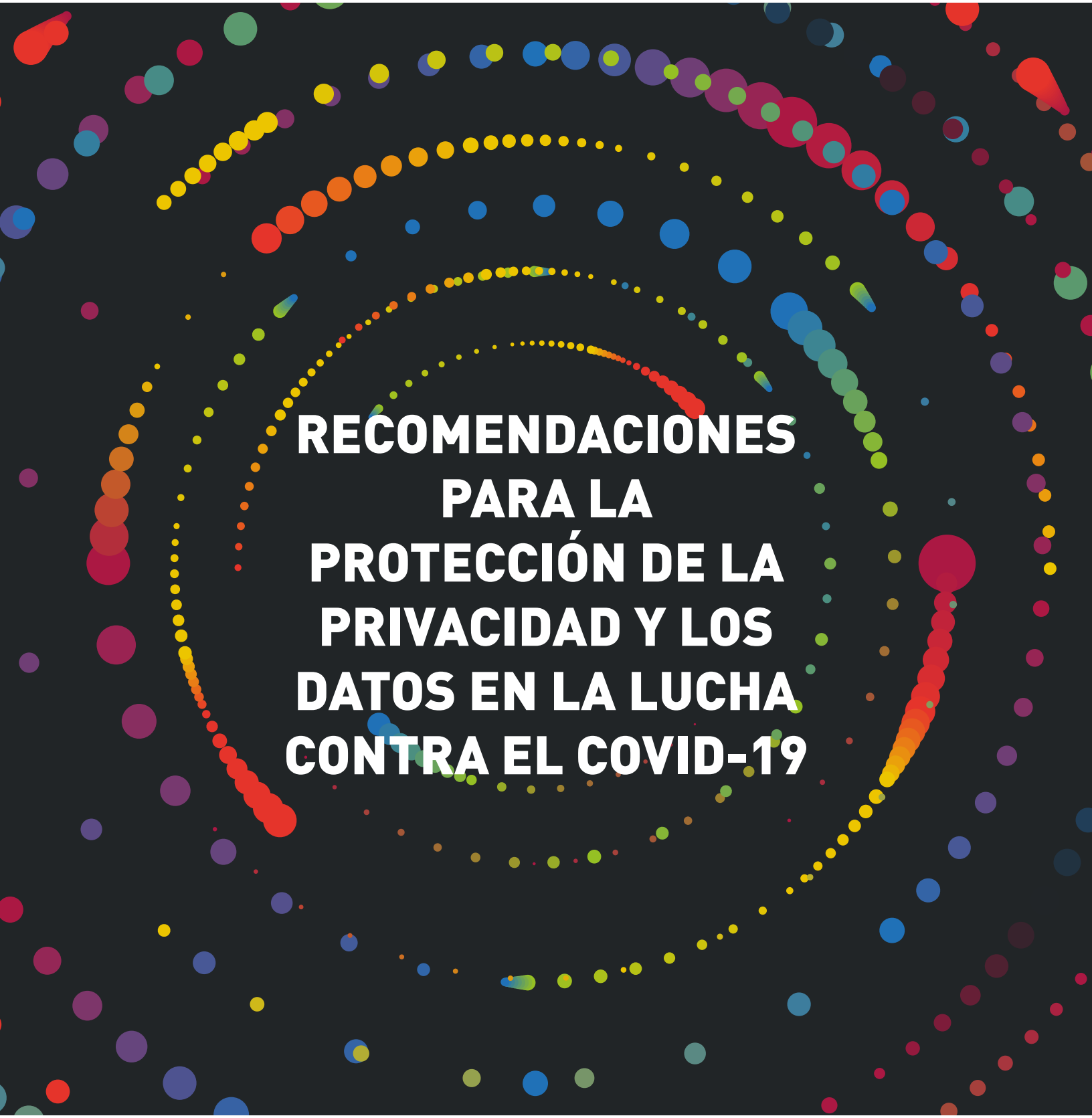

RECOMENDACIONES PARA LA PROTECCIÓN DE LA PRIVACIDAD Y LOS DATOS EN LA LUCHA CONTRA EL COVID-19

accessnow

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 y eventos como RightsCon, luchamos por los derechos humanos en la era digital.

Recomendaciones para la protección de la privacidad y los datos en la lucha contra el COVID-19

MARZO DE 2020

ÍNDICE

I. RESUMEN EJECUTIVO

Access Now se encuentra comprometida a proteger los derechos humanos y a colaborar con las respuestas de los gobiernos frente al brote de la enfermedad del coronavirus (COVID-19). Estas respuestas deben promover la salud pública, evitar la discriminación, garantizar el acceso a información confiable y oportuna, defender el acceso sin restricciones a una Internet libre, asequible y segura, asegurar la libertad de expresión y opinión y proteger la privacidad y los datos personales.

Las leyes nacionales e internacionales reconocen que las circunstancias extraordinarias requieren medidas extraordinarias. Esto significa que es posible que algunos derechos fundamentales, incluidos los derechos a la privacidad y la protección de datos, puedan encontrarse restringidos a fin de abordar la crisis de salud actual, siempre que se apliquen los principios democráticos básicos, así como una serie de salvaguardas, y que la interferencia sea lícita, temporal y no arbitraria.

Los gobiernos, las empresas, las ONG y los individuos de dichas entidades tienen la responsabilidad de colaborar para mitigar las consecuencias del COVID-19 y mostrar solidaridad y respeto entre sí. En este artículo, brindaremos algunas **recomendaciones para los gobiernos sobre cómo proteger la privacidad y los datos** en la lucha contra el COVID-19, sin descuidar los derechos de las personas.

El brote de COVID-19 dejará secuelas. Y las medidas que adopten los gobiernos ahora determinarán su alcance. Las recomendaciones que se describen a continuación ayudarán a los gobiernos a garantizar la protección del imperio de la ley, así como los derechos a la protección de datos y la privacidad, tanto en esta crisis como en el futuro.

> *"Debemos tener presente en todo momento, especialmente a la hora de recopilar información sobre ciudadanos particulares o rastrear sus ubicaciones o desplazamientos, que siempre hay implicancias críticas en la protección de datos".* — Michael Ryan, director ejecutivo del Programa de Emergencias de Salud de la Organización Mundial de la Salud; 26 de marzo de 2020.[1]

[1] Organización Mundial de la Salud. *Conferencia de prensa virtual sobre el COVID-19; 25 de marzo de 2020.* https://www.who.int/docs/default-source/coronaviruse/transcripts/who-audio-emergencies-coronavirus-press-conference-full-25mar2020.pdf

Este informe es una publicación de Access Now. Fue escrito por Estella Massé. Queremos agradecer a los miembros del equipo de Access Now que colaboraron, entre ellos, Naman Aggarwal, Verónica Arroyo, Jennifer Brody, Sage Cheng, Fanny Hidvégi, Lucie Krahulcova, Peter Micek, Eric Null, Javier Pallero, Eliska Pirkova, Gaspar Pisanu, Dima Samaro, Raman Jit Singh Chima, Berhan Taye y Donna Wentworth.

II. INTRODUCCIÓN

A fines de 2019, el mundo comenzó la batalla contra la enfermedad del coronavirus (COVID-19). En respuesta a lo que la Organización Mundial de la Salud denominó como pandemia, los gobiernos de todo el mundo comenzaron a utilizar distintas tecnologías para contener la propagación del virus y preservar la salud de las personas. Pero a pesar del apremio, las medidas que impliquen restricciones a los derechos de las personas deben tratarse con cautela y considerarse extraordinarias.

