FUTURE OF PRIVACY FORUM

JULIO 2021

TECNOLOGÍA DE RASTREO DE CONTACTOS DIGITAL:

Principios de privacidad y equidad, y marco

INTRODUCCIÓN

El rastreo de contactos siempre ha sido un proceso de seguimiento de enfermedades manual que utilizan las autoridades sanitarias públicas para monitorear la transmisión de enfermedades infecciosas. Durante la pandemia del COVID-19, las tecnologías de rastreo de contactos digital (Digital Contact Tracing Technologies – 'DCTT', en inglés) se desarrollaron como herramientas de notificación de exposición para ayudar a reabrir de manera segura las economías, los lugares de trabajo y otros espacios y entornos públicos y privados.[1] En especial, las DCTT consisten de aplicaciones y dispositivos móviles que usan bluetooth y/o características de geolocalización cuyo objetivo es brindar notificaciones rápidas y en tiempo real de exposición al virus a los usuarios.

Los expertos esperan que los esfuerzos de desarrollos de DCTT para el COVID-19 continúen un tiempo más y que las tecnologías de rastreo de contactos digital y su administración sigan evolucionando a medida que los funcionarios de salud pública establecen las bases para que los programas de DCTT aborden amenazas de pandemias nuevas y emergentes. A su vez, siguen apareciendo pruebas acerca de la eficacia y la validez científica de las DCTT a medida que se expande su uso como herramienta de vigilancia de salud pública y privada.

Future of Privacy Forum (FPF) se asoció con seis organizaciones líderes en privacidad, defensa social y equidad en el acceso a la salud para analizar las concesiones y riesgos de privacidad y equidad que puedan surgir con la implementación de las DCTT: Dialogue on Diversity, National Alliance Against Disparities in Patient Health (NADPH), BrightHive y LGBT Tech. Con un enfoque particular en los impactos de las DCTT sobre las poblaciones vulnerables, el grupo debatió los riesgos específicos, como los riesgos de enajenación o la estigmatización social relacionada con las razas o etnias, clase social, creencia religiosa y otras características.

Los esfuerzos de implementación de las DCTT que minimizan o no reconocen la presencia, función o impacto de estas concesiones y riesgos debilitarán la confianza del público en estas tecnologías. Por lo contrario, los esfuerzos de administración que reconocen, mitigan y se ocupan de estos riesgos pueden impulsar la confianza del público en las tecnologías de rastreo de contactos. Los legisladores, expertos en protección de datos y organizaciones que desarrollan, administran y proporcionan tecnologías de rastreo de contactos digital juegan un papel importante.

RESUMEN EJECUTIVO

Como parte de su iniciativa Privacy and Pandemics (“La privacidad y las pandemias”), el FPF trabajó con Dialogue on Diversity, la National Alliance Against Disparities in Patient Health (NADPH), BrightHive y LGBT Tech para crear un conjunto de principios procesables para apoyar la privacidad y la equidad en la implementación de las DCTT.

Estos principios aconsejan lo siguiente a las organizaciones que implementan DCTT:

1. Ser transparentes sobre cómo se usan y comparten los datos.
2. Aplicar soluciones y técnicas de desidentificación sólidas.
3. Facultar a los usuarios con funciones de aceptación/rechazo por niveles y minimización de datos compartidos.
4. Reconocer y abordar las brechas de protección de privacidad, seguridad y no discriminación.
5. Crear acceso equitativo a las DCTT.
6. Reconocer y abordar la parcialidad implícita en las configuraciones públicas y privadas.
7. Democratizar los datos para el bien público y, al mismo tiempo, emplear los resguardos de privacidad apropiados.
8. Adoptar estándares de privacidad por diseño que hagan que las DCTT tengan amplia accesibilidad.

FPF y estas seis organizaciones convocan a los desarrolladores de las DCTT y a las organizaciones que están implementando DCTT a que se comprometan con estos principios.

Debajo:

1. Describimos cada principio.
2. Resumimos los escenarios posibles que demuestran cómo las tecnologías de rastreo de contactos digital pueden generar riesgos a la protección de datos, en especial para personas vulnerables, como las minorías religiosas y raciales, integrantes de la comunidad LGBTQ+ y de las comunidades de inmigrantes.
3. Resaltamos las definiciones claves y otros recursos para informar acerca de la implementación de las DCTT desde una perspectiva de privacidad y equidad.

