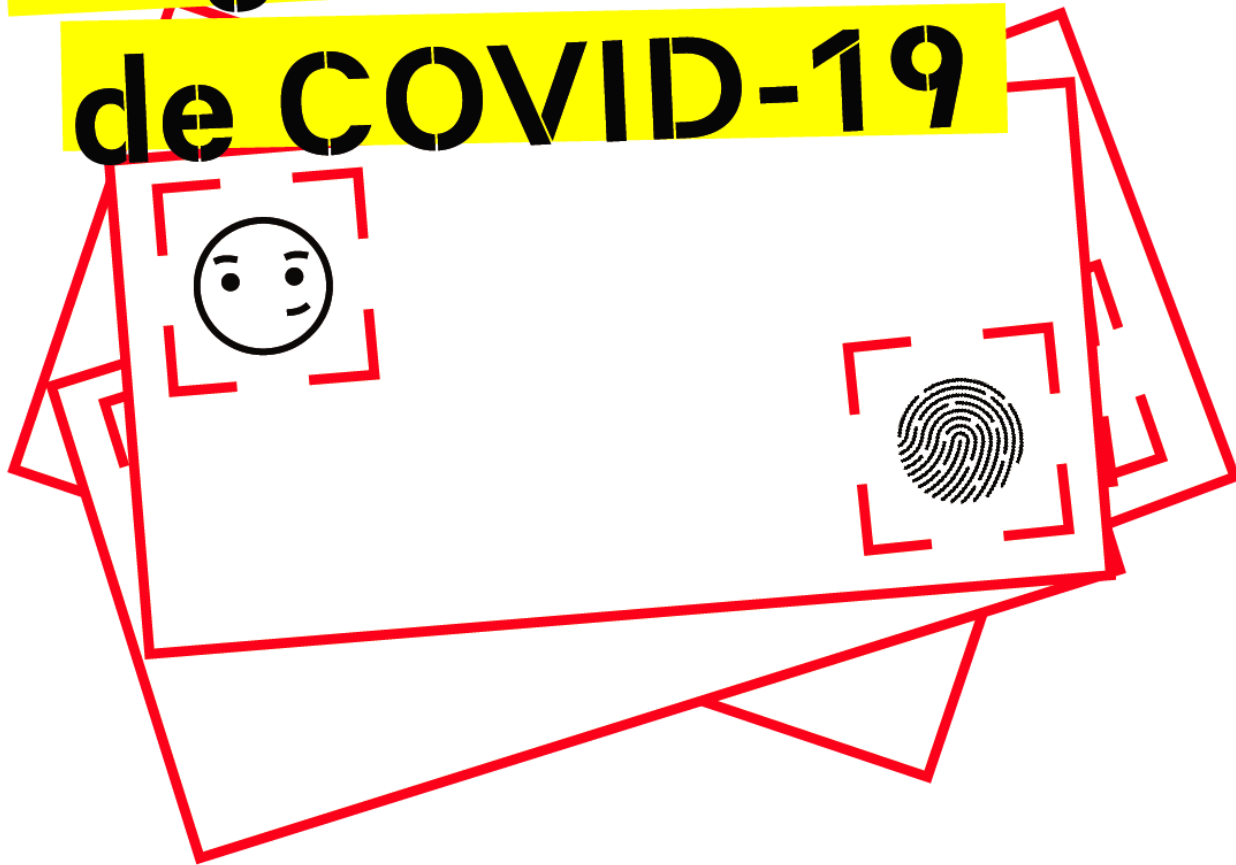


El impacto de Los certificados digitales de salud de COVID-19



Access Now defiende y extiende los derechos digitales de los usuarios en riesgo alrededor del mundo. Mediante la combinación de apoyo técnico directo, campañas globales, el análisis integral de políticas públicas, el financiamiento a grupos locales emergentes, intervenciones judiciales y eventos como RightsCon, luchamos por los derechos humanos en la era digital.