Este artículo se centra en tres categorías de medidas que han adoptado las autoridades alrededor del mundo: (1) recopilación y uso de datos de salud, (2) rastreo y geolocalización y (3) asociaciones entre entidades públicas y privadas. A continuación, presentamos un resumen de las medidas existentes y brindamos recomendaciones específicas para cada categoría a fin de ayudar a los gobiernos a abordar esta importante crisis de salud pública sin descuidar los derechos de las personas.[2]

DESARROLLO DE POLÍTICAS PÚBLICAS EN TIEMPOS DE CRISIS: Qué pautas debemos respetar cuando la excepción se convierte en la norma

En medio de una pandemia global, como lo es la del COVID-19, los gobiernos pueden adquirir facultades especiales para tomar medidas extraordinarias con el fin de prevenir y mitigar la crisis

[2] Para obtener más información sobre las medidas adoptadas en distintas partes del mundo, consulte: Privacy International. *Tracking the Global Response to COVID-19,* 2020. https://privacyinternational.org/examples/tracking-global-response-covid-19

sanitaria en función de las leyes internacionales de derechos humanos y los estándares constitucionales domésticos adicionales.[3]

¿Qué normas se pueden aplicar?

Las medidas y los poderes extraordinarios se definen estrictamente como regímenes de excepción de las constituciones nacionales y los ordenamientos jurídicos, aceptados por las leyes internacionales y regionales de derechos humanos (incluido el Artículo 4 del Pacto Internacional de Derechos Civiles y Políticos, el Artículo 15 de la Convención Europea de Derechos Humanos y el Artículo 27 de la Convención Americana sobre Derechos Humanos.[4]

¿Cuándo y cómo los estados pueden utilizar poderes extraordinarios?

Estas normas permiten a los estados suspender sus obligaciones de garantizar ciertos derechos y libertades, siempre que sea en circunstancias excepcionales y de forma limitada y supervisada. Para ello, la ley define las circunstancias en que un estado puede suspender sus obligaciones, establece límites para las medidas que se pueden tomar, protege ciertos derechos fundamentales de cualquier tipo de restricción y, por último, establece los requisitos procedimentales que los estados deben cumplir.

Algunos derechos no admiten ningún tipo de suspensión, como el derecho a la vida, la prohibición de la tortura y los castigos o los actos humillantes o inhumanos, la prohibición de la esclavitud y el principio de "no hay castigo sin ley previa".

¿Cómo se deben aplicar las medidas extraordinarias y cuáles son los límites de estos poderes?

Un régimen de excepción como una declaración de estado de emergencia o peligro no es una situación extralegal, sino que el imperio de la ley debe permanecer vigente, y se deben establecer

[3] United Nation Human Rights Office of the High Commissioner. *COVID-19: States should not abuse emergency measures to suppress human rights,* 2020. https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=25722&LangID=E; Michele Bachelet. *Coronavirus: Human rights need to be front and centre in response,* 2020. https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx; and Council of Europe. *We must respect human rights and stand united against the coronavirus pandemic*, 2020. https://www.coe.int/en/web/commissioner/-/we-must-respect-human-rights-and-stand-united-against-the-coronavirus-pandemic.

[4] European Court of Human Rights. *Guide on Article 15 of the European Convention on Human Rights*, 2019. https://www.echr.coe.int/Documents/Guide_Art_15_ENG.pdf

limitaciones de tiempo y de alcance.[5] Un estado de excepción no hace lícita a cualquier medida que se adopte en consecuencia.

Los regímenes de excepción y las medidas correspondientes se deben establecer por escrito y se deben transmitir y compartir a gran escala en los idiomas y los foros adecuados. Además, deben contar con una cláusula de caducidad, ya que las medidas con duración indefinida no son aceptables. Si bien las prórrogas son posibles ante la necesidad, las disposiciones extraordinarias deben ser limitadas respecto de su severidad, duración y alcance geográfico. Una vez que finalice el régimen de excepción, los gobiernos y las autoridades deben tomar todas las medidas necesarias para recuperar el orden habitual lo antes posible.

Los derechos humanos fundamentales se deben seguir respetando durante los regímenes de excepción o los períodos de emergencia. Las restricciones de derechos solo deben aplicarse cuando esto sea necesario para prevenir y mitigar los riesgos que provoca la crisis en cuestión, y las medidas restrictivas no deben extenderse más allá del alcance estrictamente necesario y proporcional para las exigencias de las circunstancias.

III. RECOPILACIÓN Y USO DE DATOS DE SALUD

La información de salud es privada y sensible por naturaleza y revela detalles íntimos sobre la vida de las personas. El uso, la recolección y cualquier otro procesamiento de esta información se deben proteger, idealmente, mediante una ley integral de protección de datos.[6] El uso de la información de salud (que comprende el tipo de sangre, las condiciones médicas preexistentes, la información sobre el género y los registros de temperatura corporal, entre otros datos) se encuentra, por lo general, estrictamente limitado. No obstante, en una crisis de la salud pública, el dilema no es *si* los gobiernos pueden usar los datos de salud para ayudar a combatir la crisis, sino *cómo* deben hacerlo para garantizar la dignidad y la privacidad individual en la mayor medida posible.

Defender los derechos digitales también ayuda a proteger la salud pública. Según el Comité de Derechos Económicos, Sociales y Culturales de la ONU, "El derecho a la salud se encuentra estrechamente relacionado y ligado al cumplimiento de otros derechos humanos, tal como

[5] Hungarian Civil Liberties Union. *Unlimited power is not the panacea*, 2020. https://hclu.hu/en/articles/unlimited-power-is-not-the-panacea

[6] 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

se indica en la Carta Internacional de Derechos Humanos, lo que incluye el derecho al alimento, la vivienda, el trabajo, la educación, la dignidad, la vida, la no discriminación, la igualdad, la prohibición de la tortura, la privacidad, el acceso a la información y las libertades de asociación, reunión y movimiento. Estos y otros derechos y libertades son componentes integrales del derecho a la salud".[7]

En la lucha contra el COVID-19, las autoridades públicas deben poder confiar en los datos, incluidos los datos de salud, a fin de determinar el mejor procedimiento para mitigar la expansión del virus e identificar qué medidas se deben adoptar para proteger a las personas y sus derechos durante y después de la crisis. Las disposiciones aplicadas deben ser transparentes, necesarias y proporcionadas. Además, cuando existan leyes de privacidad y protección de datos, estas deben incluir excepciones claras que se apliquen a las crisis de salud pública a fin de permitir un uso más permisivo del habitual.

> *"En una crisis de la salud pública, el dilema no es si los gobiernos pueden usar los datos de salud para ayudar a combatir la crisis, sino cómo deben hacerlo".*

CASOS PRÁCTICOS

En muchos países, las autoridades gubernamentales y las entidades privadas han publicado datos de salud con el propósito de informar al público y brindar a las personas la oportunidad de evaluar si han estado en contacto con algún individuo infectado. Desafortunadamente, debido a la especificidad de los datos publicados (que, generalmente, no incluyen el nombre, pero sí otros identificadores únicos), otras personas han podido identificar a los individuos infectados y sus familiares. Divulgar información relacionada con la salud durante la crisis del COVID-19 (incluidos los resultados positivo o negativo de una persona) no solo incrementa los desafíos relacionados con la protección de la privacidad y los datos personales, sino que también pone en peligro la seguridad y el orden público, genera riesgos de discriminación y hasta puede provocar ataque físicos o en línea y amenazas de muerte.[8]

[7] Comité de Derechos Económicos, Sociales y Culturales de la ONU. *The right to the highest attainable standard of health,* 2000. https://apps.who.int/disasters/repo/13849_files/o/UN_human_rights.htm
[8] The New York Times. *As Coronavirus Surveillance Escalates, Personal Privacy Plummets*, 2020. https://www.nytimes.com/2020/03/23/technology/coronavirus-surveillance-tracking-privacy.html

A continuación, presentamos algunos casos prácticos que ilustran distintos usos de los datos de salud en la lucha contra el COVID-19 alrededor del mundo. Para cada ejemplo, brindamos recomendaciones a los gobiernos sobre cómo usar esta información de forma responsable y acorde con las leyes de derechos humanos.

