PREOCUPACIONES DE DERECHOS HUMANOS SOBRE LA APP CUIDAR

Amnistía Internacional realizó un análisis de la app "Cuidar" creada por el gobierno argentino a través de la Decisión Administrativa 432/2020 de Jefatura de Gabinete de Ministros de la Nación para la autoevaluación de la salud, así como para obtención del Certificado Único Habilitante de Circulación (CUHC) que permite a los usuarios y usuarias circular siempre y cuando no hayan indicado un autodiagnóstico sospechoso de coronavirus.

Amnistía Internacional examinó la aplicación argentina a la luz del marco regulatorio aplicable, sus Términos y Condiciones (TyC), y comunicaciones oficiales del Estado, para corroborar si la misma cumple con los estándares de derechos humanos y las recomendaciones de Amnistía Internacional para este tipo de tecnología. Este análisis se complementó con información oficial brindada por la Subsecretaría de Gobierno Abierto y País Digital de la Secretaría de Innovación Pública de la Jefatura de Gabinete de Ministros de la Nación, responsable del desarrollo de Cuidar, mediante un pedido de acceso a la información pública realizado por nuestra organización. También compartimos nuestro análisis preliminar y recomendaciones con esta Secretaría, quien nos brindó aclaraciones adicionales por escrito y luego en una reunión de intercambio el pasado 10 de septiembre, las cuales incorporamos a este análisis.

El proyecto Security Lab de Amnistía Internacional basado en Alemania ya había analizado apps destinadas al control del COVID-19 en 11 países. La tecnología puede y debe jugar un papel importante en la búsqueda de respuestas a la pandemia causada por el COVID-19. La salud pública es un fin legítimo que justifica restricciones y limitaciones en la mayoría de los tratados de derechos humanos. Sin embargo, las medidas que se tomen en este contexto serán legales solamente si pueden cumplir con criterios estrictos.

CUALQUIER MEDIDA RESTRICTIVA DE DERECHOS DEBE ESTAR PRESCRIPTA POR LEY, SER JUSTIFICADAMENTE NECESARIA, PROPORCIONADA, DE DURACIÓN DEFINIDA, IMPLEMENTADA CON TRANSPARENCIA Y CONTAR CON SUPERVISIÓN ADECUADA. LAS INICIATIVAS QUE LOS ESTADOS IMPLEMENTEN PARA CONTENER EL VIRUS NO DEBEN SERVIR PARA REALIZAR UNA VIGILANCIA DIGITAL INVASIVA SOBRE LAS PERSONAS.

Luego de analizar la regulación y el funcionamiento de la app Cuidar, a Amnistía Internacional le preocupan los riesgos que su implementación representa para los derechos humanos, especialmente para la privacidad y la protección de datos personales. El acceso a datos personales y sensibles como los datos de salud, sumados a la falta de transparencia sobre cómo estos datos son almacenados y utilizados por parte del gobierno, son algunos de los motivos de preocupación que representa la app.

A CONTINUACIÓN, DETALLAMOS ALGUNOS DE ESTOS FACTORES DE PREOCUPACIÓN:

OBTENCIÓN DE DATOS SENSIBLES SIN PRESERVACIÓN DE LA IDENTIDAD

Los datos de salud de las personas son datos privados y sensibles que reciben protección especial. La Ley Nº 25.326 de Protección de Datos Personales es clara al exigir mecanismos de disociación adecuados y preservación de la identidad cuando se trata de estos tipos de datos. Sin embargo, en el caso de Cuidar, la identificación es un requisito necesario para poder utilizar la app.

El gobierno debería ser capaz de demostrar técnicamente y de forma transparente que es imposible desanonimizar los datos sensibles recogidos, incluso combinándolos con otros conjuntos de datos. Sin embargo, en el caso de Cuidar no solo no es este el caso, sino que además el Estado exige a los usuarios y usuarias realizarse un autodiagnóstico de síntomas antes de tramitar el permiso de circulación en la app. Esta exigencia resulta prescindible ya que cualquier persona puede tramitar el permiso de circulación a través de la página web del gobierno sin que se le solicite información sobre su salud.