Este informe es una publicación de Access Now. Escrito por Naman M. Aggarwal y Carolyn Tackett. Agradecemos a los miembros del equipo de Access Now que brindaron su apoyo: Fanny Hidvégi, Estelle Massé, Verónica Arroyo, Marwa Fatafta, Raman Jit Singh Chima, Carolina Gonçalves, Eric Null, Elizabeth Metts, Juliana Castro y Sage Cheng. Además, agradecemos a la comunidad de [#WhyID](#) por su participación en el debate y sus perspectivas clave para esta publicación. Esperamos recibir comentarios y más contribuciones de expertos en derechos digitales, identidad y salud.



ÍNDICE

JULIO DE 2020

| | |
|--|----|
| I. INTRODUCCIÓN | 3 |
| II. QUÉ SON LOS CERTIFICADOS DIGITALES DE SALUD | 4 |
| III. BASES PARA LA CERTIFICACIÓN | 5 |
| 1. INMUNIDAD | 5 |
| 2. PERFIL DE RIESGO | 6 |
| Caso de estudio: India | 7 |
| IV. IMPACTO EN LOS DERECHOS DE LOS USUARIOS | 8 |
| 1. DERECHO A LA PRIVACIDAD | 8 |
| 2. DERECHO A LA CIRCULACIÓN Y A LA LIBERTAD DE REUNIÓN | 10 |
| 3. EXCLUSIÓN | 10 |
| 4. DISCRIMINACIÓN | 11 |
| 5. CREACIÓN DE UNA INFRAESTRUCTURA DE VIGILANCIA DE SALUD PERMANENTE | 12 |
| VI. CONCLUSIÓN | 13 |

I. INTRODUCCIÓN

A fines de 2019, el mundo comenzó la batalla contra el nuevo Coronavirus (COVID-19). Los gobiernos, las organizaciones sin fines de lucro, las empresas y los ciudadanos de todo el mundo están respondiendo al virus y a su propagación, por lo general, recurriendo a la tecnología para encontrar posibles soluciones. En Access Now, hemos hecho un seguimiento de estos desarrollos y de su impacto en los derechos humanos, especialmente para las comunidades marginalizadas. Hemos publicado recomendaciones específicas sobre la protección de la privacidad y los datos para las tecnologías que se despliegan como respuesta al COVID-19, junto con recomendaciones específicas para las aplicaciones de rastreo de contactos.¹ El desarrollo de soluciones sostenibles y efectivas para combatir el virus y su propagación requiere que los derechos humanos, incluido el derecho fundamental a la privacidad, se ubiquen en el centro de su diseño e implementación.

En esta publicación, describimos los diferentes modelos de certificados digitales de salud que se encuentran actualmente bajo consideración y las inquietudes sobre derechos humanos que estos generan. Remarcamos la importancia de tomar un enfoque orientado a los derechos humanos en el desarrollo de todo programa de certificados digitales de salud.

¹ Access Now, Recomendaciones para la protección de la privacidad y los datos en la lucha contra el COVID-19, <https://www.accessnow.org/covid19-data-protection/>; Access Now, Privacidad y salud pública: qué hacer y qué no en el desarrollo de aplicaciones de rastreo de contactos para combatir el COVID-19 <https://www.accessnow.org/privacy-and-public-health-the-dos-and-donts-for-covid-19-contact-tracing-apps/>