PRINCIPIOS DE PRIVACIDAD Y EQUIDAD PROCESABLES PARA LAS TECNOLOGÍAS DE RASTREO DE CONTACTOS DIGITAL

1 Ser transparentes sobre cómo se usan, recopilan y comparten los datos

Los proveedores de las DCTT pueden usar y compartir datos de rastreo de contactos para beneficio de la salud pública u objetivos similares. Las evidencias históricas y actuales indican que instituciones fuertes, como las fuerzas policiales, pueden utilizar los datos sensibles de forma discriminatoria y someter a ciertos grupos de personas a opresión, violencia y otras circunstancias sociales extremas. Asimismo, si la precisión técnica de las DCTT no está clara ni se muestra correctamente, es posible que las DCTT puedan generar acciones basadas en falsos positivos o rastreo de contactos incorrectos, como acciones de las fuerzas policiales contra poblaciones socialmente vulnerables.

Los usuarios de las DCTT deben saber cómo se recopilan, usan y comparten sus datos mediante declaraciones visibles, comprensibles y accesibles. Por ejemplo, se pueden mostrar avisos claros sobre recopilación, uso y divulgación de datos antes de la instalación de DCTT con notificaciones en la tienda de aplicaciones, al momento de descargar o instalar con avisos de términos del servicio en la aplicación o al momento del primer uso de la aplicación con notificaciones en el momento justo. Los avisos y/o configuraciones de privacidad también deben mostrar de manera explícita cuándo se recopilarán datos sensibles y por cuánto tiempo.

2 Aplicar soluciones y técnicas de desidentificación sólidas

Los proveedores de DCTT deben aplicar técnicas y soluciones de protección de privacidad sólidas para evitar que partes maliciosas y/o no autorizadas aprovechen los datos sensibles que recopilan las DCTT de forma que no coincida o entre en conflicto con el espíritu de la salud pública, o que generen un riesgo de daño. Las organizaciones pueden implementar controles de políticas, técnicos, contractuales o legales sobre los datos para lograr este cometido. Los controles pueden incluir técnicas de desidentificación sólidas, respaldos de la seguridad de los datos, descentralización de datos y cortafuegos de privacidad para datos de notificaciones de exposición. Por ejemplo, las técnicas sólidas de desidentificación pueden ser la eliminación de identificadores directos e indirectos conocidos para ocultar identidades del mundo real. Los resguardos de seguridad de datos y los cortafuegos de privacidad incluyen permisos técnicos que limitan el acceso a personas no autorizadas, así como los controles organizacionales y legales que prohíben que terceros identifiquen o vuelvan a identificar a usuarios de las DCTT. Por último, la descentralización de datos significa que los datos de notificaciones de exposición permanecen en el dispositivo y, por tanto, las identidades de los dueños de los dispositivos no se divulgan al momento de las notificaciones de exposición.

Las arquitecturas de datos interoperables y los tipos de datos que contienen información individual por usuarios, como la edad y el género emparejados con los datos de geolocalización, se deben resguardar con protecciones de seguridad apropiadas y sólidas que funcionen de manera efectiva en diferentes arquitecturas de datos. Sin dichas medidas de protección, existe el riesgo o el potencial de un uso indebido o abuso de los datos, minimización de la falta de datos y, por tanto, adopción de usuarios y/o cumplimiento de pruebas de detección de enfermedades infecciosas limitados.

PRINCIPIOS DE PRIVACIDAD Y EQUIDAD PROCESABLES PARA LAS TECNOLOGÍAS DE RASTREO DE CONTACTOS DIGITAL (continuo)

3 Facultar a los usuarios con funciones de aceptación/rechazo por niveles y minimización de datos compartidos

La participación en las DCTT debería ser voluntaria (ni obligatoria o forzosa), y los usuarios de las DCTT deberían, en general, tener la posibilidad de aceptar ciertas características de las DCTT (es decir, habilitar modos "activos" (aceptar) en lugar de tener solo modos de participación "pasivos" (de base; rechazado por defecto)).

