tecnológica disponible y la normativa aplicable. El proyecto tiene dos objetivos específicos:

1. Identificar opciones tecnológicas disponibles para el desarrollo de una aplicación de rastreo aplicable masivamente en Uruguay y evaluar las capacidades del país en relación a los requisitos de esas aplicaciones.
2. Analizar los desafíos en materia de seguridad informática y protección de datos personales involucrados en soluciones digitales disponibles y proponer soluciones específicas para su aplicación en el país en condiciones seguras.

Más específicamente, el propósito de nuestro trabajo es analizar soluciones tecnológicas basadas en dispositivos móviles para notificar de manera rápida y confiable a las personas sobre la co-localización pasada o presente con una persona o superficie infectada con un compromiso *mínimo* de la privacidad individual y sin mantener ninguna base de datos sobre personas infectadas o sus ubicaciones.

III-A. Sobre las tecnologías de localización

Los datos de *Global Positioning System (GPS)* han sido, y son, una herramienta natural para la (geo)localización. Sin embargo pueden ser un mecanismo relativamente pobre para determinar la co-localización cercana de individuos, especialmente en entornos densamente poblados: la efectividad del GPS está ampliamente influenciada por una serie de factores, como la densidad de edificios y las condiciones atmosféricas. En ambientes interiores, el GPS también tiene problemas para discernir efectivamente la separación vertical (por ejemplo, diferentes pisos de un edificio) o la separación horizontal a través de las paredes. Como tal, la información de co-localización generada solo por la señal de GPS está destinada a tener una alta tasa de falsos positivos, por lo que generalmente se combina en implementaciones prácticas con fuentes de localización adicionales, degradando aún más la privacidad de los participantes.

En contraste, las tecnologías de comunicación de corto alcance, como *Bluetooth Low Energy (BLE)*, son más propicias para determinar con precisión la co-localización de dispositivos. De hecho, en el caso de algunos dispositivos es posible reducir la potencia de transmisión de estas tecnologías para limitar la recepción con dispositivos de uso común a rangos tan cortos como 2 (dos) metros. Otro aspecto atractivo de las tecnologías de comunicación de corto alcance es que están naturalmente descentralizadas: la información se intercambia directamente entre dispositivos próximos sin ninguna intervención central.

La naturaleza de las tecnologías analizadas previamente ha llevado a la elaboración y propuesta de un esquema básico para la implementación de rastreo de proximidad:

1. cada dispositivo móvil participante transmite constantemente, a través de sus dispositivos de comunicación de corto alcance, un número aleatorio (identificador efímero) que cambia cada pocos minutos; simultáneamente, cada dispositivo registra los identificadores recibidos de los dispositivos vecinos,
2. tan pronto como el propietario de un dispositivo es notificado que ha sido diagnosticado positivo y fue potencialmente contagioso durante un cierto período de tiempo, se carga con su consentimiento los identificadores que su dispositivo transmitió durante ese período de tiempo en un registro público,
3. haciendo uso de ese registro público otros participantes pueden verificar si los identificadores que han recibido y recopilan coinciden con los identificadores en el registro público. Si se encuentra una coincidencia, el propietario sabe que debe hacerse la prueba lo antes posible.

Es importante notar que el esquema antes descrito, al igual que otras variantes similares, puede definirse de forma tal que solamente se notifica al usuario del dispositivo móvil la existencia de la co-localización, no la hora o la ubicación del evento de co-localización. Además, el registro público solo contiene identificadores aleatorios (pseudo)anonimizados. Este esquema, a pesar de capturar la esencia del problema a resolver, tiene una serie de debilidades, en relación en particular a la seguridad y protección de datos personales, que serán analizadas más adelante en este documento.

III-B. Enfoques y soluciones implementadas

En lo que va del año 2020 han surgido distintas iniciativas en relación al diseño, implementación y despliegue de tecnologías de rastreo de proximidad [19][20].

Por un lado, varios países han desarrollado y puesto en producción soluciones para ser utilizadas por su población. Algunos ejemplos de estas iniciativas son:

- China, Taiwán y Corea del Sur parecen estar centralizando y analizando datos de rastreo de teléfonos celulares para seguir los movimientos de personas infectadas y en cuarentena y notificar a otros de posible situación de co-localización. No se conocen detalles técnicos públicos de cómo funcionan estos sistemas.
- Singapur ha implementado recientemente su aplicación de teléfono celular TraceTogether [21] que utiliza Bluetooth e identificadores aleatorios similares al mecanismo descripto en la sección anterior. En el artículo [22] se presenta un análisis de los beneficios y los inconvenientes de la privacidad de TraceTogether. En particular, se señala que el sistema solo brinda privacidad limitada, en relación

al gobierno, a los usuarios infectados y a los ciudadanos co-localizados geográficamente.
- Israel también ha desplegado una aplicación de teléfono celular, llamada Hamagen [23], que descarga periódicamente a todos los teléfonos participantes una lista pseudoanonimizada de las rutas de todas las personas infectadas. Los teléfonos luego comparan localmente sus propias ubicaciones pasadas con las rutas infectadas.