II. QUÉ SON LOS CERTIFICADOS DIGITALES DE SALUD

Mientras algunos países y regiones avanzan hacia las últimas fases de respuesta ante el COVID-19, los gobiernos exploran cómo habilitar la circulación de las personas a nivel interurbano, internacional y transfronterizo. Existen cada vez más propuestas para el uso de certificados o pases basados en la condición de salud de las personas para determinar quién puede volver a trabajar o ingresar a espacios recreativos, las respuestas ante emergencias, y mucho más. Denominamos “certificados digitales de salud” a aquellas iniciativas en las que la certificación basada en la condición de salud de una persona se administra y autentica de manera digital para permitir o prohibir la circulación o el acceso a servicios. Si bien hay precedentes en el requerimiento de certificados de vacunación para los viajes a países específicos (por ejemplo, el certificado de vacunación contra la fiebre amarilla para los viajes entre países con distintos niveles de exposición), las propuestas actuales se basan en una escala diferente y se diferencian de las prácticas preexistentes. A diferencia de la fiebre amarilla, el COVID-19 se ha confirmado en muchos más países, lo que certifica que esta enfermedad se trata de una pandemia en lugar de una enfermedad endémica en ciertos países.² Además, como observamos a continuación, la ciencia detrás de la inmunidad y los anticuerpos está poco desarrollada y, por lo tanto, la certeza de la protección contra el COVID-19 no está garantizada.

² Elizabeth M. Renieris, Dr. Sherri Bucher, y Christian Smith, “The Dangers of Blockchain-Enabled “Immunity Passports” for COVID-19,” Medium, 18 de mayo, 2020, <https://medium.com/berkman-klein-center/the-dangers-of-blockchain-enabled-immunity-passports-for-covid-19-5ff84cacb290>

III. BASES PARA LA CERTIFICACIÓN

Por lo general, las propuestas actuales de certificados digitales de salud se basan en uno de dos indicadores: la verificación de la inmunidad de una persona ante el COVID-19, la cual no es posible establecer aún con total certeza científica, o la determinación del nivel de riesgo de una persona en base a factores del entorno no específicos, los que también se basan generalmente en tecnologías no probadas.

1. INMUNIDAD

Conocidos como “certificados de inmunidad” o “pasaportes de inmunidad”, estos programas tienen el objetivo de certificar que un individuo ha adquirido inmunidad a una enfermedad particular y, por lo tanto, debería tener permitido el acceso a espacios o servicios determinados. Dichos certificados se emiten, normalmente, en base al testeo que verifica que una persona posee los anticuerpos necesarios o a la administración de una vacuna segura y eficaz.

Si bien se está llevando a cabo el desarrollo y testeo de las vacunas contra el COVID-19, no hay vacunas disponibles hasta el momento. Además, continúan las investigaciones sobre la eficacia de los anticuerpos de los pacientes sobrevivientes de COVID-19. Según las últimas pautas provistas por la Organización Mundial de la Salud (OMS) en abril de 2020, no hay pruebas suficientes de que una persona que haya sobrevivido al COVID-19 una vez sea inmune a una segunda infección.³ Se desconoce también cuánto tiempo pueden estar presentes los anticuerpos en la sangre de una persona, aunque ya hay evidencia temprana de que los anticuerpos desaparecen rápidamente del cuerpo.⁴ Sin tal evidencia ni una vacuna disponible, no hay argumentos sólidos para el uso de certificados digitales de salud basados en la inmunidad al COVID-19. Como observa la OMS, la emisión y el uso de dichos certificados puede incluso aumentar el riesgo de transmisión continua.⁵

³ «Pasaportes de inmunidad» en el contexto de la COVID-19, Organización Mundial de la Salud, 24 de abril, 2020, <https://www.who.int/news-room/commentaries/detail/immunity-passports-in-the-context-of-covid-19>

⁴ Charlotte Joe, “Immunity to covid-19 could disappear in months, a new study suggests,” MIT Technology Review, 13 de julio, 2020, <https://www.technologyreview.com/2020/07/13/1005103/immunity-to-covid-19-could-disappear-in-months-a-new-study-suggests/>

⁵ OMS, «Pasaportes de inmunidad» en el contexto de la COVID-19, <https://www.who.int/news-room/commentaries/detail/immunity-passports-in-the-context-of-covid-19>