A su vez, la app Cuidar utiliza un sistema de tipo centralizado. Esto quiere decir que cuando los usuarios registran sus datos, esos datos, que

no están anonimizados, se envían a servidores centrales de una empresa privada contratada por el Estado y son administrados por las autoridades gubernamentales, quienes podrán disponer de ellos para analizarlos. En cambio, los sistemas descentralizados permiten que los datos se almacenen en los dispositivos móviles de los usuarios y usuarias y que el análisis se realice en el propio dispositivo. Por esta razón, existe consenso en que los sistemas descentralizados son menos invasivos de la privacidad al preservar el anonimato y proteger la identidad, permitiendo que los usuarios y usuarias tengan el control sobre sus datos.

Por último, es importante recordar que la información relativa a la salud es un dato sensible y su recolección y tratamiento, no solo debe ser objeto del consentimiento libre, expreso e informado de su titular, sino que además debe estar autorizado por ley, de conformidad con los arts. 2, 5 y 7 de la Ley N.º 25.326 de Protección de Datos Personales. En este sentido, el punto 5.3 de los TyC establece que el usuario presta su consentimiento expreso para que la Secretaría de Innovación Pública (SIP) trate sus datos personales, incluyendo sus datos sensibles de salud. Sin embargo, no existe hoy una ley que autorice la recolección y tratamiento de estos datos por parte del Estado.

Es importante recordar también que el Estado está autorizado a tratar datos sensibles de salud con finalidades estadísticas o científicas, pero en este caso, tienen que garantizar que no puedan ser identificados sus titulares (Ley N.º 25.326, art. 7, inc. 2).

- ## RECOMENDACIONES:

› Eliminar el requisito de identificación para la utilización de la app para fines de autodiagnóstico.

› Garantizar la anonimidad de los datos sensibles recogidos, incluyendo la imposibilidad de desanonimizarlos combinándolos con otros conjuntos de datos.

› No recolectar ni tratar datos sensibles, como la información relativa a la salud, sin la debida autorización legal.

TRANSPARENCIA

Como mencionamos anteriormente en nuestras recomendaciones, los gobiernos deben ser transparentes con respecto a las medidas que tomen para que estas puedan ser analizadas y modificadas, retiradas o anuladas posteriormente, si procede.

En este sentido, nos preocupa la falta de claridad en la comunicación de algunos aspectos de la app como, por ejemplo, de las actualizaciones de sus funcionalidades. El punto 8 de los TyC de Cuidar faculta a la SIP a introducir todos los cambios y modificaciones que estime convenientes, lo que

incluye, pero no se limita, a agregar, alterar, sustituir o suprimir cualquier contenido de la app en todo momento. Frente a ello, es importante que los usuarios y usuarias sean notificados fehacientemente de las funcionalidades que se modifiquen, eliminen o agreguen, de forma tal que no se vulnere el consentimiento informado que brindaron inicialmente al descargar la app.

A su vez, al momento de realizar el pedido de acceso a la información, habían pasado más de cuatro meses desde el lanzamiento de la app Cuidar y el código fuente de la app no se había hecho público. Al consultar por este aspecto en nuestro pedido de acceso a la información, el Estado respondió que estaba trabajando para publicar el código de manera segura próximamente. Finalmente, el 31 de julio se publicó el código fuente de la app Cuidar, pero no se hizo público el código del "backend" que es el que permite conocer cómo guarda los datos la app y qué hace con ellos. Ofrecer garantías que permitan verificar el nivel de protección y seguridad con que se almacenan y tratan los datos recolectados resulta indispensable para permitir el control externo y la posibilidad de que sea auditada por expertos independientes.

En lo que respecta a la eliminación de datos personales, a través del punto 5.9 de los TyC se indica que los datos sensibles y los relacionados a la geolocalización se preservarán únicamente mientras sean necesarios y dure la emergencia sanitaria. Así lo ha reafirmado el Estado al responder sobre este punto en el pedido de acceso a la información. Con relación a la forma de eliminación de estos datos, la SIP informó en sus comentarios a este análisis que la misma será *"debidamente comunicada y monitoreada"* y que *"el proceso será supervisado por la Agencia Nacional de Acceso a la Información Pública"*. Asimismo, nos aclararon que desde la Secretaría *"garantizan la destrucción de la información y asumen que responderán ante cualquier reclamo de los usuarios, así como a todo pedido de informes o auditoría que resulten necesarios"*.

Los Estados deben ser transparentes sobre la naturaleza y el alcance de las medidas implementadas. Por ello, deben brindar información que permita el control externo independiente sobre la forma en que se almacenan y tratan los datos compartidos por el usuario o usuaria y se debe especificar la forma en que serán eliminados una vez que termine la emergencia sanitaria, incorporando así salvaguardas contra el uso indebido.