Por defecto, las DCTT deberían solo recopilar los datos necesarios para brindarles el servicio a los usuarios. Las DCTT deberían brindarles a los usuarios la posibilidad de aceptar o rechazar la recopilación y divulgación de más datos. Se deben ofrecer opciones de aceptar/rechazar funciones significativas, y los usuarios de las DCTT deberían poder acceder a estas fácilmente.

4 Reconocer y abordar las brechas de protección de privacidad, seguridad y no discriminación

Es posible que haya protecciones administrativas obligatorias limitadas para controlar y regular las prácticas de privacidad, no discriminación y vigilancia de las organizaciones o proveedores de servicios. Por tanto, los desarrolladores de las DCTT y las instituciones que las adopten deben respaldar públicamente los códigos de ética, estándares, manuales y/o marcos que aboguen por la diversidad y equidad en las DCTT, y ser responsables ante el no cumplimiento de dichos estándares. Entre estos, se podría incluir el "Responsible Data Use Playbook for Digital Contact Tracing" (*Manual de uso responsable de datos para el rastreo de contactos digital*) del FPF y BrightHive, el "Ethical Framework for Assessing Manual and Digital Contact Tracing for COVID-19" (*Marco ético para la evaluación del rastreo de contactos manual y digital del COVID-19*) de Lo and Sim o la "Guide to Community-Based Workforce Principles for Contact Tracing" (*Guía de principios de la fuerza laboral comunitaria para el rastreo de contactos*) de la National Association of County and City Health Officials (*Asociación Nacional de Funcionarios de Salud del Condado y la Ciudad*). Se debe impulsar y facultar a los usuarios de las DCTT para que participen de manera activa en el desarrollo e implementación de dichos códigos de ética, estándares y/o marcos.

PRINCIPIOS DE PRIVACIDAD Y EQUIDAD PROCESABLES PARA LAS TECNOLOGÍAS DE RASTREO DE CONTACTOS DIGITAL (continuo)

5 Crear acceso equitativo a las DCTT

Tomando en cuenta que algunos dispositivos pueden ser más compatibles con ciertas DCTT que otros, es importante que los desarrolladores eviten vincular algún tipo de dispositivo en particular a las funciones más beneficiosas de las DCTT. Al crear un acceso equitativo (versus igualitario) a las DCTT, es importante considerar y abordar las barreras estructurales y procesales únicas que las personas o grupos puedan llegar a experimentar al buscar acceso a los beneficios del uso de las DCTT. Es fundamental tener un rol en la facilitación del acceso equitativo a dispositivos personales e infraestructuras necesarios para la adopción y uso de las DCTT. Por ejemplo, crear DCTT que funcionen sin la necesidad de servicio a internet inalámbrico o que sean compatibles con dispositivos móviles antiguos y nuevos puede garantizar que las DCTT lleguen ampliamente a las personas, más allá de su situación económica.

6 Reconocer y abordar la parcialidad implícita en las configuraciones públicas y privadas

Es importante aceptar la realidad e impacto actuales de la parcialidad que existe en diferentes ámbitos, como el de la atención médica o salud pública, y abordar escenarios en los que las DCTT puedan exponer, perpetuar o incluso agravar la parcialidad social dentro de dichos ámbitos. Dado que las personas y los grupos sujetos a parcialidades implícitas en dichos ámbitos pueden enfrentarse a casos de mala administración y/o discriminación, estos tienden a evitar dichos ámbitos, a pesar de su importancia y de la importancia de las DCTT para la gestión de la salud pública durante las pandemias. Por ejemplo, si una persona o grupo socialmente marginados se enfrentan con frecuencia a situaciones de incomodidad, miedo o vergüenza al buscar atención médica dentro de un sistema de salud público parcial, es probable que dicha persona o grupo no confíe o no participe de un programa de DCTT que se implemente o que forme parte de dicho sistema. Por lo tanto, aceptar y abordar la parcialidad implícita dentro de los diferentes ámbitos en los que se implementan las DCTT podría aumentar la probabilidad de que las personas se sientan más seguras de usar las DCTT.