2. PERFIL DE RIESGO

Debido a que aún no hay a disposición mecanismos de certificación basados en evidencia, los gobiernos y otras partes interesadas están explorando metodologías alternativas para la emisión de certificados digitales de salud según el nivel de riesgo general de las personas. Estos métodos crearían un “perfil de riesgo de salud” basado en diferentes señales, como el lugar de residencia de una persona (p. ej., las especificaciones de zonificación en la India), enfermedades preexistentes que exacerban el riesgo, y el rastreo de contactos (basado en la medicina y en aplicaciones).⁶ El nivel de riesgo asociado al perfil de una persona se utilizaría, entonces, para determinar adónde pueden viajar y a qué servicios pueden acceder.

Actualmente, estos sistemas se basan, en gran medida, en tecnología no probada y solo brindan aseveraciones sobre la condición de salud de una persona en base a la probabilidad y, por ende, son propensos a errores. Asimismo, estas tecnologías dependen de la recopilación masiva de datos personales sensibles y algoritmos para el perfilamiento que no cuentan con los testeos ni la transparencia suficientes. No existe un método basado en evidencia para determinar con certeza el perfil de riesgo de una persona en relación con el COVID-19.

Caso de estudio: India

Aarogya Setu, la “solución integral de la India a todo lo relacionado con el COVID-19” brinda una interfaz para la autoevaluación de los riesgos ante el COVID-19. La evaluación les pide a los usuarios información sobre sí mismos, incluidos sus hábitos y síntomas actuales. Sobre la base de esta prueba, los usuarios se clasifican en “seguros” o “no seguros”. No se conoce el protocolo de toma de decisiones de esta prueba y existe mucha incertidumbre sobre cómo se corresponden los resultados con el verdadero riesgo a la exposición.

El Ministerio del Interior de la India, inicialmente, hizo obligatorio el uso de la herramienta de autoevaluación de la aplicación para todos los empleados de empresas públicas y privadas.⁷ Poco después, actualizó esta directiva y pidió

⁶ “Explained: What are containment zones, how are they demarcated?”, Indian Express, <https://indianexpress.com/article/explained/coronavirus-cases-india-containment-zones-6487494/>

⁷ Cuenta de Twitter del Representante del Ministerio del Interior, 1 de mayo de 2020, <https://twitter.com/PIBHomeAffairs/status/1256216662900117506>

que los empleadores hicieran “su mejor esfuerzo” para hacer cumplir el uso de la aplicación por parte de sus empleados, dejando de considerarlo obligatorio.⁸

En un análisis de las diferentes aplicaciones de rastreo de contactos llevado a cabo por *MIT Technology Review*, Aarogya Setu obtuvo un bajo puntaje de 2 de 5 puntos en lo que respecta a la protección de los usuarios y la eficacia de la aplicación.⁹ Luego, los investigadores bajaron el puntaje de 2 puntos a 1 punto, debido a que la aplicación recopilaba muchos más datos de los requeridos.¹⁰

En una versión más reciente, los estándares de privacidad de la aplicación se modificaron nuevamente. Estas actualizaciones permitieron que la aplicación subiera aún más datos de los usuarios al servidor central, independientemente del estado de COVID-19 del usuario. La actualización también permitió que los usuarios accedieran a información como la fecha, la hora, la ubicación aproximada y la duración de un “contacto de Bluetooth” a quien le hayan diagnosticado COVID-19.¹¹

⁸ “Aarogya Setu: MHA Dilutes Mandatory Imposition; Says Employers On ‘Best Effort Basis’ Should Ensure Use of App By Employees With ‘Compatible Mobile Phones,’” LiveLaw News Network, 17 de mayo, 2020, <https://www.livelaw.in/top-stories/aarogya-setu-mha-dilutes-mandatory-imposition-156921>

⁹ Patrick Howell O’Neill, “India is forcing people to use its covid app, unlike any other democracy,” MIT Technology Review, 7 de mayo, 2020,

