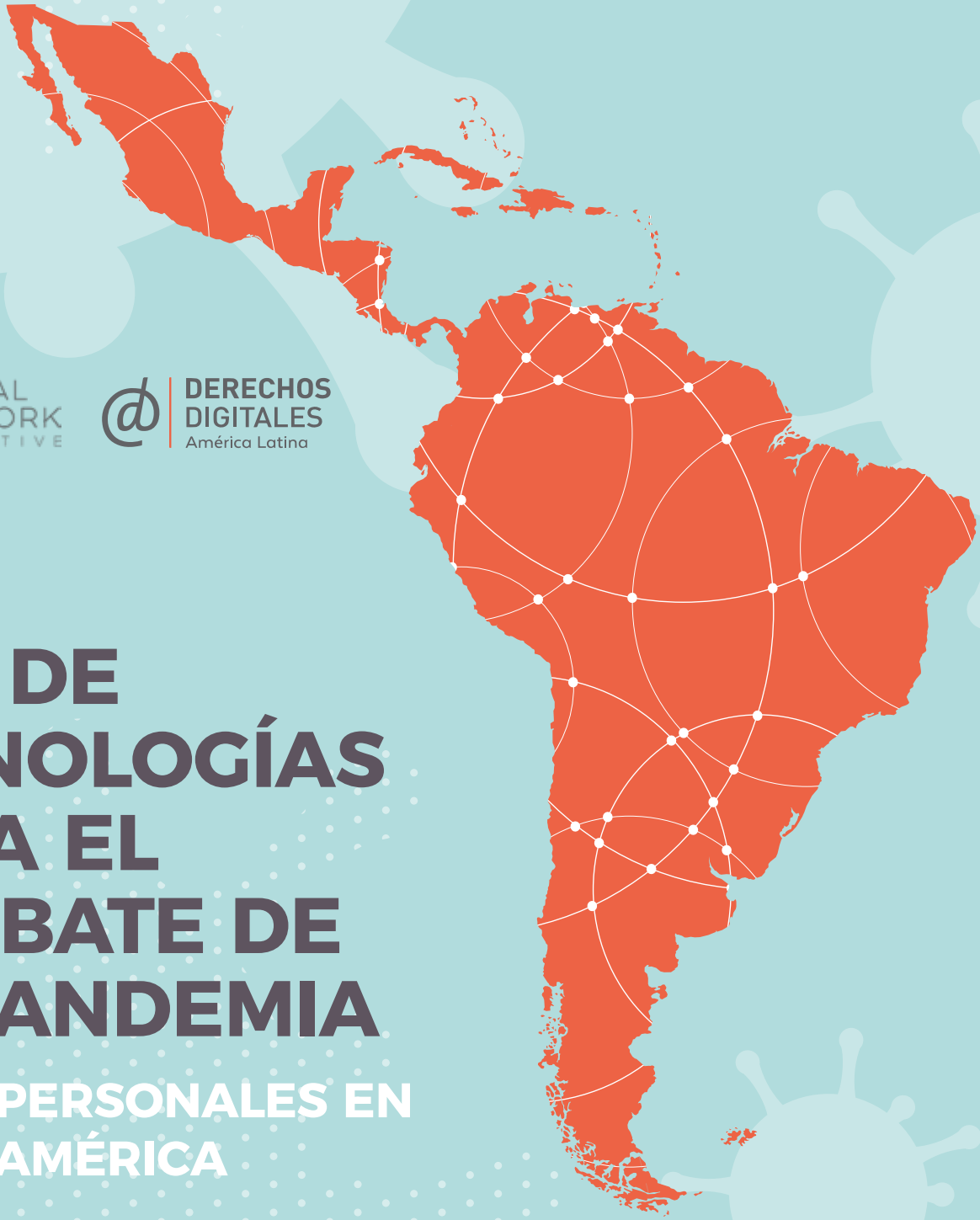


GLOBAL NETWORK INITIATIVE

DERECHOS DIGITALES América Latina

USO DE TECNOLOGÍAS PARA EL COMBATE DE LA PANDEMIA

DATOS PERSONALES EN LATINOAMÉRICA

LAURA NATHALIE HERNÁNDEZ RIVERA, DERECHOS DIGITALES
PARA LA GLOBAL NETWORK INITIATIVE | OCTOBER 2021

ESPAÑOL **ENGLISH**

ÍNDICE

RESUMEN

La emergencia sanitaria ocasionada por el virus SARS-CoV-2 obligó a los gobiernos de todo el mundo a buscar soluciones para contener la expansión del virus. Como parte de estas respuestas, la tecnología jugó un papel importante. Se desarrollaron aplicaciones y se utilizó el Big Data para monitorear las aglomeraciones y los movimientos de la población a través de datos de conexión de teléfonos celulares a torres de telefonía, datos de geolocalización y datos del *bluetooth* de los dispositivos celulares. Latinoamérica también se sumó a esta tendencia. Con el objetivo de conocer cómo fue implementado este abordaje en la región, particularmente con relación al uso y protección de los datos personales, se hizo una búsqueda de información relativa al desarrollo de herramientas tecnológicas para el combate de la pandemia, en seis países (Argentina, Bolivia, Brasil, Colombia, Ecuador y El Salvador). Para ello fueron usadas fuentes informativas oficiales, fuentes periodísticas, entrevistas con representantes de organizaciones de protección de derechos humanos en el ámbito digital, y artículos académicos que abordan estas temáticas. Los resultados muestran que, si bien ha existido un impulso significativo de despliegue de tecnologías y mecanismos de recolección y procesamiento de información, aún queda mucho trabajo por lograr que el diseño, desarrollo e implementación de tecnologías para la protección de la salud de la población sigan de manera expresa estándares de derechos humanos y sean compatibles con la protección de la privacidad y la autodeterminación informativa de las personas.

SOBRE LA AUTORA

Laura Nathalie Hernández Rivera es abogada salvadoreña especialista en Tecnologías. También es Analista de Políticas Públicas para la ONG Derechos Digitales Latinoamérica desde donde monitorea el desarrollo de eventos, iniciativas de políticas públicas y regulaciones relacionadas con los derechos humanos y la tecnología en Latinoamérica. Es doctoranda en Derecho por la Universidad Federal de Ceará, Brasil, y posee un LL. M. en Derecho de las Altas Tecnologías y Propiedad Intelectual por la Universidad de Santa Clara de Estados Unidos de América.

ATRIBUCIÓN

SECCIÓN AGRADECIMIENTOS

Por su aporte para comprender mejor el contexto de cada país estudiado y brindarme entrevistas para tal fin, brindo agradecimientos a:

- Nathalie Fragoso (InternetLab- Brasil)
- Daniel Ospina (Dejusticia- Colombia)