América Latina	En **Argentina**, un periódico publicó datos personales de las personas infectadas con COVID-19, incluidos su edad, el lugar al que habían viajado, el hospital en que se habían tratado, entre otros.[9] Después de que el público advirtió y criticó esta publicación, los nombres dejaron de estar disponibles.
	El Instituto Nacional de Salud del **Perú** desarrolló una plataforma en la que los usuarios podían consultar los informes de salud de los pacientes a los que se les había realizado la prueba del COVID-19 con solo ingresar su documento nacional de identidad. Por lo tanto, durante algunos días, esta información estuvo disponible para el público general, no solo los pacientes.[10] Tras recibir numerosas críticas, las autoridades nacionales incluyeron un segundo autenticador. Ahora, para acceder a la plataforma, los usuarios deben proporcionar un código enviado por SMS.[11]
Asia Pacífico	En **India**, al menos dos gobiernos estatales (incluidos el estado de Karnataka, donde se encuentra el centro tecnológico de Bangalore) publicaron archivos PDF en línea con los nombres, domicilios e historial de viaje de las personas con orden de cuarentena por COVID-19.[12] La información se encuentra disponible para el público general.

[9] La Nación. *Quiénes son y de dónde vinieron los 21 infectados por coronavirus en la Argentina*, 2020. https://www.lanacion.com.ar/sociedad/quienes-son-17-infectados-coronavirus-argentina-nid2341456
[10] Perú. *Instituto Nacional de Salud.* https://ins.gob.pe/resultado_coronavirus/
[11] Perú. *Debilidades de plataforma del Ministerio de Salud exponen información de pacientes COVID-19*, 2020. https://saludconlupa.com/noticias/peru-debilidades-de-plataforma-del-ministerio-de-salud-pueden-exponer-informacion-clinica-de-pacientes-covid-19/
[12] Bangalore Mirror. *Government publishes details of 19,240 home-quarantined people to keep a check,* 2020. https://bangaloremirror.indiatimes.com/bangalore/others/government-publishes-details-of-19240-home-quarantined-people-to-keep-a-check/articleshow/74807807.cms

Norteamérica	Frank King, ciudadano de **EE.UU.**, estaba en un crucero en Cambodia cuando lo identificaron de forma errónea como portador de COVID-19. Aunque los resultados de la prueba de King finalmente se corrigieron, y se determinó que todos los pasajeros del crucero se encontraban sanos, al regresar a EE.UU., recibió amenazas de muerte y ataques personales, tanto en línea como fuera de línea, durante varias semanas.[13] También en **EE.UU.**, más de 2000 trabajadores médicos de emergencias del University of California San Francisco Medical Center y el Zuckerberg San Francisco General Hospital participarán en un estudio que implica utilizar un anillo inteligente para identificar de forma anticipada a las personas con COVID-19. Los anillos se entregarán a los profesionales médicos de emergencia que entren en contacto con pacientes que puedan padecer de COVID-19. Este dispositivo, que los trabajadores deberán utilizar por tres meses, recopila información como el ritmo cardíaco, la frecuencia respiratoria y los cambios en la temperatura corporal de los pacientes. No obstante, no se ha comprobado que detecte el COVID-19.[14]

RECOMENDACIONES

Aplicar los principios y derechos a la privacidad y la protección de datos	Los gobiernos y las empresas deben aplicar los siguientes principios de privacidad y protección de datos: ➔ **Limitación de las finalidades y minimización de los datos:** La recopilación de datos de salud, así como su uso, divulgación, almacenamiento y otros procesamientos, deben limitarse a lo estrictamente necesario para la lucha contra el virus. Una pandemia no es una excusa para recopilar grandes cantidades de datos innecesarios. ➔ **Limitación del acceso y seguridad de los datos:** El acceso a los datos de salud debe limitarse a quienes necesitan esta información para realizar tratamientos, investigaciones o acciones de otros tipos para abordar la crisis. Estos datos se deben almacenar de manera segura en una base de datos separada.

[13] The New York Times. *What It's Like to Come Home to the Stigma of Coronavirus,* 2020. https://www.nytimes.com/2020/03/04/us/stigma-coronavirus.html
[14] The Verge. *New study aims to use health data from a smart ring to identify coronavirus symptoms,* 2020. https://www.theverge.com/2020/3/23/21191225/coronavirus-smart-ring-oura-ucsf-san-francisco-general-hospital-tempredict

- ➔ **Retención de datos e investigaciones futuras:** Los datos procesados en respuesta a la crisis solo se deben conservar mientras esta se encuentre vigente. Una vez finalizada la pandemia, se debe borrar la mayor parte de la información sanitaria, aunque algunos datos no identificables pueden retenerse con fines de de investigación y registro histórico. Estos datos solo deben ser accesibles y utilizados con estos fines de interés público.
- ➔ **Venta de los datos de salud:** Bajo ninguna circunstancia los datos de salud se deben vender o transferir a terceros que no trabajen en áreas de interés público.

Cuando se producen crisis de salud pública e independientemente de si el país tiene leyes vigentes de privacidad y protección de datos, los derechos de privacidad y datos no deben desprotegerse en ningún momento. Los principios centrales y los derechos de los usuarios se deben respetar en todo momento. Cuando hay leyes de privacidad y protección de datos, estas suelen incluir excepciones claras para las crisis de salud pública, pero también brindan un marco de seguridad para esta mayor capacidad de procesamiento de datos.

Por último, recomendamos a los gobiernos que sigan los lineamientos de las autoridades independientes de privacidad y protección de datos. Las autoridades de México, Argentina y la Unión Europea, entre otros, publicaron lineamientos para abordar el uso de la información sanitaria de conformidad con las leyes de protección de datos.[15]

[15] Infobae. *Coronavirus en México: el INAI emitió recomendaciones sobre el manejo de datos de los enfermos para garantizar su seguridad*, 2020. https://www.infobae.com/america/mexico/2020/03/14/coronavirus-en-mexico-el-inai-emitio-recomendaciones-sobre-el-manejo-de-datos-de-los-enfermos-para-garantizar-su-seguridad/ Agencia de Acceso a la Información Pública. *Tratamiento de datos personales ante el Coronavirus*, 2020. https://www.argentina.gob.ar/noticias/tratamiento-de-datos-personales-ante-el-coronavirus European Data Protection Board. *Statement on the processing of personal data in the context of the COVID-19 outbreak*, 2020. https://edpb.europa.eu/our-work-tools/our-documents/other/statement-processing-personal-data-context-covid-19-outbreak_en

No divulgar públicamente datos identificables acerca de los pacientes infectados y curados	Los informes de casos de infección del virus y estadísticas relacionadas no deben revelar datos personales acerca de los pacientes. Específicamente, no se debe divulgar la información identificable, en especial, el nombre, la fecha de nacimiento o el domicilio, de las personas afectadas por el virus. Estas medidas ponen en peligro el orden público y suponen riesgos para los individuos. Además, la divulgación privada de esta información debe llevarse a cabo con precaución, ya que las entidades privadas pueden tener intenciones de monetizar estos datos de maneras que no cumplan con los principios de privacidad.
Involucrar a expertos y a la sociedad civil	Siempre que se recopile información personal y sensible, los gobiernos deben involucrar a las comunidades de expertos en privacidad y salud que colaboren en el desarrollo y la implementación de mecanismos de seguridad para el uso de datos, especialmente, en los países que no cuentan con autoridades sólidas de protección de datos o privacidad. Las comunidades con riesgo de marginalización, incluidas las mujeres y las niñas, los discapacitados, las personas de comunidades indígenas, las personas de bajos recursos, la comunidad LGBTQ y las minorías religiosas o étnicas, con frecuencia sufren de discriminación y no tienen acceso a servicios de atención médica. Por lo tanto, estos grupos también deben consultarse a la hora de crear salvaguardas específicas efectivas.
Todas las medidas de respuesta a crisis deben ser transparentes, necesarias y proporcionadas	Una pandemia no es una oportunidad para reducir la transparencia. Si bien la transparencia en sí misma no es suficiente para proteger la privacidad de los individuos, las personas aún deben tener la posibilidad de comprender qué sucederá con sus datos en el caso de una crisis de salud. Asimismo, las medidas que se tomen como respuesta a la pandemia deben ser necesarias y proporcionadas a fin de garantizar que ayuden a resolver la crisis sin sacrificar la privacidad individual.