<https://www.technologyreview.com/2020/05/07/1001360/india-aarogya-setu-covid-app-mandatory/>

¹⁰ Aditya Chunduru, “After MIT tech review downgrades Aarogya Setu rating, source code for app made public,” Deccan Chronicle, 27 de mayo, 2020,

<https://www.deccanchronicle.com/technology/in-other-news/270520/after-mit-tech-review-downgrades-aarogya-setu-rating-source-code-for.html>

¹¹ Cuenta de Twitter de Aarogya Setu, 5 de julio, 2020,

<https://twitter.com/SetuAarogya/status/1279634258072465409>

IV. IMPACTO EN LOS DERECHOS DE LOS USUARIOS

Si bien la preocupación principal respecto de los certificados digitales de salud sigue siendo, hasta el momento, la falta de una solución eficaz basada en evidencia, existen muchas otras preocupaciones sobre derechos humanos que deben tomarse en cuenta.

1. DERECHO A LA PRIVACIDAD

La mayoría de los certificados digitales de salud requerirían la recopilación de información personal sensible, lo que pone en riesgo la privacidad de las personas. La información de salud es privada y sensible por naturaleza y revela detalles íntimos sobre la vida de las personas. El uso, la recopilación, el acceso y cualquier otro procesamiento de esta información se deben proteger, idealmente, mediante una ley integral de protección de datos.¹² Sin embargo, la mayoría de los países que están considerando las propuestas de certificados digitales de salud cuentan con marcos de protección débiles o desactualizados o simplemente no cuentan con ningún marco de protección. Además, cabe mencionar que las soluciones centralizadas con un almacenamiento centralizado de la información, especialmente sin mecanismos adecuados de pesos y contrapesos para la compartición de datos dentro de los gobiernos y entre ellos, pueden generar sistemas de identificación descomunales pero frágiles, que pueden poner en riesgo la privacidad y la seguridad de los datos de las personas.

Los gobiernos deben abordar el asunto de los certificados digitales de salud con precaución, reconociendo los riesgos únicos de la recopilación de datos relacionados con la salud y otros datos personales sensibles, en especial cuando pueden ser recopilados, accedidos, o procesados por personas que no son profesionales de la salud. Nadie debería tener que comprometer su derecho fundamental a la privacidad para conservar el acceso a servicios esenciales o a la libertad de circulación.

Como mencionamos anteriormente, en la lucha contra el COVID-19, las autoridades públicas deberían ser capaces de contar con datos precisos, incluidos los datos de salud, para determinar cuáles serán las mejores acciones para mitigar la propagación del virus e identificar qué medidas se pueden tomar para proteger a las personas y sus derechos durante la crisis y una vez que esta termine. Sin embargo, el uso de estos datos debe estar

¹² Access Now, La creación de un marco para la protección de datos: Una guía para los legisladores sobre qué hacer y qué no, 2018. <https://www.accessnow.org/data-protection-handbook>

fundamentado en los principios de necesidad y proporcionalidad, lo cual se puede evaluar mediante un testeo de terceros. La recopilación y el uso de los datos deben:

1. Llevarse a cabo en consonancia con la ley o según lo prescrito por esta (principio de legalidad).
2. Ser necesarios para lograr un determinado objetivo (principio de necesidad).
3. Ser proporcionados para el objetivo que se quiere alcanzar (principio de proporcionalidad).