- Lucía Camacho (Fundación Karisma- Colombia)
- Enrique Chaparro (Fundación Vía Libre- Argentina)
- Eduardo Ferreyra (Asociación por los Derechos Civiles- Argentina)
- Carlos Palomo (Transparencia-Contraloria Social-Datos Abiertos- El Salvador)
- Wilson Sandoval (Centro de Asesoría Legal Anticorrupción de El Salvador- El Salvador)
- Paloma Villa Mateos (Telefónica, S.A.)

1. INTRODUCCIÓN

El 11 de marzo del año 2020, la Organización Mundial de la Salud (OMS) declaró la pandemia de la enfermedad COVID-19, originada por el coronavirus SARS-CoV-2.[1] A medida que la enfermedad se iba expandiendo por el continente americano[2] y los sistemas de salud comenzaban a experimentar saturación, los gobiernos fueron declarando estados de emergencia,[3][4][5][6][7][8] con lo cual se restringieron algunos derechos y se implementaron diversas medidas para intentar contener la expansión del virus: cierre de aeropuertos y fronteras terrestres, cierre de escuelas y lugares de ocio, hasta llegar a confinamientos de la población. En algunos países, las medidas fueron declaradas oportunamente, mientras que en otros, el tiempo para su implementación fue más tardío.

Dentro de las estrategias de los países para hacer frente a este nuevo virus y su consecuente enfermedad, la mayoría de países echó mano de los recursos tecnológicos, en su afán de minimizar el contagio y mantener vigilada a la población en los momentos de las restricciones de movilidad. En este escenario, fueron desarrolladas una gran cantidad de aplicaciones que ofrecían información oficial sobre el desarrollo de la enfermedad, test para realizar autodiagnóstico, rastreo de contagios, entre otros.[9]

Uno de los principales puntos de debate se centra en la tensión entre el derecho a la salud y el derecho a la privacidad que ocurre cuando los

1 https://www.paho.org/es/noticias/11-3-2020-oms-caracteriza-covid-19-como-pandemia
2 https://www.bbc.com/mundo/noticias-america-latina-51802906
3 https://es.euronews.com/2020/03/13/argentina-declara-emergencia-sanitaria-ante-nuevos-casos-de-coronavirus-en-el-pais
4 https://www.elperiodico.com/es/internacional/20200326/bolivia-emergencia-sanitaria-medidas-covid-19-7905461
5 https://www1.folha.uol.com.br/equilibrioesaude/2020/02/governo-decreta-estado-de-emergencia-por-causa-de-surto-do-coronavirus.shtml
6 https://www.minsalud.gov.co/Paginas/Presidente-Duque-declara-Emergencia-Sanitaria-frente-a-COVID-19.aspx
7 https://www.efe.com/efe/america/sociedad/el-presidente-de-ecuador-declara-la-emergencia-sanitaria-por-coronavirus/20000013-4193906
8 https://www.france24.com/es/20200314-el-salvador-declara-estado-de-emergencia-en-prevenci%C3%B3n-de-coronavirus
9 https://www.apc.org/sites/default/files/herejia-tecno-optimista.pdf