IV. RASTREO Y GEOLOCALIZACIÓN

Los datos de ubicación revelan una gran cantidad de información. Tan solo hacer un seguimiento de los movimientos de una persona mediante los datos de ubicación que procesa un teléfono inteligente permite deducir su domicilio y lugar de trabajo, sus

interacciones con otras personas, sus visitas al médico y su nivel socioeconómico, entre otros datos. Y si no se aplican los mecanismos de protección adecuados, las herramientas de rastreo y geolocalización pueden permitir procesos de vigilancia ubicuos.

En el contexto de una crisis de salud pública, como la del brote de COVID-19, es posible que algunos gobiernos deseen utilizar la geolocalización para hacer un seguimiento de la evolución del virus y planificar sus respuestas. Sin embargo, estos mecanismos de seguimiento conllevan una gran cantidad de aspectos problemáticos. En primer lugar, es importante tener en cuenta que el rastreo de la ubicación geográfica de los teléfonos inteligentes proporciona información sobre el movimiento de los *teléfonos de las personas*, no del virus. Hacer un seguimiento de la evolución de la enfermedad mediante referencias cruzadas entre los datos geográficos de las personas con los casos de infección conlleva riesgos inherentes. En segundo lugar, incluso la supuesta "información de ubicación anónima" se puede reidentificar fácilmente; un estudio de 2013 demostró que las personas se podían volver a identificar a partir de solo cuatro puntos de observación.[16] Tercero, la ubicación geográfica no siempre es útil. Las personas pueden conducir, caminar, tomar el metro o trabajar en el 50.° piso de un edificio de 80 pisos, de modo que, además de sacrificar la privacidad de las personas, esta información no es completa.[17] Por último, los casos previos de uso de registros telefónicos y datos de ubicación para responder a crisis humanitarias demostraron no se efectivos ni eficientes.[18] Por lo tanto, la geolocalización destinada a abordar la propagación del virus solo se debe emplear de un modo respetuoso de los derechos que promueva la confianza en los gobiernos y proteja la seguridad individual. Esto ayudará a evitar que estas medidas escalen hasta convertirse en mecanismos de vigilancia masiva patrocinados por el estado.[19]

> *"La información que brinda la ubicación geográfica de las personas no es completa y sacrifica la privacidad de las personas".*

[16] Wired. *Anonymized Phone Location Data Not So Anonymous, Researchers Find*, 2013. https://www.wired.com/2013/03/anonymous-phone-location-data/
[17] Lawfare. *Location Surveillance to Counter COVID-19: Efficacy Is What Matters*, 2020. https://www.lawfareblog.com/location-surveillance-counter-covid-19-efficacy-what-matters
[18] CIS-India. *Ebola: A big data disaster,* 2016. https://cis-india.org/papers/ebola-a-big-data-disaster
[19] European Data Protection Board. *Processing of personal data in the context of the COVID-19 outbreak*, 2020. https://edpb.europa.eu/news/news/2020/statement-edpb-chair-processing-personal-data-context-covid-19-outbreak_en

CASOS PRÁCTICOS

En muchos países, las autoridades gubernamentales y entidades privadas rastrean los movimientos de las personas con el fin de hacer un seguimiento de "la expansión del virus" o para implementar los toques de queda o las medidas de confinamiento. Debido a la falta de protocolos de seguridad adecuados, la medidas de rastreo exponen información privada que no es necesariamente relevante en la lucha contra el coronavirus y que someten a toda la población a una situación de monitoreo y vigilancia.

A continuación, presentamos algunos estudios de caso regionales acerca del uso del rastreo y la geolocalización en la lucha contra el brote de COVID-19. Para cada ejemplo, brindamos recomendaciones a los gobiernos sobre cómo usar esta información de forma responsable y acorde con las leyes de derechos humanos.

África	En **Kenia**, el gobierno implementó medidas de "vigilancia electrónica" para rastrear a los individuos con orden de permanecer aislados durante 14 días debido a un viaje reciente. Distintas fuentes confirmaron a *The Standard* que, mediante el monitoreo de la actividad de los teléfonos celulares de estos viajeros (incluida la ubicación geográfica), el gobierno logró identificar a aquellos que incumplieron el aislamiento obligatorio. A estos individuos, también se les ordenó no apagar sus teléfonos móviles y llevarlos siempre consigo.[20] En **Sudáfrica**, por orden el Ministerio de Comunicaciones, Telecomunicaciones y Servicios Postales, los proveedores de servicios de telecomunicaciones acordaron compartir los datos de ubicación de los clientes con el gobierno. Aún no queda claro si se trata de los datos geográficos de los casos confirmados o los de toda la población. El ministro afirmó que "la industria acordó colectivamente brindar servicios de analítica de datos a fin de ayuda al gobierno a triunfar en… [la lucha contra el virus]".[21]

[20] The Standard Media. *State Taps Phones of Isolated Cases,* 2020. https://www.standardmedia.co.ke/article/2001365401/state-taps-phones-of-isolated-cases
[21] Business Insider SA*. South Africa will be Tracking Cellphones to Fight the Covid-19 Virus. 2020.* https://www.businessinsider.co.za/south-africa-will-be-tracking-cellphones-to-fight-covid-19-2020-3

América Latina	A través de un decreto de estado de emergencia, el presidente de **Ecuador** ordenó que los datos satelitales y de teléfonos móviles estuviesen disponibles para el monitoreo de la ubicación de las personas en cuarentena o con orden de aislamiento obligatorio.[22] En una declaración, las organizaciones de la sociedad civil le pidieron al gobierno mayor transparencia y medidas de seguridad en torno al decreto.[23]
Asia Pacífico	En **Corea del Sur**, el gobierno rastrea y publica en línea datos de ubicación detallados de los pacientes con infecciones confirmadas o sospechadas del virus.[24] Mediante la combinación de bases de datos existentes, se crean nuevos conjuntos de datos que permiten hacer un seguimiento dinámico de estas personas a través de grabaciones de CCTV, los registros de las tarjetas de crédito y los historiales de ubicación. La información publicada en línea incluye una gran cantidad de datos de estos individuos, como detalles sobre su lugar de trabajo, si utilizaron barbijos en el metro, los nombres de las estaciones en las que cambiaron de tren, los salones de masajes o los bares de karaoke que frecuentan y los nombres de las clínicas en que se realizaron la prueba. Según informes de The New York Times, acosadores cibernéticos utilizaron esta información para identificar a los pacientes por su nombre y hostigarlos.[25] **Taiwán** monitorea las redes móviles activamente para asegurar el cumplimiento de la cuarentena domiciliaria por parte de las personas recién llegadas de viaje y los individuos de riesgo. Para ello, las autoridades públicas reciben alertas cuando el dispositivo móvil de uno de estos individuos se encuentra activo fuera de su domicilio. Esta medida implica que existe un vínculo documentado entre la identidad de cada sujeto, su número de teléfono y su domicilio de residencia, el cual también incluye datos sobre sus cohabitantes.[26] Para evitar que las personas en cuarentena incumplan esta medida, las autoridades públicas llaman a su número