Distintas jurisdicciones en todo el mundo han ratificado estos principios al considerar las respuestas gubernamentales ante el COVID-19. Por ejemplo, la Corte Suprema de Israel resolvió que las fuerzas de seguridad no podrían aplicar capacidades de vigilancia para rastrear pacientes de COVID-19 sin aprobación legislativa y el Supervisor Europeo de Protección de Datos solicitó que todo uso de datos de ubicación esté regido por los principios de necesidad, proporcionalidad y efectividad.¹³

2. DERECHO A LA CIRCULACIÓN Y A LA LIBERTAD DE REUNIÓN

Los gobiernos y las empresas están considerando el uso de certificados digitales de salud para determinar quién puede viajar, tanto de manera interurbana como internacional, y quién puede tener acceso a espacios públicos, espacios de trabajo y lugares de ocio.¹⁴ En la mayoría de estos casos de uso, una persona no tendría permitido acceder a un área en particular a menos que cuente con un certificado de salud digital. Estas restricciones pueden afectar la capacidad de las personas para acceder a servicios esenciales, llevar a cabo sus actividades de subsistencia y participar en la vida ciudadana. Es de especial importancia contar con salvaguardas claras para la libertad de asociación y reunión pacífica, y para habilitar la

¹³ Noa Landau y Netael Bandel, Israel Secretly Sought To Expand Shin Bet Tracking of Coronavirus Patients Before Court Ruling (24 de junio, 2020),

<https://www.haaretz.com/israel-news/.premium-israel-secretly-sought-to-expand-tracking-of-coronavirus-patients-before-ruling-1.8801167>; https://twitter.com/EU_EDPS/status/1253623503254937600.

¹⁴ Consulte, p. ej., Saudi Press Agency, Kingdom's Government Sets Preventive, Precautionary Measures to Prevent COVID-19 Infection Transmission, Interior Ministry Says, <https://www.spa.gov.sa/viewstory.php?lang=en&newsid=2043855>, (7 de marzo, 2020); WorldAware, Saudi Arabia Maintaining Restrictions on Entry of Arrivals, <https://www.worldaware.com/saudi-arabia-maintaining-restrictions-entry-arrivals> (8 de marzo, 2020). En marzo de 2020, el gobierno de Arabia Saudita impuso una restricción en las personas que querían entrar desde países afectados por la pandemia de COVID-19, según una lista aprobada por las autoridades de salud. Al llegar a Arabia Saudita, estas personas debían presentar un certificado de Reacción en Cadena de la Polimerasa (PCR) que demostrara que no estaban infectados de COVID-19. El certificado de PCR debía haber sido emitido dentro de las 24 horas previas al abordaje del vuelo a Arabia Saudita y la aerolínea debía garantizar la validez del certificado.

circulación esencial para que prospere la justicia social, racial, económica y ambiental tanto *online* como *offline*.

Quienes están en el poder no deberían imponer esquemas de certificados digitales de salud que puedan ser utilizados para silenciar disidencias, oprimir movimientos sociales o ejercer control con propósitos distintos a los de la salud pública.

3. EXCLUSIÓN

Los certificados digitales de salud dependen tanto de la presencia general de una infraestructura digital como de un punto de conexión individual, como un teléfono celular. Estos requerimientos no son viables para muchas personas, en especial para aquellas en comunidades marginalizadas.¹⁵ Las personas que no cuentan con teléfonos celulares personales, las comunidades con insuficiente acceso a la infraestructura digital y las personas con problemas de alfabetización digital se enfrentarían a una exclusión masiva. Asimismo, obtener acceso a un certificado de salud digital puede acarrear costos. **El acceso a servicios esenciales y a la circulación no debe estar restringido para ninguna persona por su falta de acceso a infraestructura digital.**

4. DISCRIMINACIÓN

El COVID-19 ya ha tenido un impacto desproporcionado en las personas que sufren discriminación y marginalización. Desde las comunidades afroamericanas en los Estados Unidos hasta las comunidades indígenas en la región amazónica de Brasil, se han reportado más contagios y tasas de mortalidad más altas.¹⁶ Las comunidades que sufren discriminación a menudo cuentan con acceso reducido a una atención de salud efectiva, tienen trabajos que aumentan el riesgo a la exposición y tienen menores probabilidades de contar con acceso confiable a Internet en sus hogares, lo que dificulta que reciban información de salud pública crucial y cumplan con el distanciamiento social. Los certificados digitales de salud que restringen la circulación generan un alto de riesgo de reforzar y profundizar estas desigualdades existentes en el impacto del COVID-19. El gobierno de Chile reconoció dichos