• RECOMENDACIÓN:

› Asegurar transparencia sobre la naturaleza y el alcance de la medida implementada en todo momento.

› Notificar fehacientemente a los usuarios y usuarias de las funcionalidades de la app que se modifiquen, eliminen o agreguen para evitar vulnerar el consentimiento informado brindado al descargar la app.

› Ofrecer garantías que permitan el control externo e independiente sobre la forma en que se almacenan y tratan los datos que recolecta la app.

IGUALDAD Y NO DISCRIMINACIÓN

La exigencia de que las personas cuenten con determinada tecnología y conectividad para el acceso a derechos representa una preocupación adicional con relación al derecho a la igualdad y la no discriminación, ya que son muchas las personas que no cuentan con un dispositivo móvil con la tecnología y la conectividad necesaria para descargar y usar la app, lo que las excluiría de la posibilidad de acceder a los mismos derechos.

Al consultar sobre este punto, el Estado ha informado que cuentan con la versión web para tramitar el CUCH y que las personas pueden descargar el permiso en sus dispositivos o bien imprimirlo. Además, la SIP nos informó en sus comentarios sobre este análisis que *"se acordó con las empresas operadores nacionales de telefonía móvil la bonificación en el servicio de datos para el uso de la aplicación Cuidar"*, lo cual consideramos una medida positiva que contribuye a reducir la brecha en el acceso a la app. Sin embargo, la respuesta no hace referencia a las personas que por falta de tecnología o conectividad no podrían acceder al trámite por la página web o a las herramientas que proporciona la app en términos de asistencia y recomendaciones de salud.

Lo mismo sucede con las personas que no cuentan con un DNI, por ejemplo. Al consultar sobre el requisito de identificación exclusiva con DNI, el Estado ha informado que la app está en constante evolución y que no se descarta la posibilidad de incorporar otras formas de validación de identidad distintas al DNI. A los fines de tramitar el CUHC, quienes cuenten con residencia precaria pueden tramitar el mismo desde la página web oficial indicada para ello, pero, nuevamente, no podrían acceder a los mismos derechos en términos de salud.

Es importante que cualquier tecnología desarrollada para el control de la emergencia sanitaria cuente con requisitos de accesibilidad. Por ello, nos preocupa que la accesibilidad de una herramienta pensada para recomendar medidas de prevención y facilitar el acceso a la salud de los usuarios conectándolos con la atención sanitaria más cercana, deje afuera a los grupos más vulnerables como las personas mayores, las poblaciones marginadas que no cuentan con la tecnología o la conectividad necesaria, o las personas que no cuentan con un DNI, siendo estos grupos los de mayor riesgo y los que más necesitan protección en términos de acceso a la salud.

Además, el mal uso de datos y las violaciones a la privacidad impactan de manera diferente en las personas. Los Estados deben garantizar que los datos que recolecten no se utilicen de manera que impacten desproporcionadamente en las personas debido a su edad, posición social, económica, política, estatus migratorio, discapacidad o cualquier otro motivo.

Todo uso de tecnologías en la respuesta al COVID-19 debe tener en cuenta el riesgo de que tales herramientas refuercen la discriminación y otros abusos contra los derechos de las poblaciones más vulnerables.

No podemos dejar que la pandemia de COVID-19 aumente aún más las desigualdades existentes en el disfrute de los derechos humanos entre distintos grupos de la sociedad.

- ## RECOMENDACIONES:

› Garantizar que todas las personas puedan acceder a los mismos derechos y servicios, sin ningún tipo de discriminación.

CONSIDERACIONES FINALES

La tecnología resulta fundamental para controlar la pandemia del COVID-19 y buscar la mejor manera de enfrentar una crisis muy compleja.

Sin embargo, los Estados no pueden desatender derechos como la privacidad y la protección de datos personales con el pretexto de gestionar una crisis de salud pública. Ahora más que nunca, los gobiernos deben garantizar que sus iniciativas son respetuosas de los derechos humanos.

Como consecuencia, le pedimos a los Estados que en la medida que implementen tecnología para combatir esta crisis, incorporen las salvaguardas necesarias para demostrar que respetan plenamente los derechos humanos.

Los derechos humanos no son un obstáculo para el progreso, son esenciales y nos ayudarán a construir la confianza en la tecnología que se necesita para que sea efectiva y pueda desempeñar un papel significativo en esta crisis.

AMNISTÍA INTERNACIONAL