[22] El Comercio. *Lenín Moreno decreta el estado de excepción en Ecuador por el covid-19*, 2020. https://www.elcomercio.com/actualidad/moreno-medidas-coronavirus-covid19-excepcion.html
[23] Asociación para el Progreso de las Comunicaciones. *Ecuador: Las tecnologías de vigilancia en contexto de pandemia no deben poner en riesgo los derechos humanos*, 2020. https://www.apc.org/es/pubs/ecuador-las-tecnologias-de-vigilancia-en-contexto-de-pandemia-no-deben-poner-en-riesgo-los
[24] The New York Times. *As Coronavirus Surveillance Escalates, Personal Privacy Plummets*, 2020. https://www.nytimes.com/2020/03/23/technology/coronavirus-surveillance-tracking-privacy.html
[25] The New York Times. *As Coronavirus Surveillance Escalates, Personal Privacy Plummets*, 2020. https://www.nytimes.com/2020/03/23/technology/coronavirus-surveillance-tracking-privacy.html
[26] Reuters. *Taiwan's new 'electronic fence' for quarantines leads wave of virus monitoring*, 2020. https://www.reuters.com/article/us-health-coronavirus-taiwan-surveillanc-idUSKBN2170SK

	telefónico (dos veces al día, según indican los informes) a fin de verificar que el individuo en cuestión no haya salido de su domicilio sin su dispositivo móvil.

Europa	En toda la Unión Europea, las empresas de telecomunicaciones y las autoridades públicas están realizando acuerdos de intercambio de datos de ubicación. Hasta el momento, es escasa la transparencia respecto de qué datos se compartirán y cuánto tiempo durarán estos acuerdos, que suelen ser extralegales. También es poco claro si las empresas están proporcionando registros de los metadatos o si permiten a los gobiernos llevar a cabo un monitoreo de las personas en tiempo real: ➔ En **Bélgica**, las empresas de telecomunicaciones como Orange y Proximus aceptaron compartir "parte de su base de datos" para ayudar a las autoridades a afrontar el brote de coronavirus.[27] ➔ En **Alemania**, Deutsche Telekom proporciona parte de sus datos de ubicación a la Agencia Federal de Prevención de Enfermedades para ayudar a contener la pandemia. Además de los gobiernos nacionales, la Comisión Europea solicitó los metadatos agregados a los operadores de telecomunicaciones para "hacer un seguimiento de la expansión del virus" y determinar dónde es más apremiante la necesidad de suministros médicos.[28] Actualmente, este pedido no se basa en un requerimiento legal y, por lo tanto, no se puede someter a escrutinio.

Norteamérica	En **Estados Unidos**, los investigadores utilizan datos de Facebook para medir el distanciamiento social.[29] Los datos recopilados a partir de los usuarios de esta plataforma que tienen el historial de ubicaciones activado se utilizan para desarrollar mapas de datos agregados desidentificados. Este proyecto presenta riesgos significativos para la privacidad y la protección de datos, ya que da por hecho que los usuarios de Facebook aceptan que la plataforma realice un seguimiento de su actividad durante la lucha contra el coronavirus.

[27] Le Soir. *Coronavirus: le cabinet De Block dit «oui» à l'utilisation des données télécoms*, 2020. https://plus.lesoir.be/286535/article/2020-03-12/coronavirus-le-cabinet-de-block-dit-oui-lutilisation-des-donnees-telecoms

[28] Politico. *Commission tells carriers to hand over mobile data in coronavirus fight,* 2020. https://www.politico.eu/article/european-commission-mobile-phone-data-thierry-breton-coronavirus-covid19/

[29] Protocol. *Facebook data can help measure social distancing in California*, 2020. https://www.protocol.com/facebook-data-help-california-coronavirus

RECOMENDACIONES	
Considerar todas las opciones posibles para hacer un seguimiento de la expansión del virus	Algunos países decidieron no adoptar medidas de rastreo y geolocalización y, en cambio, optaron por realizar un rastreo personal de los contactos. Este método, además de funcionar para identificar a las personas infectadas a gran escala, supone menos riesgos para el derecho a la privacidad y permite hacer un seguimiento preciso del avance del virus.
Tener en cuenta que los datos de ubicación pueden ser incorrectos	El uso de datos de ubicación para determinar si las personas estuvieron en contacto con otros individuos infectados por el virus presenta varias limitaciones. El rastreo de ubicación mediante torres de telefonía celular no ofrece granularidad. Puede brindar información de ubicación general, de modo que puede proporcionar datos de localización aproximados, pero no puede detectar si dos teléfonos estuvieron a dos metros de distancia, lo cual sería necesario para generar datos relevantes en el caso del COVID-19. Las señales de GPS podrían ofrecer una precisión mayor, pero no funcionan dentro de algunos edificios o medios de transporte y pueden sufrir de interferencias en los edificios altos, lo que significa que una gran porción de la ciudad quedaría sin cobertura.[30] Nuevamente, conocer la ubicación geográfica de las personas no proporciona información completa y sacrifica la privacidad de las personas, por lo que los gobiernos no deben confiar ciegamente en el rastreo por geolocalización. Tal vez un sondeo de las conexiones de Bluetooth de distancia corta podría determinar cuántas personas estuvieron en contacto estrecho, pero esta técnica implicaría problemas de privacidad, y su uso solo debería explorarse si se contara con medidas de transparencia y seguridad para el acceso, la retención y el uso de los datos.

[30] Lawfare. *Location Surveillance to Counter COVID-19: Efficacy Is What Matters*, 2020. https://www.lawfareblog.com/location-surveillance-counter-covid-19-efficacy-what-matters

Proteger el imperio de la ley: Los acuerdos de intercambio de datos entre los estados y las empresas deben basarse en la ley	Cuando los gobiernos y las autoridades públicas determinen que es necesario establecer acuerdos de intercambio de datos para abordar la lucha contra el virus, dichos acuerdos deben basarse en las leyes existentes o de emergencia. Debido a los riesgos inherentes que estas medidas suponen para la privacidad y la protección de datos, las autoridades independientes y públicas deben poder examinarlas de forma exhaustiva, y los períodos de vigencia deben ser limitados. Por lo tanto, los gobiernos deben asegurar que estos acuerdos sean transparentes y respeten las normas legales. Los acuerdos *ad-hoc*, extralegales y poco transparentes con las empresas y operadoras de telecomunicaciones no son aceptables.
Utilizar datos anonimizados y aplicar principios de privacidad y protección de datos	A los gobiernos que decidan utilizar datos de ubicación según las leyes existentes o de emergencia, les recomendamos que empleen datos anonimizados. Un punto importante es que incluso los datos considerados como anónimos se pueden reidentificar, y solo cuatro puntos de observación pueden ser suficientes, de modo que los riesgos para la privacidad y la protección de datos permanecen vigentes.[31] Por lo tanto, se deben aplicar en todo momento los principios de privacidad y protección de datos; esto incluye la minimización de datos, para garantizar que la información utilizada sea relevante, precisa y necesaria para abordar la crisis actual, y las limitaciones de uso, que garantizan que los datos se usen únicamente para responder ante la crisis. Además, las empresas y operadoras de telecomunicaciones que proporcionen datos deben trabajar con autoridades de supervisión y expertos en privacidad para garantizar que se implementen las medidas de seguridad adecuadas. Por último, instamos a los gobiernos a limitar el acceso a estos datos únicamente a quienes los necesitan para luchar contra el virus. Esta información se debe etiquetar o almacenar en una base de datos independiente dedicada a la respuesta a crisis de modo que se pueda eliminar fácilmente una vez que termine la pandemia.