¹⁵ Natalie Kofler y Françoise Baylis, “Ten reasons why immunity passports are a bad idea,” *Nature*, 21 de mayo, 2020, <https://www.nature.com/articles/d41586-020-01451-0>

¹⁶ Centros para el Control y la Prevención de Enfermedades, COVID-19 in Racial and Ethnic Minority Groups (25 de junio, 2020) <https://www.cdc.gov/coronavirus/2019-ncov/need-extra-precautions/racial-ethnic-minorities.html>; Dom Philips, “‘We are facing extermination’: Brazil losing a generation of indigenous leaders to Covid-19,” *The Guardian*, 21 de junio, 2020, <https://www.theguardian.com/global-development/2020/jun/21/brazil-losing-generation-indigenous-leaders-covid-19>

riesgos y suspendió la implementación del carnet COVID-19.¹⁷ Según el ministro de salud Jaime Mañalich, “el hecho de que una persona tenga un carnet COVID-19 podría darle ciertos privilegios en comparación con otra que no lo tenga, como la prioridad de ser contratada o recontratada, la entrada a espacios públicos y otras situaciones”.¹⁸

También ha habido múltiples casos de estigmatización y discriminación contra personas con COVID-19 en todo el mundo, lo que incluye discurso de odio en línea dirigido a muchos grupos vulnerables.¹⁹ Además de las restricciones legales, es probable que los certificados digitales de salud tengan un fuerte impacto social. Las personas que no los tengan podrían enfrentarse a discriminación injustificada por parte de pares, de la sociedad, de su lugar de trabajo y del gobierno.²⁰ En la India, por ejemplo, los dueños de farmacias se han apropiado de la aplicación Aarogya Setu de rastreo de contactos para uso no oficial, impidiendo el acceso de personas a sus tiendas a menos que mostraran tener instalada la aplicación en sus teléfonos.²¹ Una respuesta similar a los certificados digitales de salud podría generar una mayor discriminación, tanto de manera directa como involuntaria.

Los gobiernos, empleadores y otros actores que están considerando estas herramientas deben evaluar los mecanismos para contener la propagación del COVID-19 en base a su impacto desigual en aquellos que ya se enfrentan a riesgos más altos. En cuanto a los certificados digitales de salud, una herramienta cuya eficacia no se ha probado mediante ninguna medida, el riesgo de daños puede exceder considerablemente a los beneficios.

¹⁷ Cuenta de Twitter del Ministerio de Salud, 10 de mayo, 2020, <https://twitter.com/ministeriosalud/status/1259512225888448512>

¹⁸ “Gobierno posterga por posible “discriminación odiosa” entrega de polémico carnet Covid-19,” Diario La Prensa, 10 de mayo, 2020, <https://new.diariolaprensa.cl/index.php/2020/05/10/gobierno-posterga-por-posible-discriminacion-odiosa-entrega-de-polemico-carnet-covid-19/>

¹⁹ Access Now, Recomendaciones para los estados para combatir la desinformación y defender la libre expresión durante COVID-19, <https://www.accessnow.org/covid19-fighting-misinformation/>; Equality Labs, Coronajihad: An Analysis of COVID-19 Hate Speech and Disinformation, <https://www.equalitylabs.org/coronajihad/>

²⁰ Carr Center, Examining the Ethics of Immunity Certificates, https://carrcenter.hks.harvard.edu/files/cchr/files/005-covid_discussion_paper.pdf

²¹ Pranav Dixit, “For A Billion Indians, The Government’s Voluntary Contact Tracing App Might Actually Be Mandatory,” BuzzFeed News, 30 de abril, 2020, <https://www.buzzfeednews.com/article/pranavdixit/for-a-billion-indians-the-governments-voluntary-contact>