gobiernos usan tecnologías para capturar una gran cantidad de datos personales y sensibles, que sirvan para elaborar estrategias de contención de la enfermedad; cuando solicitan a las empresas privadas la entrega de los datos que recolectan y cuando esas tecnologías se emplazan sin un ejercicio de prudencia sobre los impactos que pueden causar en los derechos humanos de la población. En este contexto, este estudio analiza la forma en que los gobiernos de seis países de Latinoamérica –Argentina, Bolivia, Brasil, Colombia, Ecuador y El Salvador– utilizaron las tecnologías como parte de su estrategia para frenar la expansión del virus, con el fin de conocer de qué manera fueron aplicadas y analizar los puntos en los cuales se presentaron riesgos a la privacidad de las personas. También hace un primer acercamiento a los casos en los cuales fueron solicitados, por parte de los gobiernos, los datos recopilados por las empresas de telefonía móvil, para entender cómo fue realizada esta colaboración, desde el punto de vista de los derechos humanos.

La mayoría de países echó mano de los recursos tecnológicos, en su afán de minimizar el contagio y mantener vigilada a la población en los momentos de las restricciones de movilidad.

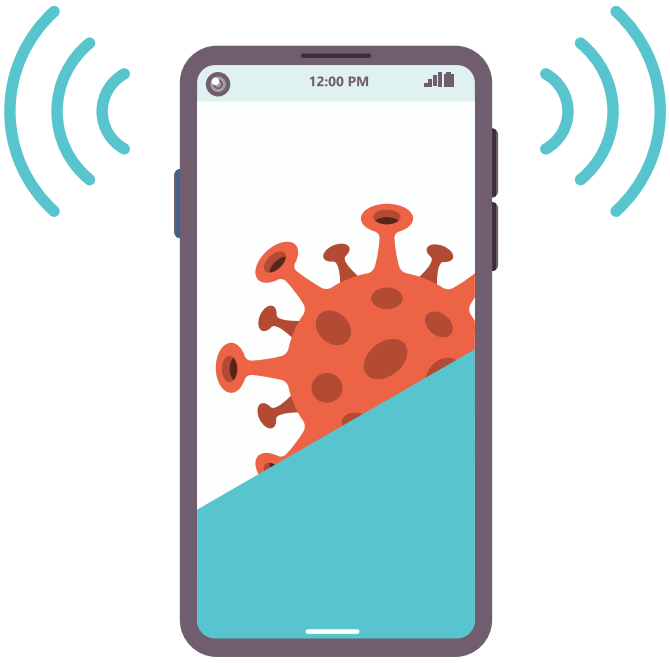
El estudio se divide en cuatro secciones. En la primera sección se presenta un resumen de las principales herramientas tecnológicas implementadas por los gobiernos de los países estudiados, para conocer sus características y algunos inconvenientes suscitados. En la segunda sección se expone el contexto jurídico de los países estudiados, para saber el grado de protección que los datos personales gozan en los ordenamientos jurídicos nacionales. La tercera sección presenta los países en los cuales los gobiernos solicitaron a las compañías de telefonía móvil las bases de datos de sus usuarios, para conocer si existieron límites jurídicos a este intercambio de información. Finalmente, en la cuarta sección se exponen las conclusiones del estudio y se presentan algunas recomendaciones para que la implementación de estas soluciones se base en las mejores prácticas y en concordancia con el respeto a los derechos humanos.

2.1. SITUACIÓN DE LA IMPLEMENTACIÓN DE TECNOLOGÍAS COMO PARTE DE LA RESPUESTA ANTE LA EMERGENCIA POR COVID-19

En la presente sección se presenta una recopilación de las herramientas tecnológicas creadas o implementadas como respuesta a la emergencia por la pandemia por COVID-19, sus funcionalidades, sus defectos, el nivel de seguridad de la información o aspectos relevantes de la seguridad de las herramientas que puedan comprometer los datos, así como algunos casos de filtraciones de datos o vulnerabilidades de los sistemas.[10]

ARGENTINA

Argentina, junto a Brasil fue uno de los países donde se reportó una explosión descontrolada de aplicaciones. En un trabajo realizado por la Asociación por los Derechos Civiles (ADC),[11,12] fueron reportadas 11 aplicaciones: una de cobertura nacional; ocho de cobertura provincial y dos de cobertura municipal.