[31] Wired. *Anonymized Phone Location Data Not So Anonymous, Researchers Find*, 2013. https://www.wired.com/2013/03/anonymous-phone-location-data/

Aprender de los errores pasados: No emplear medidas de vigilancia masiva	Una pandemia no debe servir como excusa para adoptar nuevos poderes generales de vigilancia masiva. De las respuestas a crisis de salud anteriores, aprendimos que emplear medidas invasivas de vigilancia es desacertado y potencialmente perjudicial, tanto para los derechos humanos como para la salud pública. De hecho, con las medidas de procesamiento masivo de datos (*big data*) que se implementaron durante el brote de ébola, se violó el derecho a la privacidad de millones de personas, y la contribución en la lucha contra la enfermedad fue ínfima.[32] En cuanto al rastreo, los gobiernos no deben requerir a los ciudadanos que utilicen aplicaciones o servicios de geolocalización, ya que esto resultaría en nuevas formas de vigilancia.
No establecer disposiciones de retención de datos desproporcionadas	La crisis de salud actual no se debe aprovechar como una oportunidad para implementar medidas desproporcionadas de retención de datos. La información necesaria para combatir el virus debe encontrarse actualizada y, por lo tanto, no necesita conservarse durante muchos años. En términos generales, estos datos deben eliminarse tan pronto como termine la crisis.

V. ASOCIACIONES ENTRE ENTIDADES PÚBLICAS Y PRIVADAS: APLICACIONES, SITIOS WEB Y SERVICIOS UTILIZADOS EN LA LUCHA CONTRA EL COVID-19

Desde el comienzo de la crisis, los gobiernos y las empresas de tecnología han trabajado en conjunto para desarrollar soluciones tecnológicas que ayuden a combatir el brote de COVID-19. Esta amplia variedad de soluciones que el sector privado ofrece a las autoridades públicas comprende desde la recopilación de información y el rastreo de los movimientos de los ciudadanos infectados hasta la difusión de alertas de salud pública y el monitoreo de la ubicación geográfica del público general. En cualquier crisis de salud pública, es necesaria la solidaridad entre los distintos sectores de la sociedad.

La crisis actual, en particular, pone de relieve en qué medida el público y las autoridades públicas necesitan de las empresas de tecnología para funcionar: desde el acceso a la banda ancha para que las personas puedan trabajar desde su casa, hasta las soluciones de videoconferencia y las herramientas que responden directamente a la crisis, como las

[32] The Centre for Internet & Society. *Ebola: A Big Data Disaster*, 2016. https://cis-india.org/papers/ebola-a-big-data-disaster

aplicaciones de diagnóstico. Pero, si no se aplican las medidas de seguridad adecuadas y consideraciones significativas respecto de los derechos humanos, las soluciones tecnológicas implican numerosos riesgos. Al utilizar el respaldo de las empresas privadas, los gobiernos pueden reforzar los poderes de las plataformas dominantes, exacerbar los riesgos asociados con la recopilación de datos y la monetización de la información de salud y legitimar los servicios que invaden la privacidad. Más aún, una gran cantidad de empresas conocidas por posibilitar violaciones de derechos humanos están ofreciendo públicamente productos diseñados para responder al brote de COVID-19 que podrían utilizarse como herramientas de vigilancia masiva una vez finalizada la crisis.[33]

> *"Al utilizar el respaldo de las empresas privadas, los gobiernos pueden reforzar los poderes de las plataformas dominantes, exacerbar los riesgos asociados con la recopilación de datos y la monetización de la información sanitaria y legitimar los servicios que invaden la privacidad".*

CASOS PRÁCTICOS

Se han creado numerosas aplicaciones, sitios web y otros servicios en línea para ayudar a las personas a hacer un seguimiento del avance del COVID-19 y combatirlo, así como adaptarse y organizarse durante el brote. El sector de la tecnología desempeña un rol fundamental en la respuesta ante la crisis. No obstante, el historial mediocre de respeto por los derechos humanos que caracteriza a la mayoría de las empresas de tecnología, en especial en el área de la protección de datos y la privacidad, presenta un gran desafío en la búsqueda de soluciones sustentables para combatir el virus.

A continuación, presentamos algunos casos regionales que ilustran las propuestas de ciertas empresas tecnológicas para combatir el COVID-19. Para cada ejemplo, brindamos recomendaciones a los gobiernos sobre cómo usar los datos de forma responsable y acorde con las leyes de derechos humanos.

---

[33] Ver por ejemplo: Ranking Digital Rights. *Corporate Accountability Index*, 2019. https://rankingdigitalrights.org/index2019/
The Wall Street Journal. *To Track Virus, Governments Weigh Surveillance Tools That Push Privacy Limits,* 2020. https://www.wsj.com/articles/to-track-virus-governments-weigh-surveillance-tools-that-push-privacy-limits-11584479841
Bloomberg. *Israeli Spyware Firm Wants to Track Data to Stop Coronavirus Spreading,* 2020. https://www.bloomberg.com/news/articles/2020-03-17/surveillance-company-nso-supplying-data-analysis-to-stop-virus

África	En **Kenia**, se lanzó la aplicación *mSafari* para ayudar a hacer un seguimiento de los contactos personales.[34] En teoría, esta aplicación, cuyo desarrollo se encuentra actualmente en manos del sector privado, se utilizará para hacer un seguimiento de los pasajeros de vehículos de transporte público, como autobuses y taxis, entre otros. Los conductores deberán descargarla y llevar un registro de todos los pasajeros. En el momento de la publicación, el sitio web de *mSafari* no contaba con términos ni políticas disponibles públicamente que explicaran qué información se utilizaría, con quién se compartiría o cómo se procesaría.[35]
América Latina	En **Argentina**, el presidente y los representantes del gobierno llevaron a cabo una videollamada con las empresas de tecnología, en la que les pidieron desarrollar una aplicación que ayudara a impedir que las personas salgan de sus casas.[36] En **Colombia**, se reformuló el propósito de una aplicación existente, que se denominó CoronApp, para brindar información sobre el virus.[37] La aplicación requiere una gran cantidad de información personal (como el origen étnico) para funcionar. Además, no ofrece transparencia respecto de quién tendrá acceso a esos datos y cómo se podrían llegar a utilizar. En **Guatemala**, el gobierno lanzó una aplicación oficial llamada Alerta Guate diseñada para informar a las personas sobre el COVID-19. Al descargarla, los usuarios deben autorizar el acceso a sus datos de ubicación y al micrófono de su teléfono y proporcionar una dirección de correo electrónico o un número de teléfono.[38]

[34] The Standard. *Government to Launch Contract Tracking Application,* 2020. https://www.standardmedia.co.ke/health/article/2001365263/app-uses-passenger-data-to-trace-virus-path
[35] *mSafari,* 2020. http://msafari.co.ke/
[36] Gobierno Nacional de Argentina. *Soluciones conjuntas entre el Gobierno y empresas tech para enfrentar el Coronavirus*, 2020. https://www.argentina.gob.ar/noticias/soluciones-conjuntas-entre-el-gobierno-y-empresas-tech-para-enfrentar-el-coronavirus
[37] Fundación Karisma. *CoronApp, una barrera para el acceso a información pública y una pesadilla para la privacidad*, 2020. https://stats.karisma.org.co/coronapp-inscolombia/
[38] La Hora. *Sandoval sobre Alerta Guate: "Quien la quiera descargar lo puede hacer"*, 2020. https://lahora.gt/sandoval-sobre-alerta-guate-quien-la-quiera-descargar-lo-puede-hacer/

Oriente Medio y Norte de África	En **Túnez**, Enova Robotics firmó un acuerdo con el Ministerio del Interior para comenzar a utilizar robots PGuard.[39] Estos dispositivos estarán equipados con una serie de cámaras infrarrojas que ayudarán a impedir que las personas salgan de sus casas. No hay información respecto de dónde se ubicarán estos robots, qué datos recopilarán, durante cuánto tiempo retendrán la información ni quién tendrá acceso a ella. La infame compañía NSO Group aprovecha la crisis mundial ofreciendo sus servicios de rastreo a gobiernos de todo el mundo.[40] El software de hackeo de la empresa se ha visto implicado en numerosas violaciones de derechos humanos, incluido asesinato de Jamal Khashoggi, tal vez uno de los casos más destacados.[41] La aplicación que en este momento desarrolla NSO Group, supuestamente probada en alrededor de una docena de países, toma la información de rastreo de las últimas dos semanas del teléfono móvil de una persona infectada y la vincula con los datos de ubicación recopilados por las empresas nacionales de telefonía móvil.[42] Así, la aplicación busca identificar a las personas que estuvieron cerca de pacientes por más de 15 minutos y, por lo tanto, podrían correr riesgo de contagio.