PRINCIPIOS DE PRIVACIDAD Y EQUIDAD PROCESABLES PARA LAS TECNOLOGÍAS DE RASTREO DE CONTACTOS DIGITAL (continuo)

7 Democratizar los datos para el bien público y, al mismo tiempo, emplear los resguardos de privacidad apropiados

En la medida de lo posible, los datos se deben democratizar para ofrecer beneficios a los programas e infraestructuras de salud pública. En general, los datos de las DCTT se pueden compartir de forma limitada y desidentificada para impulsar dichos objetivos. Los datos se pueden compartir con socios de investigación confiables, gestionar como parte de la red de información de salud comunitaria o, en casos excepcionales, poner a disposición del público. Los gobiernos y otras entidades relevantes deben implementar medidas sólidas para garantizar la privacidad, en especial si los datos de las DCTT se ponen a disposición del público o es fácil acceder a ellos.

Las políticas públicas deberían apoyar y proteger el uso de los datos de las DCTT para la investigación en salud pública mediante la incorporación o respaldo de procesos, prácticas y procedimientos de administración de datos sólidos. Por ejemplo, dichos procesos, prácticas o procedimientos podrían incluir la identificación de las categorías mínimas necesarias de datos que se pueden hacer públicas; aplicar resguardos técnicos, contractuales y/o procesales para evitar la divulgación excesiva de información personal; y garantizar que los datos de usuarios de las DCTT estén resguardados mediante sistemas de encriptado sólidos u otros estándares de seguridad de datos.

8 Adoptar estándares de privacidad por diseño que hagan que las DCTT tengan amplia accesibilidad

Los desarrolladores deben adoptar estándares de diseño de privacidad por diseño que también puedan garantizar el amplio acceso de los usuarios a las DCTT. Dichos estándares deben garantizar que los beneficios de las DCTT se puedan maximizar para servir al público sin comprometer, por diseño, la privacidad y la equidad de los usuarios de las DCTT en el proceso.

Para firmar los Principios de tecnologías de rastreo de contactos digitales, póngase en contacto con nosotros en info@fpf.org.

DEFINICIONES

1. **DCTT:** Tecnología que se usa para detectar una posible exposición a una enfermedad o infección. Incluye a las aplicaciones que rastrean los movimientos de los usuarios y su estado de salud, y vinculan los datos entre muchos usuarios para identificar posibles exposiciones.
2. **Usuario de las DCTT:** Personas que usan las DCTT en un dispositivo personal o a través de este para objetivos públicos o privados.
3. **Minimización de datos:** Datos adecuados, relevantes y limitados a lo que es necesario en relación con los objetivos para los cuales se los procesa. (*Reglamento General de Protección de Datos (GDPR), capítulo 2, artículo 5*)
4. **Desidentificación:** Proceso mediante el cual se elimina la información personal identificable de los datos que las organizaciones recopilan, almacenan y usan. (*Future of Privacy Forum, A Visual Guide to Practical Data De-Identification (Guía visual para la desidentificación de datos práctica) [abril 2016]*)
5. **Seudonimización:** Proceso mediante el cual se eliminan o modifican identificadores directos, pero no se cambian los identificadores indirectos. (*Future of Privacy Forum, A Visual Guide to Practical Data De-Identification (Guía visual para la desidentificación de datos práctica) [abril 2016]*)
6. **Datos sensibles:** Datos sujetos a condiciones de procesamiento específicas que convierten a la información en identificable, en los siguientes contextos: 1) datos que revelan origen racial o étnico, opiniones políticas, creencias religiosas o filosóficas; 2) datos genéticos, datos biométricos procesados con el único fin de identificar a una persona; 3) datos de salud; 4) datos relacionados con la vida y orientación sexuales de una persona; y 5) geolocalización precisa. (Adaptado de los artículos 4(13), (14) y (15), y de los considerandos (51) a (56) del Reglamento General de Protección de Datos (GDPR); también adaptados de la Sección 14 de la Ley de Derechos de Privacidad de California (CPRA)).
7. **Descentralización:** Proceso en el cual la información disponible se divide en diferentes partes y se almacena en distintos sitios (agentes móviles, centros de edge computing, etc.) de una red en lugar de almacenar todo en un servidor central; además, ninguna entidad tiene control total o completo de la información. (*Shubina et al. 2020*)