Por otro lado, y dado el impacto que este tipo de aplicaciones puede tener en la privacidad individual, han surgido también soluciones más generales y globales que consideran la privacidad desde su diseño y apuntan a servir como base para la implementación de aplicaciones específicas (p. ej. en un país). Estas soluciones siguen distintos enfoques en cuanto a la tecnología base que utilizan y las responsabilidades de sus distintos componentes (aplicación móvil, servidor central), entre otros. Dentro de estas iniciativas se encuentran:

- El MIT tiene soluciones centradas en la privacidad [24, 25] que intentan difuminar los datos de ubicación del teléfono celular para mantener la privacidad del usuario y también para realizar un seguimiento de la ubicación que preserva la privacidad.
- La agencia de tecnología del gobierno de Singapur publicó el protocolo Bluetrace (sobre el cual se basa la aplicación TraceTogether) así como una implementación de referencia denominada OpenTrace, debido al interés de varios gobiernos en su aplicación [26].
- El grupo Covid-Watch [27] propuso una variante distribuida del enfoque TraceTogether. Según la descripción en su sitio web el esquema Covid-Watch puede ser susceptible a un ataque de enlace (ver Sección 5.2.2 de [20]).
- El grupo DP-3T [28] (Decentralized Privacy-Preserving Proximity Tracing) propone un esquema de solución para implementar rastreo de proximidad descentralizado que respeta los principios de privacidad desde el diseño y por defecto.
- En abril de 2020 Inria y Fraunhofer AISEC publicaron la primera versión del esquema ROBERT (ROBust and privacy-presERving proximity Tracing), como resultado de un trabajo colaborativo entre ambas instituciones [29].
- Más recientemente las empresas tecnológicas Apple Inc. y Google Inc. anunciaron [30] un esfuerzo conjunto para combatir la pandemia de COVID-19 para desarrollar una tecnología de rastreo de contactos para ayudar a los gobiernos y las agencias de salud a reducir la propagación del virus, tomando como criterio central la privacidad y seguridad del usuario. El anuncio de la asociación incluyó especificaciones técnicas de la tecnología planificada, que tiene un gran potencial para una adopción generalizada debido al alcance global de las dos compañías.

En el cuadro I se presenta un resumen de las principales características de las propuestas generales presentadas, en base a las especificaciones existentes, incluyendo el enlace al repositorio con el código fuente asociado, en caso de tenerlo.

Se puede observar que la mayoría de las propuestas se basan en la tecnología Bluetooth (solo [25] utiliza GPS), almacenando en el dispositivo móvil identificadores (ids, datos mínimos anonimizados). Varían en aspectos como la generación del identificador (solo en el dispositivo móvil o con participación del servidor central), en el período de tiempo en que se mantienen los registros, entre otros aspectos. Cuando una persona es confirmada positiva COVID-19, puede opcionalmente enviar los datos registrados en su celular (varían según la propuesta) al servidor central para que los contactos puedan ser puestos sobre aviso o chequear posible exposición.

Por su parte, en [25, 27, 28, 30] la verificación de exposición es realizada en el dispositivo móvil contra la lista de positivos (ids) obtenida desde el servidor central. Por el contrario, en [26, 29] la verificación de exposición es realizada en el servidor central y se envía aviso a la aplicación móvil. Todas las propuestas (con código) incluyen aplicaciones móviles para los sistemas operativos IOS y Android. En el caso de la iniciativa Apple & Google se trata de una API (Application Programming Inteface) para utilizar en desarrollos de aplicaciones específicas.

Notar que la mayoría de estos desarrollos y trabajos son muy recientes. Como también lo son diversos trabajos que ya están circulando donde se presentan análisis de seguridad que señalan vulnerabilidades de privacidad que varias de las soluciones arriba listadas conllevan, incluida la tecnología de rastreo de proximidad que implementarán Google y Apple [10].

Interesa asimismo hacer notar que existe un sustancial esfuerzo de investigación desarrollado sobre la cuestión relacionada con la privacidad del testeo de proximidad (ver, por ejemplo, [31, 32]).

IV. Desafíos y principios

La eficacia de cualquier solución tecnológica de rastreo descansa en una amplia y rápida adopción por parte de la población. A su vez, la solución que se adopte deberá respetar principios y derechos, tales como la protección de los datos personales y la participación voluntaria y debidamente informada de los usuarios (la tecnología a adoptar deberá requerir -en principio- el previo consentimiento informado del usuario). Todo esto implica fuertes desafíos para el desarrollo de esta política pública, la cual deberá contar con un amplio respaldo social y político.

IV-A. El derecho a la protección de datos personales

A la complejidad tecnológica se suman problemas éticos y políticos. Recientemente, Yehuda Lindell, CEO y cofundador de Unbound Tech, y Matt Green, Professor of Computer Science, Johns Hopkins University, brindaron un webinar [33] discutiendo los desafíos científicos y políticos asociados con el rastreo de proximidad en el contexto de COVID-19.

El día 19 de abril pasado, investigadores de renombre internacional en el área de la seguridad informática y la privacidad lanzaron una *declaración conjunta* [34] en la que manifiestan su preocupación en que a través del abuso de algunas soluciones a la crisis del coronavirus puedan dar como resultado sistemas que permitan una vigilancia sin precedentes de la sociedad en general.