[39] African Manager. *A first in Tunisia: Pguard, the security robot to report violations*, 2020. https://africanmanager.com/une-premiere-en-tunisie-pguard-le-robot-de-securite-pour-signaler-les-infractions/

[40] Bloomberg. *Israeli Spyware Firm Wants to Track Data to Stop Coronavirus Spreading*, 2020. https://www.bloomberg.com/news/articles/2020-03-17/surveillance-company-nso-supplying-data-analysis-to-stop-virus

[41] The New York Times. *Israeli Software Helped Saudis Spy on Khashoggi, Lawsuit Says*, 2020. https://www.nytimes.com/2018/12/02/world/middleeast/saudi-khashoggi-spyware-israel.html

[42] Independent. *Coronavirus: Controversial Israeli spyware firm NSO builds software tracking mobile data to map Covid-19*, 2020. https://www.independent.co.uk/news/world/middle-east/coronavirus-israel-cases-tracking-mobile-phone-nso-spyware-covid-19-a9410011.html

Asia Pacífico	En **China**, aplicaciones como Alipay y WeChat marcaron a los individuos de riesgo alto, a quienes luego se les ordenó permanecer en cuarentena o se les prohibió ingresar a espacios públicos. Cuando la región vuelva a la normalidad, estas personas deberán obtener un "permiso" de estas aplicaciones para volver a recorrer espacios públicos y moverse libremente.[43] También en **China**, empresas como SenseTime afirman que su software de detección de temperatura corporal sin contacto ya se implementó en Pekín, Shangái y Shenzhen. La compañía también indica que cuenta con una herramienta de reconocimiento facial. Si bien las cámaras de reconocimiento facial son frecuentes en China, ahora se les están implementando actualizaciones para mejorar la precisión y la medición de la temperatura corporal.[44] **Singapur** cuenta con una aplicación llamada Tracetogether. Permite que los usuarios compartan su información de forma voluntaria y hace un seguimiento de las demás personas con quienes entraron en contacto mediante Bluetooth. Si un usuario de la aplicación contrae COVID-19, se envía una notificación a todos los demás usuarios que estuvieron en contacto con esta persona y al gobierno. No hay transparencia respecto de quién podrá tener acceso a esta información.
Europa	En **España**, los gobiernos de Catalunia y Madrid crearon aplicaciones que permiten informar a la población acerca de los síntomas del COVID-19.[45] Estas aplicaciones recopilan datos de salud y de ubicación en tiempo real a partir de sus usuarios para crear mapas de calor. En **Eslovaquia**, se lanzó una aplicación llamada Zostan Zdravy ("Cuida tu salud"). Tiene el propósito de informar a los usuarios si hay una persona infectada con

[43] The New York Times. *In Coronavirus Fight, China Gives Citizens a Color Code, With Red Flags,* 2020. https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html
[44] BBC. *Coronavirus: China's tech fights back*, 2020. https://www.bbc.com/news/technology-51717164
[45] Carto. *CARTO collaborates on 'AsistenciaCovid19' App against Coronavirus*, 2020. https://carto.com/blog/carto-develops-app-against-coronavirus/
CatalanNews. *How the health department's new app to monitor coronavirus symptoms works,* 2020. https://www.catalannews.com/society-science/item/how-the-health-department-s-new-app-to-monitor-coronavirus-symptoms-works

COVID-19 cerca.[46] Hasta el momento, la aplicación cuenta con más de 10.000 descargas y funciona de la siguiente manera:

1. El usuario descarga la aplicación de forma "gratuita".
2. El usuario se registra con su número de teléfono o correo electrónico.
3. La aplicación crea una base de datos de las posibles exposiciones cercanas a personas infectadas con COVID-19. El usuario no recibe información sobre cómo se creó la base de datos.
4. Supuestamente, el usuario puede ver si estuvo cerca de personas con infecciones confirmadas de COVID-19, así como el momento y la distancia de dichos encuentros.
5. Los dispositivos anónimos que estuvieron a distancias estrechas de casos confirmados reciben un aviso sobre su potencial exposición al COVID-19, y se les pide que se realicen la prueba.
6. El usuario puede solicitar realizar la prueba del COVID-19 mediante la aplicación con un código de "identificación anónima".
7. El usuario acude al hospital para realizarse la prueba. Si el usuario obtiene un resultado positivo, los miembros del personal médico reciben un código de identificación del usuario, el cual ingresan al sistema de salud. El usuario recibe los resultados a través de la aplicación. Luego, el sistema envía un mensaje de advertencia a todos los demás usuarios de la aplicación que estuvieron cerca de la persona con un resultado positivo.

En **Polonia**, el gobierno lanzó una aplicación diseñada para supervisar a los pacientes en cuarentena. Requiere que los pacientes se tomen fotografías de sí mismos para demostrar que no están incumpliendo el confinamiento obligatorio. La alternativa es recibir visitas inesperadas de la policía. Tras su registro con una autofoto, los residentes de Polonia deben cumplir con solicitudes periódicas de autofotos geolocalizadas.[47] Salvo la foto de registro, los datos que se suben a la aplicación y se almacenan en ella se eliminan una vez que finaliza la cuarentena del individuo. La foto de registro se almacena durante 6 años.[48]

[46] TechBox. *Appka Zostaň zdravý upozorní na koronavírus v okolí*, 2020. https://techbox.dennikn.sk/aplikacia-zostan-zdravy-vas-upozorni-na-potvrdenie-koronavirusu-vo-vasom-okoli/

[47] Business Insider. *Poland made an app that forces coronavirus patients to take regular selfies to prove they're indoors or face a police visit*, 2020. https://www.businessinsider.com/poland-app-coronavirus-patients-mandaotory-selfie-2020-3?r=US&IR=T

[48] Niebezpiecznik. *Aplikacja "kwarantanna domowa" wzbudza obawy o inwigilację. Czy słusznie?*, 2020. https://niebezpiecznik.pl/post/aplikacja-kwarantanna-domowa-wzbudza-obawy-o-inwigilacje-czy-slusznie/

Norteamérica	En **Estados Unidos**, un grupo de programadores está desarrollando una aplicación que permitiría a las personas registrar sus movimientos para, luego, compararlos con los de los pacientes confirmados de COVID-19. Para ello, se planea utilizar datos proporcionados por los departamentos de salud pública nacional o estatal. Después de un tiempo, se les preguntará a los usuarios si se encuentran infectados. No es claro quién tendrá acceso a esta información.[49] También en **Estados Unidos**, la organización de investigación Verily, de Alphabet, lanzó un sitio web limitado de prueba y detección de COVID-19.[50] A fin de calificar para la prueba, los usuarios deben tener una cuenta de Google y aceptar la posibilidad de que su información se comparta con esta empresa.[51] El sitio web es una colaboración entre la compañía de biotecnología basada en el Área de la Bahía, la oficina de gobierno de California y otros funcionarios estatales y federales.