ESCENARIOS POSIBLES

ESCENARIO 1

Comunidad LGBT en Seúl, Corea del Sur

Durante los primeros meses de la pandemia del COVID-19, se acusó a las lesbianas, gais, bisexuales y transgénero (LGBT) en Corea del Sur de propagar el COVID-19 luego de que el Gobierno comenzara a relajar las medidas a principios de mayo de 2020, cuando permitió que reabrieran bares y otros espacios sociales. Luego de la reapertura, aparecieron varios casos nuevos de COVID-19 y se pudo rastrear su origen a clubes nocturnos en Itaewon, una zona de la ciudad de Seúl muy conocida por sus restaurantes y lugares de vida nocturna cosmopolitas descritos por los medios como centros sociales o espacios seguros para "club gais". El alcalde de Seúl declaró que aquellas personas "expuestas al virus que no se realicen testeos recibirán una visita en sus hogares del Gobierno y la Policía". Para muchos, esto puso a los grupos de la comunidad LGBT en riesgo de ser víctimas de discriminación y especulación acerca de la sexualidad de las personas como resultado de los esfuerzos de rastreo. Thoreson, 2020, *Human Rights Watch*

ESCENARIO 2

Tensiones no resueltas de la era del sida en los EUA

Las historias de tensiones no resueltas entre los rastreadores de contactos y la comunidad gay en San Francisco, California, siguen vigentes en la actualidad después de casi 40 años. Desde la década del 1980, los rastreadores de contactos y los abogados defensores de los derechos de la comunidad gay vienen expresando que los efectos de los esfuerzos de rastreo de contactos generalizados de las agencias de salud pública por el virus del sida y el VIH hicieron que la comunidad gay se oponga al rastreo de contactos. Identificar a los individuos con exposición al virus del sida y el VIH puede llevar, y ha llevado, a la pérdida de trabajos, vivienda y otras necesidades y servicios esenciales en la comunidad gay.

Inspirada en diferentes historias y aprendizajes relacionados con los problemas de confianza pendientes entre la comunidad gay y las agencias de salud pública, una periodista de KQED concluyó que, en la actualidad, los departamentos de salud locales, estatales y de los condados están "creando puentes con las poblaciones afectadas gracias a la asociación con grupos comunitarios" que tienen buenas relaciones con la comunidad gay. Dembosky, 2020, *KQED*

ESCENARIOS 1 Y 2: APRENDIZAJES

Los escenarios 1 y 2 destacan por qué es importante aplicar los siguientes principios:

- **Principio 4 Reconocer y abordar las brechas de protección de privacidad, seguridad y no discriminación.**

  Los desarrolladores de las DCTT y las instituciones que las adopten pueden promover la confianza al ofrecer un respaldo público a estas y al respetar códigos de ética, estándares, manuales y/o marcos desarrollados con comentarios directos de comunidades con un historial de abuso y problemas de confianza con ciertas instituciones.

- **Principio 6: Reconocer y abordar la parcialidad implícita en las configuraciones públicas y privadas.**

  Los desarrolladores de las DCTT y las instituciones que las adopten deben anticipar y abordar los escenarios actuales o posibles en los que las DCTT pueden exponer, perpetuar o incluso agravar las parcialidades dañinas en un rango o en una multitud de ámbitos privados y públicos para ayudar a garantizar que las personas se sientan seguras y protegidas de los daños y desgracias concatenados que se pueden dar por culpa de una parcialidad implícita dentro de un sistema o ámbito.

- **Principio 8: Adoptar estándares de privacidad por diseño que hagan que las DCTT tengan amplia accesibilidad.**

  Las funciones o estándares de privacidad por diseño, como las notificaciones a exposiciones anónimas, hacen que las personas tomen decisiones privadas acerca del seguimiento y control de sus comportamientos y circunstancias personales, comunicación con otras personas y movimientos después de la exposición a enfermedades contagiosas.

APORTE CLAVE

Los esfuerzos de rastreo de contactos para el seguimiento de la propagación de enfermedades contagiosas en grupos socialmente vulnerables pueden colocar a dichos grupos en riesgo de sufrir discriminación u ostracismo en su hogar o dentro de sus comunidades. Dichos grupos son los que más pueden sufrir, desde un punto de vista social y económico, y pueden llegar a no querer utilizar ningún tipo de tecnología, incluidas las DCTT, que pueda divulgar sus vínculos sociales y paraderos.