5. CREACIÓN DE UNA INFRAESTRUCTURA DE VIGILANCIA DE SALUD PERMANENTE

Si bien el uso de certificados digitales de salud se propone como medida temporal y única para combatir el COVID-19, existe una amenaza real de que la infraestructura resultante pueda volverse permanente o se integre a programas de identificación digital existentes o sistemas de vigilancia fronteriza. Debemos evitar que la crisis se convierta en una “oportunidad” para establecer una infraestructura de vigilancia de salud en todo el mundo.

Por ejemplo, en este momento, el Reino Unido está activamente considerando el uso de certificados de inmunidad en el país como medida para abrir las actividades luego del confinamiento.²² Hay cada vez más preocupaciones que surgen a partir de que estas iniciativas podrían terminar convirtiéndose en un portal hacia la capacidad de las personas de acceder a servicios, empleos y espacios públicos. Además, estas iniciativas pueden ser “exploraciones iniciales” en el sistema de Identidad de Salud Pública (PHI, por sus siglas en inglés), donde se puede crear una infraestructura de salud permanente que exija que se comparta la información médica privada para cuestiones relacionadas con la salud pública.²³

Además de los marcos sólidos para la protección de datos *durante* la crisis de COVID-19, **los gobiernos y demás actores que recopilen o reutilicen los datos como parte de una respuesta ante el COVID-19 deben adoptar plazos claros para la eliminación de los datos de salud y otra información sensible, incluida la geolocalización y la información sobre contactos personales y redes comunitarias.**

²² Chris Smyth y Tom Whipple, “Immunity forms planned for coronavirus survivors,” The Times, 22 de mayo, 2020, <https://www.thetimes.co.uk/article/immunity-forms-planned-for-coronavirus-survivors-6gz0szlhw>

²³ Imogen Parker y Elliot Jones, “Something to declare? Surfacing issues with immunity certificates,” Ada Lovelace Institute, 2 de junio, 2020, <https://www.adalovelaceinstitute.org/something-to-declare-surfacing-issues-with-immunity-certificates/>

VI. CONCLUSIÓN

La respuesta ante el COVID-19 ha impulsado muchas soluciones y enfoques de los diversos sectores. Se debe lidiar con esta crisis sin precedentes mediante soluciones innovadoras y audaces centradas en la protección de la salud y los derechos de las personas. Sin embargo, debemos estar alertas ante la tendencia de tomar de blanco a las personas en lugar de al virus. Toda medida contra el COVID-19 debe proteger los derechos de las personas, ya que solo así podremos ser capaces de idear soluciones sostenibles para esta crisis.

En particular, los gobiernos y demás actores que consideren el uso de los certificados digitales de salud como parte de su respuesta ante el COVID-19 deberían, ante todo, avanzar con propuestas basadas en evidencia científica sólida sobre su efectividad, creadas con tecnologías revisadas en cuanto a su seguridad y estabilidad, y diseñadas para mitigar los impactos en los derechos humanos, en especial para aquellos que sean más vulnerables.

"Pedir a las personas que elijan entre la privacidad y la salud es, en realidad, el origen del problema. Porque representa un dilema falso. Podemos y debemos gozar de ambos. Podemos proteger nuestra salud y detener la epidemia del coronavirus sin necesidad de implementar regímenes totalitarios de vigilancia, sino empoderando a los ciudadanos". — Yuval Noah Harari²⁴

²⁴ Yuval Noah Harari, "The world after coronavirus," Financial Times, 20 de marzo, 2020, <https://www.ft.com/content/19d90308-6858-11ea-a3c9-1fe6fedcca75>

Para obtener más información, comuníquese con:

Naman M. Aggarwal | Global Digital Identity Lead, Access Now | naman@accessnow.org