[49] Wired. *Phones Could Track the Spread of Covid-19. Is It a Good Idea?,* 2020. https://www.wired.com/story/phones-track-spread-covid19-good-idea/

[50] CNBC. *Alphabet's Verily launches a limited coronavirus screening website*, 2020. https://www.cnbc.com/2020/03/15/alphabets-verily-says-it-will-launch-a-limited-coronavirus-testing-website-monday.html

[51] Project Baseline by Verily. *California COVID-19 risk screening and testing*. https://www.projectbaseline.com/study/covid-19/

RECOMENDACIONES	
Ofrecer transparencia acerca de las asociaciones entre entidades públicas y privadas	Las colaboraciones entre gobiernos, autoridades y empresas, o cualquier otro tipo de organización, deben ser transparentes. Deben implementar estándares de datos abiertos, gobierno abierto y contratación abierta, proporcionar informes de transparencia y facilitar el acceso público a la información. A fin de incentivar la competencia, el software o los servicios no deben limitarse a contratos exclusivos o de largo plazo. Los gobiernos deben tener flexibilidad para elegir a los mejores socios en función del interés público.
Implementar evaluaciones del impacto en los derechos humanos y procesos de debida diligencia de carácter obligatorio en todas las asociaciones de entidades públicas y privadas y las contrataciones públicas	**Para los actores del sector privado:** Los actores del sector privado que diseñen, desarrollen o implementen sistemas para combatir el COVID-19 deben actuar dentro de un marco de debida diligencia estándar de la industria respecto de los derechos humanos a fin de identificar los riesgos más prominentes, evitar el fomento de la discriminación y respetar los derechos humanos de manera integral en sus sistemas. Según sea necesario, los actores del sector privado deberán crear procesos para supervisar, mitigar e informar los peligros potenciales y notificar a los individuos afectados. **Para el sector público:** Las evaluaciones del impacto en los derechos humanos deben seguir estos lineamientos: ➔ Llevarse a cabo de forma periódica, antes de las contrataciones públicas y durante su desarrollo, en momentos clave habituales y a lo largo de su uso específico en el contexto[52] ➔ Incluir una evaluación de las posibles transformaciones que pueden generar en las estructuras social, institucional o gubernamental existentes ➔ Estar disponibles para el público con facilidad de acceso y un formato legible por máquina Cuando no sea posible mitigar significativamente los riesgos identificados, el sistema en cuestión no deberá implementarse ni utilizarse por ninguna autoridad pública. Las evaluaciones deben expeditarse para responder a la crisis.

[52] Danish Institute for Human Rights. *Driving change through public procurement*, 2020. https://www.humanrights.dk/publications/driving-change-through-public-procurement

Considerar el historial del impacto en los derechos humanos de las distintas empresas y excluir a aquellas que muestren violaciones sistemáticas	Los gobiernos deben considerar los riesgos adicionales que implica delegar servicios estatales de la lucha contra el COVID-19 al sector privado antes de concretar asociaciones de carácter público-privado. A su vez, los gobiernos deben garantizar que las soluciones de las entidades privadas hayan sido probadas y deben demostrar sus beneficios antes de colaborar. Por último, los gobiernos deben asegurarse de que sus asociados utilicen las salvaguardas necesarias para proteger los derechos humanos. Las empresas con historiales de incumplimientos de derechos humanos o que hayan facilitado dichas prácticas deben excluirse de las licitaciones públicas de soluciones y aplicaciones técnicas para abordar la lucha contra la pandemia.[53]
Aplicar los principios de privacidad y protección de datos	Las empresas que desarrollen servicios y aplicaciones diseñadas para abordar el brote de COVID-19 deben asegurar el cumplimiento de los derechos de protección de datos de los usuarios, así como respetar los principios de minimización de datos y de limitación de uso, finalidad, acceso y retención de la información.[54]

[53] Las empresas que hayan desarrollado su modelo de negocio en torno al debilitamiento de la seguridad y la integridad de nuestra infraestructura digital no se deben considerar como confiables para crear una aplicación segura al servicio de la salud pública. Ver Ranking Digital Rights. Ver: *Corporate Accountability Index*, 2019. https://rankingdigitalrights.org/index2019/
The Wall Street Journal. *To Track Virus, Governments Weigh Surveillance Tools That Push Privacy Limits,* 2020. https://www.wsj.com/articles/to-track-virus-governments-weigh-surveillance-tools-that-push-privacy-limits-11584479841
Bloomberg. *Israeli Spyware Firm Wants to Track Data to Stop Coronavirus Spreading,* 2020. https://www.bloomberg.com/news/articles/2020-03-17/surveillance-company-nso-supplying-data-analysis-to-stop-virus

[54] Ver nuestra recomendación "Aplicar los principios y derechos a la privacidad y la protección de datos" en la sección III de este artículo. Para obtener más información, consulte también: 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

Prohibir a las empresas privadas que reutilicen o moneticen los datos	Al crear aplicaciones para responder a una crisis de salud pública, no se debe permitir que las empresas privadas moneticen los datos obtenidos mediante el uso de sus productos. Además, se deben aplicar limitaciones claras respecto de los usos secundarios o los procesamientos futuros de los datos.
Permitir la revisión abierta y transparente de los productos	Cualquier aplicación o solución tecnológica del sector privado diseñada para ayudar en la lucha contra el COVID-19 debe poder someterse completamente a escrutinios y a auditorías por parte de las autoridades de regulación independientes y los grupos de la sociedad civil.
Evitar el "tecnosolucionismo"	Debemos vigilar de cerca las soluciones tecnológicas propuestas en situaciones de alto riesgo, como una crisis de salud, particularmente, los proyectos de inteligencia artificial y reconocimiento facial. Se deben priorizar las medidas ya comprobadas por sobre las soluciones tecnológicas rápidas, en especial, cuando estas últimas impliquen la transgresión de protecciones legales y la recolección de datos personales.
No invertir en sistemas de vigilancia controversiales	Si bien los recursos para la salud pública son escasos, los gobiernos de todo el mundo no deben ver esta crisis sanitaria como una oportunidad para invertir en sistemas de vigilancia controversiales, como las tecnologías de reconocimiento facial.

VI. CONCLUSIÓN

El mundo se encuentra frente a una crisis de salud pública, y las respuestas y medidas que adopten los gobiernos para combatir el COVID-19 tendrán un impacto más allá de esta emergencia. A partir de las crisis de salud anteriores, aprendimos que no debemos caer en las soluciones rápidas, sino mantener en alto la bandera de los derechos humanos para evitar mayores daños a la población. Los datos y la tecnología serán factores clave en la lucha contra el COVID-19. El dilema no es *si* los gobiernos pueden usar datos y tecnología para ganar la lucha contra el virus, sino *cómo* deben hacerlo, y nuestro mensaje es simple: **defender los derechos digitales también ayuda a proteger la salud pública**.

En un momento de crisis, la confianza pública es clave para garantizar la unidad detrás de las respuestas. Socavar los derechos humanos sería desacertado y perjudicial, tanto durante la crisis como después de esta. En esta lucha colaborativa contra el COVID-19, todos somos responsables de tomar medidas y brindar asesoramiento y protección: los gobiernos, las empresas, las ONG y los individuos. Esperamos que estas recomendaciones ayuden a los gobiernos a encontrar respuestas comunes a la crisis, y estamos a su disposición para brindarles asistencia en cuanto a su implementación.

> *"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 Harari [55]

Para obtener más información, comuníquese con:
Estelle Massé
Analista de Políticas Públicas y Líder Global de Protección de Datos, Access Now.
estelle@accessnow.org

[55] Financial Times. *The world after coronavirus*, 2020. https://www.ft.com/content/19d90308-6858-11ea-a3c9-1fe6fedcca75