De estas aplicaciones, Cuidar App es la aplicación lanzada por el gobierno central. En su versión actual, la aplicación tiene dos objetivos: a) Ser una herramienta para el auto diagnóstico; y, b) Ser una alternativa para las personas para almacenar el Certificado Único Habilitante de Circulación (presentado como código QR por defecto), para ser presentado a las autoridades cuando sea procedente. En caso de mostrar síntomas de la enfermedad, se envía la información al Comité Operativo

10 Un resumen de esta sección es presentado al final del artículo como anexo.
11 https://adc.org.ar/2020/05/21/en-caso-de-emergencia-descargue-una-app/
12 https://adc.org.ar/2020/12/22/en-caso-de-emergencia-descargue-una-app-parte-ii/

de Emergencia Provincial de la jurisdicción en la que el paciente se encuentre, para ser contactado y brindar la asistencia que requiere. Si la persona presenta un resultado negativo en la autoevaluación, obtiene el código que le permite movilizarse en los espacios públicos.

Una de las principales críticas a la versión para Android de esta aplicación fue que solicitaba una gran cantidad de permisos para el teléfono, por ejemplo, acceso a la geolocalización (aproximada y precisa), calendario, contactos, micrófono, cámara, acceso completo a la red con la capacidad de ver las conexiones de red, configuración de audio, inicio cuando se enciende el dispositivo y prevenir que el teléfono se duerma.

Otro problema fue, siempre de acuerdo con el citado trabajo de ADC, la detección de vulnerabilidades y problemas de seguridad que tuvieron su origen en el desarrollo de la aplicación. De acuerdo con el informe: "Expertos de la comunidad técnica compartieron, principalmente por redes sociales, que la aplicación (app) tendría una vulnerabilidad en la generación del token de validación de un solo uso asociado al dispositivo, convirtiendo a la autenticación de dos factores absolutamente predecible." También fueron reportados problemas de funcionamiento, especialmente en la generación del código QR para poder circular.[13]

Los datos colectados por la aplicación, de acuerdo con la Disposición 3/2020, fueron centralizados en una plataforma llamada "COVID-19 Ministerio de Salud"; en este caso, la información recolectada fue almacenada en la nube, proveída por Amazon Web Services, Inc.

De acuerdo con el informe de ADC ya citado, la Secretaría de Innovación anunció la publicación del código fuente de la aplicación, con la intención de garantizar la transparencia, en tanto que éste podía ser auditado y revisado. Sin embargo, además de la tardanza en publicar el código, cuando se hizo, se hizo incompleto, puesto que únicamente se subió el código del lado del cliente y no del lado del servidor, lo que hubiera permitido "... analizar y transparentar efectivamente todo el circuito de recolección y tratamiento de datos personales."

13 https://www.cronista.com/economia-politica/Fallas-en-la-app-CuidAR-como-evitar-el-estres-de-no-tener-el-certificado-a-mano-20200703-0004.html

Respecto de las otras aplicaciones creadas a otros niveles, la ADC señaló algunos de los inconvenientes que estas presentan:

1. Un solapamiento de las finalidades que dicen perseguir, lo que dificulta saber cuál es la necesidad que pretenden solucionar;
2. Términos y condiciones que no establecen el periodo de tiempo para eliminar los datos recolectados, así como cláusulas muy amplias de cesión de datos entre instituciones;
3. La limitada calidad y precisión de los datos obtenidos en las aplicaciones de autoevaluación; y,
4. Una fuerte tendencia a la cultura de persecución ciudadana en aquellas aplicaciones que permiten interponer avisos de personas incumpliendo la cuarentena.

FILTRACIONES DE DATOS Y OTROS RIESGOS

Durante la pandemia ocurrió un incidente de exposición de datos personales con una aplicación que pertenecía a la provincia de San Juan, por medio de la cual podía solicitarse permisos para la circulación durante la cuarentena. Según un informe[14], "la base de datos, con información de más de 115 000 argentinos que solicitaron permisos de circulación, se subió a la red sin contraseña ni ningún otro tipo de autenticación de acceso". La información filtrada contenía datos personales como el nombre, el número de identidad, el número fiscal (CUIL), la foto y en algunos casos, el número de teléfono. Además, usando la opción para comprobar el estado de la solicitud, usando los datos expuestos, se podía consultar el permiso, que revelaba más datos, como el lugar y empresa donde la persona trabaja, los lugares a los que puede ir durante la cuarentena, si la persona es personal sanitario o no, y otros.

También la aplicación desarrollada en la provincia de Salta fue puesta a disposición de los ciudadanos con serios problemas de seguridad, con el potencial riesgo de exponer datos personales y de salud de las personas que la instalaran.