ESCENARIO 3

Comunidad africana en Guangzhou, una ciudad sureña de China

Integrantes de una comunidad africana en Guangzhou sufrieron discriminación luego de que el Gobierno de China emitiera advertencias facialmente neutrales en las redes sociales contra las cepas importadas del coronavirus. Las autoridades de Guangzhou indicaron que cinco nigerianos dieron positivo de COVID-19 y rastrearon el riesgo de contagio de coronavirus a las zonas Yuexiu y Baiyun de Guangzhou, que son predominantemente comunidades africanas. En un artículo de CNN, se indicó que los integrantes de esta comunidad africana fueron expulsados de sus casas de alquiler y se les negó servicios hoteleros, a pesar de sus afirmaciones de no haber viajado recientemente ni haber tenido contactos con casos positivos de COVID-19. Muchos de los integrantes de esta comunidad africana usan visas de trabajo de corto plazo y viajan entre África y China varias veces al año.

La hostilidad contra los residentes africanos era previa a la emergencia de la pandemia de COVID-19 en la ciudad, pero empeoró a causa de ella. Se obligó a las personas con "contactos africanos" a ponerse en cuarentena. El consulado de los Estados Unidos en Guangzhou advirtió a los afroamericanos que evitaran viajar a Guangzhou ante el aumento de la situación hostil. Su advertencia: "...la Policía ordenó a bares y restaurantes que no sirvieran a clientes de origen africano". Marsh, Deng y Gan, 2020, CNN; *Consulado de los Estados Unidos en Guangzhou, República Popular de China [13 de abril de 2020]:* Discriminación contra afroamericanos en Guangzhou (en inglés)

ESCENARIO 4

Comunidad musulmana en Camboya

El Ministerio de Salud de Camboya nombró, en su página oficial en las redes sociales, grupos específicos de personas que contrajeron COVID-19 luego de que un rastreo de contactos revelara que "no existieron señales de transmisión en sus comunidades [locales]". Uno de los grupos específicos fue denominado "Khmer Islam". Se informó que la publicación en las redes sociales provocó un "estallido" de comentarios y gestos discriminatorios y de odio contra las comunidades musulmanes minoritarias de Camboya, tanto en internet como en mercados, tiendas y otras zonas públicas. Luego de estos eventos, un vocero del Gobierno de Camboya solicitó a los medios que evitaran dar información identificatoria acerca de personas con COVID-19. Chhin, 2020, *Human Rights Watch*; Penh, *2020, VOA*

ESCENARIOS 3 Y 4: APRENDIZAJES

Los escenarios 3 y 4 destacan por qué es importante aplicar los siguientes principios:

- **Principio 4: Reconocer y abordar las brechas de protección de privacidad, seguridad y no discriminación.**

  Los desarrolladores de las DCTT y las instituciones que las adopten pueden promover la confianza al ofrecer un respaldo público a estas y al respetar códigos de ética, estándares, manuales y/o marcos desarrollados con comentarios directos de comunidades con un historial de abuso y problemas de confianza con ciertas instituciones.

- **Principio 6: Reconocer y abordar la parcialidad implícita en las configuraciones públicas y privadas.**

  Cuando entidades de poder como las autoridades sanitarias o gubernamentales atribuyen una enfermedad contagiosa a una zona hipersegregada o a un grupo de personas que viaja con frecuencia a una zona, esto puede provocar o agravar las parcialidades dañinas de las personas contra dichos grupos hipersegregados o de viajeros frecuentes. Los desarrolladores y usuarios de las DCTT deben crear e implementar estrategias de DCTT y de información de datos que resguarden los efectos concatenados de parcialidades implícitas o dañinas, como la estigmatización o los comentarios de odio, y proteger el bienestar y la reputación de las comunidades hipersegregadas o de los grupos que viajan a ciertas zonas de una comunidad.

- **Principio 7: Democratizar los datos para el bien público y, al mismo tiempo, emplear los resguardos de privacidad apropiados.**

  Cuando se recopilan y divulgan públicamente datos mínimos, esto puede ayudar a prevenir que ciertas personas sean blanco social o que se las señale erróneamente y de forma dañina sobre la base de sus vínculos personales, atributos biológicos o parcialidades, y suposiciones inherentes de otras personas.