Cuadro I
PRINCIPALES CARACTERÍSTICAS DE PROPUESTAS EXISTENTES

Propuestas	Tecnología	Aplicación Móvil	Servidor back-end	Verificación de exposición	Almacenamiento y transmisión de datos	Código
Private Kit: Safe Paths (MIT) [25]	GPS	Registra datos de geolocalización y chequea si tuvo exposición	Recibe datos de usuario positivo, comparte ubicaciones anonimizadas con todos los usuarios	Dispositivo móvil	Se guardan en dispositivo móvil y se transmiten desde el back-end anonimizados y encriptados	https://github.com/tripleblindmarket/covid-safe-paths
Open Trace (Blue trace) [26]	Bluetooth	Registra datos (id temporario generado encriptando id de usuario con llave privada en poder del ministerio de salud, que es re-generado)	Genera y registra id de usuario aleatorio asociado al número celular, recibe datos de usuario positivo (ids, con código autorización), verifica contactos para aviso de exposición	Back-end	Se guardan en dispositivo móvil, en servidor el id de usuario asociado al número celular y lista de contactos expuestos	https://github.com/OpenTrace-community
Covid Watch [27]	Bluetooth	Registra datos (número aleatorio enviado y recibido), recibe lista de positivos y verifica exposición	Recibe datos de usuario positivo (ids emitidos y recibidos, con número de permiso otorgado), registra y envía lista de positivos	Dispositivo móvil	Se guardan en dispositivo móvil, en servidor lista de positivos, número de permiso se elimina	https://github.com/covid19risk
DP-3T [28]	Bluetooth	Registra datos (id temporario regenerado periódicamente generado en base a clave secreta), recibe par (clave, día) de positivos para regenerar ids y verifica exposición	Recibe par (clave, día) de usuario positivo (con token otorgado por autoridades de salud) y re-envía a aplicaciones	Dispositivo móvil	Se guardan en dispositivo móvil, en servidor pares (clave, día) de positivos por tiempo x	https://github.com/DP-3T
ROBERT [29]	Bluetooth	Se registra con back-end, recibe ids temporarios a emitir, registra datos (ids). Periódicamente chequea con back-end si estuvo expuesto	Genera y registra id permanente por aplicación, clave simétrica e ids temporarios a emitir. Recibe datos de usuario positivo (ids, canal anónimo), desencripta id permanentes y marca expuestos	Back-end	Se guardan en dispositivo móvil, en servidor lista de contactos expuestos, comunicaciones encriptadas	Sin código aún
Apple & Google [30]	Bluetooth	Registra datos (id temporario regenerado periódicamente en base a clave temporaria diaria), obtiene lista de positivos y verifica exposición	Recibe datos de positivo (ids), registra y comparte datos en lista de positivos	Dispositivo móvil	Se guardan en dispositivo móvil, en servidor lista de positivos	Sin código aún. API para desarrollar aplicaciones específicas.

Asimismo, el día 20 de marzo pasado el European Data Protection Board (EDPB) también manifestó en una declaración [35] su preocupación en relación al manejo de los datos personales en el contexto de la gestión de la pandemia del COVID-19. En particular, en una carta enviada a Olivier Micol (Head of the Unit European Commision) el EDBP manifiesta que *"las soluciones técnicas previstas deben ser examinadas en detalle, caso por caso"* [36].

La expresión de estas inquietudes tiene su origen no en la tecnología en sí misma, sino en el impacto negativo que su utilización pueda tener en el derecho a la protección de datos de los usuarios y, consecuentemente, en otros derechos y libertades. Recordemos que el derecho a la protección de datos personales es un derecho fundamental que se encuentra reconocido en los instrumentos jurídicos más importantes en la materia.

En el ámbito internacional cabe mencionar la Declaración Universal de Derechos Humanos, de 10 de diciembre de 1948, que en su artículo 12 dispone "[n]adie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques". Similar texto ha sido recogido por el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos, de 16 de diciembre de 1966. En los ámbitos regionales, la Convención Americana de Derechos Humanos (Pacto de San José de Costa Rica) en su artículo 11 establece "[t]oda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad. Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques". En el mismo sentido, el Convenio Europeo de Derechos Humanos dispone en su artículo 8 "[t]oda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia". De igual forma se pronuncia la Carta de los Derechos Fundamentales de la Unión Europea y el Tratado de Lisboa.

En Uruguay el derecho a la protección de datos personales se encuentra principalmente regulado por la Ley Nº 18.331 que lo reconoce como "inherente a la persona humana, por lo que está comprendido en el artículo 72 de la Constitución de la República" (artículo 1º).

Esta norma se estructura en torno a dos pilares que son: a) los principios enunciados en su artículo 5 (legalidad, veracidad, finalidad, previo consentimiento informado, seguridad de los datos, reserva y responsabilidad), y b) los derechos consagrados en los artículos 13 a 17 (información, acceso, rectificación, actualización, inclusión, supresión, impugnación a las valoraciones personales derivadas de tratamientos automatizados con efectos jurídicos y comunicación de datos).

Instituye al consentimiento expreso como regla general, y expreso y escrito para la categoría de datos sensibles (aquellos que revelen origen racial y étnico, preferencias políticas, convicciones religiosas o morales, afiliación sindical e informaciones referentes a la salud o a la vida sexual). Asimismo, establece categorías de datos especialmente protegidos, dentro de los cuales se encuentran los datos sensibles, datos relativos a la salud y a las telecomunicaciones, entre otros.

Sin perjuicio de la regla general, y en el entendido que no existen derechos absolutos, el legislador ha previsto excepciones en las que la licitud del tratamiento no reposa en el consentimiento, dentro de las cuales se encuentran a texto expreso las razones sanitarias, de emergencia o para la realización de estudios epidemiológicos (artículos 9 y 17 de la ante citada Ley).