Otro hecho que puso en evidencia el bajo nivel de seguridad informática fue el ataque de *ransomware* perpetrado en contra de la base de datos de la Oficina Nacional de Migraciones[15]. Al no ser pagado el "rescate" exigido, los datos fueron publicados en internet; entre los datos publicados se encontraban los datos de todas las personas repatriadas a Argentina en el contexto de la pandemia.

14 https://www.comparitech.com/es/blog/seguridad-de-informacion/en-argentina-el-ministerio-de-sanidad-hace-publica-la-informacion-personal/
15 https://www.pagina12.com.ar/290338-hackers-atacaron-la-direccion-nacional-de-migraciones

Uno de los temas que generó mucho debate fue la presentación del denominado "Protocolo General para la Prevención Policial del Delito con Uso de Fuentes Digitales Abiertas", mediante el cual se buscaba "...establecer principios, criterios y directrices generales para las tareas de prevención del delito que desarrollan en el espacio cibernético los cuerpos policiales y fuerzas de seguridad dependientes del MINISTERIO DE SEGURIDAD" (Art.1).

El Protocolo buscaba atender "...al desarrollo de la criminalidad vinculada a la comercialización, distribución y transporte de medicamentos apócrifos y de insumos sanitarios críticos; a la venta de presuntos medicamentos comercializados bajo nomenclaturas y referencias al COVID-19 o sus derivaciones nominales, sin aprobación ni certificación de la autoridad competente; y a los ataques informáticos a infraestructura crítica —especialmente a hospitales y a centros de salud—..." (Art. 3).

Sobre esta norma, diversas organizaciones[16,17] criticaron que las actividades reguladas en el Protocolo siguen siendo constitutivas de ciberpatrullaje y no prácticas de "tareas preventivas" como se les ha denominado. Asimismo, la Agencia de Acceso a la Información Pública (AAIP) expresó sus observaciones, recomendando la suspensión de la aplicación del Protocolo hasta que se revise la adecuación de éste con la norma vigente de protección de datos personales.[18]

BOLIVIA

Durante la pandemia, Bolivia utilizó herramientas tecnológicas, al igual que la mayoría de los países alrededor del mundo, como una medida para evitar la propagación del virus.

Por un lado, se desarrolló la plataforma "Bolivia Segura," con el objetivo de brindar información confiable a la población, estadísticas sobre la evolución de la enfermedad y la posibilidad de realizar una autoevaluación para determinar si se había contraído el virus; esta plataforma originalmente fue administrada por la Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación (AGETIC) y posteriormente por el Ministerio de Comunicación. Según fue reportado, la información epidemiológica ahí mostrada presentó inconsistencias y demoras considerables de actualización; observándose, incluso, cambios en los números de decesos.

16 https://www.vialibre.org.ar/wp-content/uploads/2020/04/Respuesta.-Res.-Ministerial.-Ciberpatrullaje.pdf
17 https://observatoriolegislativocele.com/ciberpatrullaje-o-inteligencia/
18 https://www.vialibre.org.ar/wp-content/uploads/2020/08/NO-2020-47326285-APN-AAIP-1.pdf

Posteriormente fue lanzada la aplicación “Bolivia Segura”, la cual contenía un módulo para realizar auto evaluación. La aplicación solicitaba el nombre, número de documento de identidad, la edad y la dirección del usuario; esta información era contrastada con la base de Datos del Servicio General de Identificación Personal (Segip), para la validación. La aplicación también ofrecía autenticación biométrica a través de la huella dactilar. Otros datos que solicitaba eran la sintomatología (por el módulo de autoevaluación) y, la geolocalización para notificar a una persona en riesgo de contagio, conforme al lugar en el que se encontraba en un determinado momento. De acuerdo con los términos y condiciones, la información se almacenaba en los servidores de la AGETIC, bajo la responsabilidad del Ministerio de Comunicaciones.

Sobre esta aplicación, se alertó que:

1. permitía el acceso a los datos por parte de terceros para fines lícitos, sin detallar quiénes podían ser esos terceros y qué se entendería por “fines lícitos”;
2. la ausencia de medidas de seguridad para la protección de los datos personales;
3. la ausencia de un proceso para acceder a los datos que el usuario ingresa; y,
4. la interoperabilidad con otras instituciones como el SEGIP y el Ministerio de Salud, sin contar con una Ley de Protección de Datos Personales que garantice el uso adecuado de los datos y los mecanismos de seguridad apropiados.

Otras herramientas de carácter regional que fueron creadas son: la aplicación “Salud Cochabamba” para el Departamento de Cochabamba y el *chatbot* “Dr. Sammy Bot” para los departamentos de La Paz y Santa Cruz.