APORTE CLAVE

Las DCTT no deben convertir a grupos que comparten ciertas características o vínculos sociales en blancos de las fuerzas policiales, de la difamación de los medios o del escarnio público. Los desarrolladores de las DCTT, los legisladores y otras partes influyentes, como los medios o las empresas dueñas de redes sociales y sus usuarios, deben anticipar los usos erróneos potenciales de los datos de rastreo de contactos. Esto se debe hacer con el objetivo de resguardar a las poblaciones vulnerables o a las personas del ostracismo social o de la discrimi nación basada en creencias religiosas, características únicas u otros atributos personales.

ESCENARIO 5

Aplicación de rastreo de contactos del COVID-19 en North Dakota, EUA

Care19, una aplicación voluntaria desarrollada por ProudCrowd, una empresa de North Dakota, fue una de las primeras aplicaciones de rastreo de contactos que se implementó en respuesta a la pandemia de COVID-19. La aplicación recibió el apoyo oficial de los funcionarios gubernamentales de los estados de North Dakota y South Dakota. Luego, Jumbo Privacy, una empresa de privacidad tecnológica descubrió que la aplicación Care19 incluía código que enviaba la ubicación de los usuarios y datos de identificación a empresas locales e internacionales, incluidas compañías publicitarias. Si bien la aplicación contenía dicho código, la declaración de privacidad les informaba a los usuarios que sus datos de ubicación "no serán compartidos con nadie, ni con entidades gubernamentales o terceros, a menos que otorgue su consenso o que ProudCrowd se vea obligado a hacerlo por disposiciones federales". Groves, 2020, *USA Today*

ESCENARIO 5: APRENDIZAJES

El escenario 6 destaca por qué es importante aplicar los siguientes principios:

- **Principio 1: Ser transparentes sobre cómo se usan, recopilan y comparten los datos.**

  Si los usuarios de las DCTT están bien informados y saben si su información se recopila, usa y comparte con terceros, y cómo se lleva adelante dicho proceso, pueden tomar decisiones informadas sobre con quién desean compartir la información. Esto protege los intereses no solo de los usuarios de las DCTT, sino también de sus desarrolladores que buscan ofrecer estándares altos de servicio al usuario/cliente.

- **Principio 3: Facultar a los usuarios con funciones de aceptación/rechazo por niveles y minimización de datos compartidos.**

  Las funciones y minimización de datos de aceptación/rechazo por niveles les dan a los usuarios de las DCTT la posibilidad de elegir para participar de tal manera que se adapte a sus preferencias de privacidad y a su bienestar e intereses personales. Las empresas o desarrolladores de las DCTT deben auditar minuciosamente el código que quieren adoptar o usar para comprobar que sus plataformas no sean engañosas ni engañen a los usuarios y autoridades regulatorias en sus declaraciones y políticas de privacidad.

APORTE CLAVE

Las políticas de privacidad, acuerdos de uso y avisos similares deben ser claros y reflejar perfectamente las prácticas de privacidad del desarrollador de las DCTT, y deben estar escritos de tal manera que sean accesibles para todo el mundo. Las políticas de privacidad no deben incluir jerga, disposiciones o términos intimidatorios sobre las prácticas de privacidad de la aplicación que sean difíciles de entender o de interpretar para la mayoría de los usuarios. Los avisos no deben incluir términos coercitivos que presionen a los usuarios a optar por funciones con menor nivel de privacidad, particularmente si los usuarios necesitan, dependen o están obligados a usar la aplicación por cuestiones personales, legales u otras. Los desarrolladores de aplicaciones, incluidos los desarrolladores de las DCTT, deben auditar minuciosamente el código que adoptan o lograr que el código respete sus estándares, políticas y términos de privacidad internos, así como las normativas de las tiendas de aplicaciones y las expectativas de privacidad de sus usuarios.