Este derecho supone el poder de disposición de nuestra información personal frente al Estado y los particulares. Su respeto implica no sólo su propia tutela, sino la de un conjunto de otros derechos tales como la libertad ambulatoria, de reunión, de asociación, el respeto del honor y de la dignidad, que podrían verse comprometidos, puesto que violentar la protección de datos suele ser la puerta hacia otras vulneraciones. Por ello, localizaciones o rastreos a gran escala pueden implicar vigilancia masiva que afecte la libertad ambulatoria y revele datos relacionados con actividades de reunión y posiblemente asociación. Los datos de salud –particularmente en casos de pandemias- pueden generar estigmas que conlleven discriminación. Es por lo tanto crucial que nos ocupemos de conjugar tecnología y Derecho en instancias y contextos como los actuales.

Es importante en este punto hacer notar que la normativa uruguaya en materia de protección de datos personales se ajusta fuertemente a los principios y lineamientos de las disposiciones y doctrinas más recientes y relevantes.

En efecto, tanto la sanción de la Ley Nº 19.670, como del Decreto Nº 64/020, muestran un claro alineamiento al Reglamento Europeo 2016/679 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 (GDPR por sus siglas en inglés), los Estándares en Protección de Datos Personales para los Estados Iberoamericanos emitidos por la Red Iberoamericana de Protección de Datos en junio de 2017, el Convenio Nº 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, su Protocolo Adicional de 8 de noviembre de 2001, ambos aprobados por la Ley Nº 19.030 de 27 de diciembre de 2012, y el Protocolo de Modernización del citado Convenio aprobado por el Comité de Ministros del Consejo de Europa el 18 de mayo de 2018, suscripto por nuestro país el 10 de octubre de 2018.

Esto implica que los requerimientos jurídicos nacionales están a nivel de los más altos estándares internacionales y suponen mínimos que deben ser cumplidos, por lo que no se trata únicamente de buenas o mejores prácticas a considerar, sino de obligaciones legales a contemplar en los requerimientos técnicos. Muestra de ello son las nuevas exigencias en materia de seguridad, que imponen a los responsables y encargados de tratamiento de datos personales adoptar las medidas técnicas y organizativas necesarias para conservar la integridad, confidencialidad y disponibilidad de la información y las exigencia de contención de incidentes y notificación de vulneraciones de seguridad al Regulador y a los titulares, cuando corresponda. Asimismo, esta adecuación se traduce en el fortalecimiento legal y reglamentario del principio de responsabilidad, en

su evolución a la responsabilidad demostrada, que impone a los responsables y encargados demostrar que cumplen con la legislación vigente. Este principio se traduce en medidas de responsabilidad proactiva que deben ser adoptadas, documentadas, revisadas periódicamente y evaluadas en su efectividad. Nos referimos concretamente a la Evaluación de Impacto en la protección de datos personales (EIPD) y a la Privacidad por Diseño y por Defecto, ambas, enteramente aplicables y determinantes para valorar el uso de aplicaciones, como las que nos ocupan.

De acuerdo con las definiciones dadas por la Unidad Reguladora y de Control de Datos Personales [37], la EIPD es "un proceso que las organizaciones deben efectuar para identificar y tratar los riesgos que puedan producir sus actividades habituales, sus nuevos proyectos o sus políticas corporativas cuando involucran el tratamiento de datos personales."

Por su parte, la Privacidad por Diseño es considerada como "un enfoque que considera que la protección de la privacidad debe estar integrada con el sistema, aplicación o dispositivo desde su diseño. Desde esta perspectiva, la protección de los datos personales no debe ser analizada a posteriori, como si se tratara de un anexo, sino que debe estar presente en todas las etapas del proceso", y la Privacidad por Defecto es el "enfoque que exige que, por defecto, solo sean objeto de tratamiento aquellos datos personales que sean necesarios para cada una de las finalidades específicas del tratamiento."[37]

IV-B. Principios y requerimientos tecnológicos

Cada una de las soluciones técnicas para aplicaciones de rastreo de proximidad mencionadas en la sección III se basa en una arquitectura compleja, que incluye al menos las aplicaciones instaladas en los dispositivos móviles de los usuarios y los sistemas de *back-end*[2] administrados por las autoridades.

A continuación se presentan principios y criterios que están siendo discutidos por la comunidad internacional y que se entiende deberían ser tenidos en cuenta para el diseño e implementación de soluciones tecnológicas de rastreo de colocalización. Realizar un estudio en profundidad del alcance de estos requerimientos y la forma en que deben ser respetados por soluciones que intenten contribuir a la gestión de la crisis pandémica, en particular en nuestro país, constituyen los desafíos principales en los que se concentrará el trabajo de investigación a desarrollar en nuestro proyecto.

IV-B1. Principio de minimización de datos: La gran mayoría de los esquemas y soluciones que se han propuesto reconocen la importancia de respetar el principio de minimización de datos del GDPR. Si el único objetivo de la aplicación es notificar a las personas que han estado en contacto con personas diagnosticadas con COVID positivo, entonces la aplicación debe recopilar y procesar solo los datos necesarios para este propósito, por lo tanto, datos sobre la proximidad de las personas. No se debe recopilar ninguna otra información, como la ubicación de los usuarios, números de teléfono, nombres o cualquier otra información que pueda usarse para identificar a la persona.

Cabe destacar, que el principio de minimización ha sido expresamente recogido por el literal a) del artículo 8 del Decreto Nº 64/020, como una medida de aplicación de la Privacidad por Diseño, lo que lo transforma en una exigencia legal y reglamentaria ineludible para cualquier aplicación que pretenda utilizarse.

IV-B2. Sobre la (des)centralización de la verificación de contactos: Como se ha descrito en la sección precedente, el enfoque seguido para procesar la verificación de contactos difiere en las soluciones propuestas. En particular, y en lo que refiere a una de las iniciativas europeas más importantes, como lo es DP-3T, esta posiciona lo que llama un enfoque descentralizado, entendiendo por descentralización el hecho de que la determinación de si el propietario de un dispositivo ha estado expuesto a un posible contagio es computada en el dispositivo.