FILTRACIONES DE DATOS Y OTROS RIESGOS

Además de lo señalado respecto a la ausencia de una ley específica para la protección de los datos personales, hay que añadir que en Bolivia se presentó, por lo menos, un caso de filtración de datos personales, desde una cuenta institucional del gobierno, que resguardaba datos de personas infectadas por COVID-19.[19]

19 https://internetbolivia.org/wp-content/uploads/2020/11/fd_tecnopandemia_2021.pdf

Esto ocurrió en el mes de abril, en una cuenta institucional del Ministerio de Justicia en Twitter, desde la cual se divulgó una lista con pacientes que padecían COVID-19, perteneciente a la Gobernación de Santa Cruz, que contenía otros datos personales como la edad, la dirección, entre otros. Aunque las autoridades locales emitieron un comunicado señalando que la lista era falsa, se logró establecer que la referida lista sí estuvo alojada en la página oficial de esa Gobernación, lo que implica que existió, de hecho, una vulneración a la seguridad de la información.

Es prudente señalar que, a pesar de no haber evidencia de que esta información haya sido usada maliciosamente por terceros, el hecho en sí mismo refleja los peligros de una mala gestión de seguridad en el resguardo de los datos personales.

BRASIL

En Brasil hubo una aplicación de alcance nacional y algunas iniciativas estatales. La aplicación "Coronavirus-SUS", de aplicación nacional, fue desarrollada por el Departamento de Informática del Sistema Único de Salud (DataSUS), vinculado al Ministerio de Salud del Gobierno Federal, según informaciones oficiales originalmente publicadas en el sitio web del Ministerio que actualmente están indisponibles. Según la Política de Privacidad de la aplicación, el fin específico del tratamiento de los datos es permitir al Ministerio de Salud identificar e informar a los usuarios y usuarias sobre eventuales contactos con personas que se detectaron como infectadas con COVID-19.

Según información analizada por la organización de la sociedad civil InternetLab, aunque existe una Política de Privacidad disponible en la versión actual de la aplicación, su redacción presenta inconsistencias relevantes. En la solicitud de consentimiento presente en dicha política se indica que no hay recolección de datos personales, pero que la aplicación recolecta "la llave del teléfono móvil", algo que teóricamente puede identificar al sujeto de los datos, así como un test positivo para el COVID-19. La solicitud de consentimiento tampoco explicita el rol de Amazon Web Services, con quien se comparten datos, o el hecho de que parte de la comunicación de datos de la aplicación no esté encriptada. Siempre con información de InternetLab, la Política de Privacidad explicita cómo los titulares de datos pueden ejercer los derechos de acceso, rectificación, cancelación y oposición por medio del correo electrónico dpo@saude.gov.br; sin embargo, el usuario debe consentir con todos los usos después de la instalación para poder utilizar la aplicación. La única funcionalidad a la que el usuario puede consentir de manera optativa (*opt-in*) es la ubicación y el *bluetooth*, necesarios para la trazabilidad de contactos. El régimen normativo aplicable a esta aplicación es el de la Ley General de Protección de Datos.

Además, fueron desarrolladas soluciones tecnológicas en otros estados y municipios. Por ejemplo, en Río de Janeiro y Sao Paulo fueron desarrolladas soluciones para el monitoreo de las aglomeraciones y movimientos de la población mediante uso de datos agregados y anonimizados de conexión del celular a las torres de telefonía; estas fueron logradas a través de acuerdos firmados con las empresas Claro, Oi, TIM y Vivo.

También fueron desarrolladas soluciones por empresas dedicadas a las herramientas de geolocalización para el monitoreo de movimiento de la población usando datos de geolocalización, en Recife y Santa Catarina. El sistema implementado en Recife también notificaba a las personas que mantenían un nivel de movimiento considerado "encima de la media"[20]; mientras que el sistema implementado en Santa Catarina incluso enviaba notificaciones a las personas que vivían cerca de personas infectadas con el virus.

Otra aplicación que hizo uso de la geolocalización fue la implementada en Amazonas, la cual monitoreaba a personas contagiadas con el virus y les ofrecía servicios de telemedicina. El monitoreo se hacía a través de la información sobre la evolución del cuadro de la enfermedad que debía ofrecer los pacientes.