PROPUESTAS LEGISLATIVAS CLAVES PARA LOS EUA SOBRE LA TECNOLOGÍA DE RASTREO DE CONTACTOS DIGITAL

Proyectos de ley estatales

- **Nueva York:** Ley para modificar las normativas de salud pública en relación con la confidencialidad de la información de rastreo de contactos (A10500C/S8450C)
- **Nueva York:** Se relaciona con los requisitos de la recopilación y uso de datos de salud de emergencia e información personal, y el uso de la tecnología para ayudar durante la pandemia del COVID-19 (A10583/S8448)
- **California:** Información personal: rastreo de contactos (AB660; AB814)

Proyectos de ley federales

- Ley de Protección de Datos de los Consumidores durante la Pandemia del COVID–19 de 2020
- Ley de Privacidad ante la Emergencia de la Salud Pública
- Ley de Privacidad ante las Notificaciones de Exposición
- Creación de un marco estadounidense para garantizar el acceso a los datos, la transparencia y la responsabilidad (Ley SAFE DATA)
- Ley de Privacidad ante la Emergencia de la Salud Pública
- Ley de Datos Seguros y Privacidad en el Rastreo de Contactos

Resumen de los esfuerzos legislativos de las DCTT

- Resumen del FPF sobre tendencias legislativas adicionales en los EUA a agosto de 2020 (en inglés)

RECURSOS CLAVE SOBRE PRIVACIDAD Y EQUIDAD EN LA IMPLEMENTACIÓN DE LAS DCTT

- Rastreo de contactos digital: Manual para el uso responsable de datos (en inglés)
- Ley para el Rastreo de Contactos Digital y la Protección de Datos (en inglés)
- Vidas privadas y políticas públicas, confidencialidad y accesibilidad a estadísticas gubernamentales (en inglés)
- Taxonomía de las definiciones del ecosistema de datos de salud (en inglés)
- Derechos durante la pandemia del COVID-19: aprendizajes del VIH para una respuesta efectiva y comunitaria (en inglés)
- Tecnología en conflicto: cómo las aplicaciones de rastreo de contactos de COVID-19 pueden agravar los conflictos violentos (en inglés)
- Aplicaciones de rastreo de contactos: riesgos adicionales para mujeres y grupos marginalizados (en inglés)
- La ética detrás del rastreo de contactos instantáneo con aplicaciones móviles para el control de la pandemia de COVID-19 (en inglés)
- Mesa redonda virtual sobre el COVID-19 y los derechos humanos con investigadores de Human Rights Watch (en inglés)
- ¿Las aplicaciones de rastreo de contactos son la solución? Qué pueden aprender los EUA de otros países (en inglés)
- Contexto antes que código: protección de los derechos humanos durante el estado de emergencia (en inglés)
- Manual para el uso responsable de datos para el rastreo de contactos digital (en inglés)
- Marco ético para la evaluación del rastreo de contactos manual y digital para el COVID-19 (en inglés)
- Guía visual para la desidentificación práctica (en inglés)
- Mejores prácticas para los wearables para consumidores y aplicaciones y dispositivos de bienestar (en inglés)
- Encuesta integral y en tiempo real de Norton Rose Fulbright o resumen de los principales problemas de las disposiciones y políticas en diferentes jurisdicciones internacionales (en inglés)

1 Entre los ejemplos de DCTT disponibles al público encontramos COVIDWISE, una aplicación desarrollada por el Departamento de Salud del Estado de Virginia (EUA); CO Exposure Notifications, desarrollada por el Departamento de Salud y Medio Ambiente y el Centro de Operaciones de Emergencia del Estado de Colorado (EUA); y una plataforma de la Asociación de Laboratorios de Salud Pública desarrollada por epidemiólogos de diferentes estados y el Consejo de Gobiernos Metropolitano de Washington para el envío de notificaciones de exposición entre los estados vecinos de Columbia, Maryland, Virginia y West Virginia (EUA). Entre los ejemplos de DCTT fuera de los Estados Unidos de América encontramos Stopp Corona, desarrollado por el Ministerio Federal de Salud de Austria, y Coronavirus SUS, desarrollada por el gobierno federal de Brasil.

El apoyo para este programa fue proporcionado por la Fundación Robert Wood Johnson. Las opiniones expresadas aquí no reflejan necesariamente las opiniones de la Fundación.

1400 EYE STREET NW | SUITE 450 | WASHINGTON, DC 20005 INFO@FPF.ORG | 202-768-8950