Los promotores del protocolo ROBERT, otra iniciativa europea muy importante, argumentan que un enfoque totalmente descentralizado no es realista para el rastreo de proximidad, entendiendo por descentralización confiar solamente en el intercambio de datos entre aplicaciones para informar quién está en riesgo o no. En particular se señala que dado que la recepción de estas notificaciones dependería de la proximidad actual entre las personas, lo que podría implicar una entrega de información lenta e incompleta, no sería una solución segura y confiable.

La mayoría de las soluciones analizadas involucran un servidor que centraliza y comparte información con las aplicaciones. Lo que se torna entonces esencial son las decisiones que se tomen en los siguientes dos aspectos de diseño: (1) cómo distribuir los datos entre el servidor y el dispositivo y (2) dónde se verifica el estado del usuario (en riesgo o no).

Con respecto al primer aspecto, para cumplir con el principio de minimización de datos exigido por la normativa nacional e internacional citada, la información de contacto recopilada por la aplicación debe almacenarse solo localmente (en el dispositivo móvil). Para proporcionar una notificación rápida y confiable a los usuarios en riesgo, solo los datos que permitan establecer contactos de proximidad de personas con diagnóstico positivo deben enviarse al sistema de back-end. La mayoría de las soluciones siguen este enfoque.

Por lo tanto, podría decirse que el debate sobre los enfoques *centralizado* versus *descentralizado* se refiere esencialmente al segundo aspecto de diseño, es decir, dónde se verifica el estado del usuario: esta verificación se realiza en el dispositivo del usuario en las llamadas soluciones descentralizadas y en el sistema de back-end de lo contrario.

Si la verificación se realiza localmente (en forma descentralizada), todas las aplicaciones deben recibir información sobre los usuarios diagnosticados como positivos para verificar si alguna de ellas forma parte de su lista de contactos. Algunos autores, como [11], creen que con este enfoque existe el peligro de que usuarios maliciosos detecten que una persona ha sido diagnosticada como positiva. Esto puede conducir a la estigmatización, situación que muchos expertos consideran

[2]Los *sistemas de back-end* implementan operaciones comunes a todos los usuarios a través de software que opera en infraestructura informática de gran capacidad. Son fundamentales para asegurar una alta disponibilidad y eficiencia del sistema de gestión de proximidad.

un riesgo importante para las aplicaciones de rastreo de contactos [38].

Por otro lado, según los autores que proponen alternativas distribuidas [28], realizar esta verificación en un sistema de back-end centralizado podría allanar el camino a la vigilancia masiva (que es el segundo problema ético identificado en [38]) a través de lo que se denomina *function creep* (utilizar la tecnología para propósitos que no estaban originalmente definidos).

También es importante tener en cuenta que no debe almacenarse en el sistema de back-end ninguna información que permita identificar a un usuario con diagnóstico positivo. Para esto, dicho sistema debe estar asegurado, auditado y controlado regularmente por autoridades e instituciones independientes de confianza.

Por lo tanto, el impacto en la privacidad de las elecciones entre cálculos locales y centrales no es tan simple como parece, dado que ninguna de las soluciones es pura en sí misma y tienen que combinarse necesariamente. No es correcto considerar que la opción descentralizada implica que sólo se maneje información localizada en el terminal del usuario y que éste tiene absoluto control de los datos y de la opción de salirse del sistema de rastreo. Tampoco que esta solución garantiza el anonimato. Siempre existen servidores operando sistemas de back-end en forma central (o sea común a todos los usuarios), para lo cual es crucial determinar su ubicación territorial y su control, por lo que la anonimización total en el sentido de ruptura absoluta de vínculo entre el titular y sus datos, es técnicamente imposible de garantizar. El logro de la eficacia del sistema y de protección de la privacidad dependerá en gran medida de la implementación de los sistemas de back-end (que pueden estar distribuidos), de quiénes administran los datos, y de la aplicación de mecanismos de auditoría y control que generen confianza.

IV-B3. Relevancia del análisis de riesgos: Teniendo en cuenta que las soluciones implicarían un servidor central y aplicaciones ejecutando en los dispositivos de las personas, entendemos que un punto esencial es desarrollar un análisis preciso de la privacidad y los impactos éticos de cada solución.

Este análisis de riesgos debería realizarse en el marco de una Evaluación de Impacto en la Protección de Datos, de acuerdo con lo dispuesto en el artículo 12 de la Ley Nº 18.331, en la redacción dada por el artículo 39 de la Ley Nº 19.670 y artículo 6 del Decreto Nº 64/020.