En algunos casos, las principales observaciones a este tipo de soluciones tienen que ver con la falta de transparencia en relación con los términos de los acuerdos firmados entre los gobiernos, y el no consentimiento de los usuarios.[21]

En el caso del Sistema de Monitoreo Inteligente implementado en Sao Paulo, al cual se hace referencia en párrafos anteriores, existe una sección de preguntas y respuestas en el sitio del Instituto de Pesquisas Tecnológicas (IPT) en el cual se encuentran aspectos relacionados al funcionamiento del sistema[22]; e incluye un extracto del convenio firmado con las operadoras telefónicas.[23]

20 De acuerdo con declaraciones del Secretario Ejecutivo de Innovación Urbana de Recife, lo que debe analizarse primero es lo que caracteriza como "normal" la movilización en una localidad; por ejemplo, un barrio donde exista un hospital tendrá más movilización que uno en el que haya un parque. Entrevista en: https://www.uol.com.br/tilt/noticias/redacao/2020/03/28/recife-rastreia-o-celular-de-800-mil-pessoas-para-saber-quem-sai-de-casa.htm

21 https://br.boell.org/sites/default/files/2020-06/Tecnologias%20e%20Covid-19%20no%20Brasil%20vigil%C3%A2ncia%20e%20desigualdade%20social%20na%20periferia%20do%20capitalismo.pdf

22 https://www.ipt.br/noticia/1623-_perguntas_sobre_isolamento_social.htm

23 https://www.ipt.br/download.php?filename=1920-Extrato_ACT_Prestadoras_de_Servicos_de_Telecomunicacoes.pdf

FILTRACIONES DE DATOS Y OTROS RIESGOS

Durante la pandemia se documentó la fuga de datos personales en, por lo menos, dos ocasiones en el Ministerio de Salud. En el primer caso[24], fueron expuestos datos sensibles de 16 millones de brasileños afectados por la COVID-19, mientras que en el segundo[25] fueron más de 200 millones de brasileños afectados, entre quienes estaban, además de personas afectadas por la pandemia, ciudadanos registrados en el Sistema Único de Salud o en un plan de salud. En total la cifra sobrepasa el número de la

población total de Brasil, ya que en dicha filtración también se encontraban los datos de personas fallecidas. Los datos expuestos incluían nombre completo, dirección, teléfono celular y número del Registro de Personas Físicas (CPF). El sistema, llamado e-SUS-Notifica fue desarrollado por la empresa de tecnología Zello. Por estas fugas, el Ministerio de Salud podría ser sancionado conforme a la nueva Ley de Protección de Datos, pues la obligación de brindar la necesaria seguridad a los datos es del controlador de los mismos (Art. 41 y 42 LGPDP).

Además del caso de fuga de datos personales en el portal e-SUS-Notifica, citado párrafos atrás, en el mes de noviembre se reportó lo que parece haber sido un ataque cibernético a la red del Ministerio de Salud, lo que afectó la contabilización de los datos sobre COVID-19 en algunos estados.[26] No hubo evidencia, según declaraciones de las autoridades pertinentes, de compromiso, secuestro o fuga de los datos en este ataque.[27]

COLOMBIA

Colombia, al igual que muchos países en el mundo, también hizo uso de herramientas tecnológicas, como parte de su estrategia para enfrentar la pandemia. En este sentido, la aplicación lanzada por el gobierno central se denominó “CoronApp,” que fue impulsada por la presidencia de la República y estuvo a cargo del Instituto Nacional de Salud (INS) y de la Agencia Nacional Digital (AND).

24 https://www.privacytech.com.br/destaque/vazamento-no-ministerio-da-saude-expoe-dados-de-16-milhoes-de-pacientes-de-covid.,381009.jhtml
25 https://www.privacytech.com.br/destaque/mais-de-200-milhoes-de-brasileiros-tem-dados-pessoais-expostos-em-nova-falha-de-seguranca-do-ministerio-da-saude.,381645.jhtml
26 https://g1.globo.com/ciencia-e-saude/noticia/2020/11/13/ministerio-da-saude-diz-que-ha-indicios-de-que-a-pasta-tenha-sido-alvo-de-ataques-ciberneticos.ghtml
27 https://g1.globo.com/ciencia-e-saude/noticia/2020/11/06/ministerio-enfrenta-incidente-em-sistemas-que-afeta-atualizacao-de-casos-e-mortes-da-covid-19.ghtml

Esta aplicación ya existía desde el año 2017; en ese año se llamaba "Guardianes de la salud" y fue lanzada en vísperas de la visita del Papa a Colombia con los objetivos de monitorear los riesgos de salud que podrían ocasionarse entre las aglomeraciones y que los usuarios reportaran si se encontraban enfermos. Desde marzo de 2020, usando como base el código fuente de la aplicación de 2017, se convirtió en "CoronApp," que para esas fechas tenía fines informativos y de rastreo de síntomas de la enfermedad. Sus funcionalidades permitían que el usuario recibiera información sobre la enfermedad, alertas, reporte del estado de salud y autoevaluación; luego le fueron añadidas las funciones de rastreo de ubicación y rastreo de contagio por proximidad.