La EIPD procede en forma previa a la puesta en funcionamiento y deberá considerar, como mínimo, los siguientes ejes transversales:

- base de licitud del tratamiento,
- existencia de comunicación de datos,
- transferencia internacional de datos,
- medidas de seguridad adoptadas,
- proporcionalidad entre el tratamiento y la finalidad perseguida,
- uso de datos especialmente protegidos (datos de localización)
- uso de datos sensibles (datos de salud),
- cumplimiento de los principios, y
- ejercicio de los derechos

En [39] los autores estipulan que un análisis de riesgos integral debería abordar los siguientes problemas clave:

- ¿Qué datos se recopilan y cómo se protegen? ¿Es posible relacionar los datos con personas? ¿Dónde se almacenan estos datos?
- ¿Cuáles son las posibles fuentes de riesgo (por ejemplo, autoridad, usuarios de la aplicación, terceros maliciosos, etc.)?
- ¿Cuáles son las capacidades de estas fuentes de riesgo? Por ejemplo, ¿pueden modificar la aplicación o instalar antenas de comunicación inalámbrica?
- ¿Cuáles podrían ser las intenciones de estas fuentes de riesgo? Por ejemplo, ¿es posible que quieran comprometer el sistema o saber qué usuarios han sido diagnosticados como positivos?
- ¿Qué tan difícil es que tales fuentes de riesgo alcancen sus metas dadas sus capacidades?
- ¿Cuál es la robustez, calidad y confiabilidad de la aplicación y su valor agregado para combatir COVID-19?
- Teniendo en cuenta las respuestas a las preguntas anteriores, ¿cuáles serían los impactos éticos y de privacidad de posibles infracciones, incluida su probabilidad, gravedad y alcance?

En el documento [40], desde el equipo del proyecto DP-3T se anticipan respuestas a algunas de las cuestiones claves listadas precedentemente. Dicho artículo resume los resultados de un exhaustivo análisis de privacidad y seguridad de sistemas de rastreo de proximidad digital, y en particular del que el equipo ha llevado a cabo en las últimas semanas. En él se enumera riesgos inherentes a cualquier sistema de rastreo de proximidad digital, y especialmente aquellos que se basan en intercambio de identificadores generados con tecnología Bluetooth entre dispositivos móviles.

Interesa destacar algunas de las conclusiones generales a las que se arriban:

1. Todos los sistemas de rastreo de proximidad que notifican a los usuarios que están en riesgo permiten que un adversario motivado identifique a las personas infectadas con las que ha estado muy cerca. Este riesgo es una consecuencia de la funcionalidad básica de rastreo de proximidad y no depende de ninguna elección de diseño o detalles de implementación.
2. En todos los sistemas de rastreo de proximidad basados en mediciones Bluetooth existe el riesgo que un adversario haciendo uso de una antena potente, pueda activar alertas falsas sobre encuentros con una persona infectada que no reflejan la proximidad física del mundo real.
3. Todos los sistemas de rastreo de proximidad que se comunican con un servidor pueden potencialmente revelar las identidades de las personas infectadas al proveedor de red y al servidor si no se toman los recaudos apropiados.

Notar que los sistemas centralizados, como el candidato ROBERT para PEPP-PT (Pan European Privacy-Preserving Proximity Tracing) [41] y los sistemas descentralizados propuestos por el consorcio DP-3T o Apple/Google, son ejemplos de tales sistemas.

IV-B4. Federación e interoperabilidad: Considerando la movilidad de personas entre países, varias de las soluciones brindan propuestas para realizar el rastreo de proximidad a través de fronteras. En [29] se propone una arquitectura distribuida y federada donde los países pueden utilizar sus propios back-ends y aplicaciones. Por otro lado, en [26] se brindan principios guía en cuanto a los algoritmos a utilizar y el intercambio de datos, entre otros. En general, estas soluciones plantean desafíos interesantes tanto a nivel de interoperabilidad como de privacidad dado que los modelos y tecnologías utilizados por las soluciones, así como la normativa aplicable, puede variar considerablemente entre países. Asimismo, el sistema de back-end podría basarse en una solución federada.

V. Consideraciones finales

Entendemos que el debate sobre las aplicaciones de rastreo de proximidad es de gran importancia para el Uruguay como parte de las medidas para prevenir la propagación del COVID-19, y para garantizar los derechos fundamentales de las personas que residen en el país. Subrayamos la importancia de este debate y alentamos a comparar soluciones técnicas basadas en los principios delineados en la sección IV, sin perder el foco que lo que se pretende tutelar es el derecho a la vida y que el contexto exige el auxilio tecnológico para lograrlo.

En el entendido de que no es posible garantizar la utilización de tecnología exenta de riesgos, este trabajo busca aunar esfuerzos en procura de identificar rápidamente una solución tecnológica que ayude a prevenir, y por ende proteger, la vida y salud de los habitantes de nuestro país, con el menor riesgo e impacto en el resto de sus derechos.

La característica de excepcionalidad no solamente aplica a la situación epidemiológica que está viviendo la humanidad entera y a nuestra predisposición a alentar el diseño, implementación y despliegue de tecnología para su combate, sino también a la convergencia de esfuerzos científicos y académicos para su desarrollo. Muy raramente se presenta la oportunidad de poner a disposición de nuestra sociedad, una herramienta tecnológica cuyo comportamiento esté siendo objeto de tanto esfuerzo de estudio y evaluación por investigadores y técnicos de distintas disciplinas, en todo el mundo, en un plazo tan corto de tiempo.

En este marco, consideramos que el aporte académico de la Universidad de la República puede contribuir al diseño y la implementación de estos mecanismos excepcionales aportando garantías a la población.

Es de esperar que en el correr de nuestro trabajo de investigación surjan requerimientos adicionales a tener en cuenta en el momento de diseñar e implementar soluciones que puedan ser desplegadas para su uso en nuestro país. No obstante, es posible adelantar que la proporcionalidad entre los medios empleados y los fines perseguidos, la transparencia en la elección de la herramienta, el contralor constante por un equipo multidisciplinario en la implementación y uso inmediato, así como en el tratamiento posterior de la información y utilización de la tecnología desplegada, serán lineamientos claves a respetarse en todas las hipótesis de trabajo.

Referencias

[1] L. Ferretti *et al.*, "Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing," *Science*, 2020. [Online]. Disponible: https://doi.org/10.1126/science.abb6936

[2] R. Li *et al.*, "Substantial undocumented infection facilitates the rapid dissemination of novel coronavirus (SARS-CoV2)," *Science*, 2020. [Online]. Disponible: https://doi.org/10.1126/science.abb3221

[3] G. Goh, "Epidemic Calculator," Tech. Rep., 2020. [Online]. Disponible: https://gabgoh.github.io/COVID/ (Accedido: 4 de mayo de 2020).

[4] K. Boulos *et al.*, "Geographical tracking and mapping of coronavirus disease," *International journal of health geographics*, vol. 19, no. 1, 2020. [Online]. Disponible: https://doi.org/10.1186/s12942-020-00202-8

[5] D. Tom-Aba *et al.*, "Assessing the concepts and designs of 58 mobile apps for the management of the 2014-2015 west Africa Ebola outbreak: Systematic review," *JMIR public health and surveillance*, vol. 4, no. 4, 2018. [Online]. Disponible: https://doi.org/10.2196/publichealth.9015

[6] A. Moodley *et al.*, "Review of infectious diseases applications for iphone/ipad and android: from pocket to patient. clinical infectious diseases," *Clinical infectious diseases*, 2013. [Online]. Disponible: https://doi.org/10.1093/cid/cit455

[7] B. Mohanty *et al.*, "Use of mobile apps for epidemic surveillance and response – availability and gaps." *Global Biosecurity*, vol. 1, no. 2, 2019. [Online]. Disponible: http://doi.org/10.31646/gbio.39

[8] J. Choi *et al.*, "Web-based infectious disease surveillance systems and public health perspectives: a systematic review." *BMC public health*, vol. 1, no. 16, 2016. [Online]. Disponible: https://doi.org/10.1186/s12889-016-3893-0

[9] SORMAS, "Surveillance outbreak response management and analysis system," Tech. Rep., 2020. [Online]. Disponible: https://sormasorg.helmholtz-hzi.de/About_SORMAS.html. (Accedido: 4 de mayo de 2020).

[10] Y. Gvili, "Security Analysis of the Covid-19 Contact Tracing Specifications by Apple Inc. and Google Inc." Cryptomnium LLC, Tech. Rep., 2020. [Online]. Disponible: https://eprint.iacr.org/2020/428 (Accedido: 4 de mayo de 2020).

[11] S. Vaudenay, "Analysis of DP3T: Between Scylla and Charybdis," EFPL, Tech. Rep., 2020. [Online]. Disponible: https://eprint.iacr.org/2020/399 (Accedido: 4 de mayo de 2020).

[12] G. Betarte, J. D. Campo, A. Delgado, P. Ezzatti, A. Forteza, L. González, A. Martín, B. Muracciole, and R. Ruggia, "Métodos y técnicas para soporte automatizado de la gestión de brotes de enfermedades infecciosas," Proyecto postulado al Llamado CSIC: Conocimiento especializado para enfrentar la emergencia planteada por el COVID 19 y sus impactos, Tech. Rep., April 2020.

[13] C. Korman, "How long will it take to develop a coronavirus vaccine?" The New Yorker, March 2020.

[14] C. Rothe *et al.*, "Transmission of 2019-nCoV infection from an asymptomatic contact in Germany," *New England Journal of Medicine*, vol. 10, no. 382, pp. 970–971, 2020.

[15] T. Newman, "Covid-19: Study estimates rate of silent transmission," Medical News Today, March 2020.

[16] Y. Lee, "Taiwan's new 'electronic fence' for quarantines leads wave of virus monitoring," Reuters Technology News, March 2020. [Online]. Disponible: https://www.reuters.com/article/us-health-coronavirus-taiwan-surveillanc/taiwans-new-electronic-fence-for-quarantines-leads-wave-of-virus-monitoring-idUSKBN2170SK (Accedido: 4 de mayo de 2020).

[17] E. J. Markey, "Letter to the US Chief Technology Officer," March 2020. [Online]. Disponible: https://www.markey.senate.gov/imo/media/doc/Markey%20Letter%20-%20OSTP%20Location%20Data%203.18.20.pdf (Accedido: 4 de mayo de 2020).

[18] A. Cavoukian, "Global privacy and security, by design: Turning the Privacy vs. Security paradigm on its head," *Health Technology*, 2017.

[19] A. D. Carli, M. Franco, A. Gassmann, C. Killer, B. Rodrigues, E. Scheid, D. Schoenbaechler, and B. Stiller, "Wetrace – a privacy-preserving mobile covid-19 tracing approach and application," Tech. Rep., 2020. [Online]. Disponible: https://arxiv.org/pdf/2004.08812.pdf

[20] R. Canetti *et al.*, "Anonymous Collocation Discovery: Harnessing Privacy to Tame the Coronavirus," Tech. Rep., 2020. [Online]. Disponible: https://arxiv.org/abs/2003.13670 (Accedido: 4 de mayo de 2020).

[21] S. G. T. Agency, "TraceTogether app," March 2020. [Online]. Disponible: https://www.tracetogether.gov.sg/ (Accedido: 4 de mayo de 2020).

[22] H. Cho *et al.*, "Contact tracing mobile apps for covid-19: Privacy considerations and related trade-offs," Tech. Rep., 2020. [Online]. Disponible: https://arxiv.org/abs/2003.11511v1 (Accedido: 4 de mayo de 2020).

[23] I. M. of Health, "Hamagen," March 2020. [Online]. Disponible: https://github.com/MohGovIL/hamagen-react-native (Accedido: 4 de mayo de 2020).

[24] D. Belkin and K. Grind, "MIT researchers launch location-tracking effort for the new coronavirus," March 2020. [Online]. Disponible: https://www.wsj.com/articles/mit-researchers-launch-location-tracking-effort-for-the-new-coro2020 (Accedido: 4 de mayo de 2020).

[25] R. Raskar, "Private kit: Safe paths - can we slow the spread without giving up individual privacy?" March 2020. [Online]. Disponible: https://safepaths.mit.edu/ (Accedido: 4 de mayo de 2020).

[26] J. Bay *et al.*, "BlueTrace: A privacy-preserving protocol for community-driven contact tracing across borders," Government Technology Agency - Singapore, Tech. Rep., 2020. [Online]. Disponible: https://bluetrace.io/static/bluetrace_whitepaper-938063656596c104632def383eb33b3c.pdf (Accedido: 4 de mayo de 2020).

[27] Covid Watch, March 2020. [Online]. Disponible: https://covid-watch.org (Accedido: 4 de mayo de 2020).

[28] C. Troncoso *et al.*, "Decentralized Privacy-Preserving Proximity Tracing," Tech. Rep., 2020. [Online]. Disponible: https://github.com/DP-3T/documents (Accedido: 4 de mayo de 2020).

[29] "ROBERT: ROBust and privacy-presERving proximity Tracing," PRIVATICS team, Inria, France and Fraunhofer AISEC, Germany, Tech. Rep., 2020. [Online]. Disponible: https://github.com/ROBERT-proximity-tracing/documents/blob/master/ROBERT-specification-EN-v1_0.pdf (Accedido: 4 de mayo de 2020).

[30] G. Inc., "Apple and Google partner on COVID-19 contact tracing technology," April 2020. [Online]. Disponible: https://www.apple.com/newsroom/2020/04/apple-and-google-partner-on-covid-19-contact-tracing-technology/ (Accedido: 4 de mayo de 2020).

[31] A. Narayanan *et al.*, "Location privacy via private proximity testing," in *Proceedings of the Network and Distributed System Security Symposium, NDSS 2011, San Diego, California, USA, 6th February - 9th February 2011*. The Internet Society, 2011. [Online]. Disponible: https://www.ndss-symposium.org/ndss2011/privacy-private-proximity-testing-paper

[32] J. Sun, R. Zhang, and Y. Zhang, "Privacy-preserving spatiotemporal matching for secure device-to-device communications." *IEEE Internet of Things Journal*, vol. 6, no. 3, 2016.

[33] Y. Lindell and M. Green, "Privacy & tracking to mitigate pandemics: politics and technological solutions," March 2020. [Online]. Disponible: https://www.brighttalk.com/webcast/17700/392003/privacy-tracking-to-mitigate-pandemics-politic (Accedido: 4 de mayo de 2020).

[34] C. Troncoso *et al.*, "Joint Statement on Contact Tracing," April 2020. [Online]. Disponible: https://cispa.saarland/2020/04/20/joint-statement-on-contact-tracing.html (Accedido: 4 de mayo de 2020).

[35] EDPB, "Statement on the processing of personal data in the context of the COVID-19 outbreak," March 2020. [Online]. Disponible: https://edpb.europa.eu/news/news/2020/statement-processing-personal-data-context-covid-19-outbreak_en (Accedido: 4 de mayo de 2020).

[36] EDPB open letter, "Ref:OUT2020-0028," April 2020. [Online]. Disponible: https://edpb.europa.eu/sites/edpb/files/files/file1/edpbletterecadvisecodiv-appguidancefinal.pdf (Accedido: 4 de mayo de 2020).

[37] U. AAIP, “Guía de Evaluación de Impacto en la Protección de Datos Personales,” Unidad Reguladora y de Control de Datos Personales Uruguay, Agencia de Acceso a la Información Pública Argentina, Tech. Rep., 2020. [Online]. Disponible: https://www.gub.uy/unidad-reguladora-control-datos-personales/comunicacion/publicaciones/guia-evaluacion-impacto-proteccion-datos (Accedido: 4 de mayo de 2020).

[38] LECRE, “Ethical issues of anti-pandemic applications,” Université de Montréal, April 2020. [Online]. Disponible: http://www.lecre.umontreal.ca/les-enjeux-ethiques-des-applications-anti-pandemie/ (Accedido: 4 de mayo de 2020).

[39] Collaborative INRIA work led by the PRIVATICS team, “Proximity Tracing Applications: The misleading debate about centralised versus decentralised approaches,” INRIA, Tech. Rep., 2020. [Online]. Disponible: https://github.com/ROBERT-proximity-tracing/documents/blob/master/Proximity-tracing-discussion-EN.pdf (Accedido: 4 de mayo de 2020).

[40] The DP-3T Project, “Privacy and Security Risk Evaluation of Digital Proximity Tracing Systems,” Tech. Rep., 2020. [Online]. Disponible: https://github.com/DP-3T/documents/blob/master/Security%20analysis/Privacy%20and%20Security%20Attacks%20on%20Digital%20Proximity%20Tracing%20Systems.pdf (Accedido: 4 de mayo de 2020).

[41] “Pan-European Privacy-Preserving Proximity Tracing. High-Level Overview,” PEPP-PT, Tech. Rep., April 2020. [Online]. Disponible: https://github.com/pepp-pt/pepp-pt-documentation/blob/master/PEPP-PT-high-level-overview.pdf (Accedido: 4 de mayo de 2020).