La aplicación solicitaba estos datos personales: nombre y apellido, número de documento y número de celular; además solicitaba datos de salud, como los siguientes: factores de riesgo (viajes, contactos) y agravantes (enfermedades crónicas, tabaquismo, etcétera) y reporte de estado de salud (fiebre, tos, dificultad para respirar, etcétera); y, solicitaba los siguientes permisos: acceso a la localización (red y GPS), *bluetooth*, redes WIFI, ejecutarse sola al inicio e impedir que el teléfono entre en modo de suspensión y llamar directamente a números de teléfono. Mientras que el celular envía periódicamente un reporte de la ubicación GPS del dispositivo (rastreo de ubicación), el *bluetooth* y las redes WIFI circundantes sirven para identificar otros dispositivos cercanos (rastreo de proximidad).

En un inicio, la aplicación usaba el sistema de rastreo de contagio por proximidad de la empresa estadounidense HypeLabs, que fue identificado como un protocolo de *bluetooth* centralizado. Después fue incorporado el protocolo "Blue Trace" desarrollado para la aplicación de Singapur "Trace Together", por medio del cual "…cada dispositivo guarda en una base de datos local la lista de los identificadores de dispositivos con los cuales se ha cruzado". De acuerdo con la Fundación Karisma, aunque este protocolo atacaba el problema de la privacidad, realmente seguía siendo un protocolo centralizado, ya que los identificadores eran generados por una base de datos alojada en un servidor central. Como la misma institución señala, el riesgo a la privacidad con este proceso sigue siendo alto, pues el servidor tiene la capacidad de "desanonimizar" los identificadores, lo que vuelve identificable al usuario.[28]

En un informe[29] elaborado por la Fundación Karisma fueron reveladas algunas fallas en la aplicación, en sus primeras versiones. Por ejemplo, el envío de los datos se hacía sin seguridad y sin cifrado, con el protocolo HTTP. También se reportó una vulnerabilidad grave relacionada a un defecto de autenticación, que permitía a un

28 https://web.karisma.org.co/que-dice-que-hace-y-que-es-lo-que-realmente-hace-coronapp/
29 https://web.karisma.org.co/wp-content/uploads/2020/04/Informe-p%C3%BAblico-t%C3%A9cnico-CoronApp-v170320-1-1.pdf

atacante acceder a los datos personales de los usuarios en el servidor “del lado del cliente” de la aplicación. No obstante, estos defectos fueron posteriormente subsanados.

El informe, además, cuestiona la protección de los datos personales, es decir, la falta de información sobre cómo se gestiona la privacidad y seguridad de los datos. No está claro qué pasará con los datos una vez finalizada la fase de emergencia y las condiciones de servicio tienen referencias muy generales al cumplimiento de las obligaciones legales de protección de datos.

En un informe elaborado por la Fundación Karisma se cuestiona la falta de información sobre cómo se gestiona la privacidad y seguridad de los datos por la CoronApp Colombia.

En este contexto, la Superindentencia de Industria y Comercio (SIC) recomendó al Instituto Nacional de Salud (INS), a la Agencia Nacional Digital y a la Consejería Presidencial para asuntos Económicos y de Transformación Digital que se elaborara una política de tratamiento de la información especial, que la base de datos de la aplicación “CoronApp” fuera inscrita ante la SIC, que se realizara una auditoría a los niveles de seguridad de la aplicación y que se diera a conocer a la ciudadanía la política de tratamiento de la información, en términos de fácil entendimiento.

Otro problema en la implementación de la aplicación estuvo ligada a la obligatoriedad de la descarga. Aunque la última versión de la Política de Tratamiento de la Información señalaba que la descarga, uso y desinstalación de la aplicación era voluntaria, en el mismo documento se señalaba que, por estar en un contexto de emergencia, esa libertad no aplicaba en el caso de “CoronApp”.

Al igual que en otros países de Sudamérica, fueron creadas otras aplicaciones que compitieron con la aplicación impulsada por el gobierno central. En el caso colombiano, “Medellín me cuida”, para la municipalidad de Medellín, fue un formulario web y “CaliValle Corona”, una aplicación para Cali y el Valle del Cauca.

ECUADOR

Durante la emergencia por la pandemia, al igual que la mayoría de los países en el mundo, Ecuador echó mano de las herramientas tecnológicas, como parte de las medidas para mitigar la expansión del virus. En el marco del Decreto Ejecutivo Nº 1017 que permitía el uso de herramientas de georreferenciación fue creada la aplicación Salud EC, por medio de la cual, las personas podían realizar un triaje médico de manera virtual para evaluar si tenía los síntomas de la COVID-19, agendar citas no referentes

a la pandemia en el sistema de salud ecuatoriano, contactar con los diferentes canales del sistema de salud y obtener información oficial sobre la pandemia. La principal preocupación con esta aplicación tuvo que ver con la gran cantidad de datos personales que solicitaba (nombre, año de nacimiento, documento de identidad, número de teléfono, correo electrónico y dirección geolocalizada), lo cual iba en contra del principio de minimización de datos, pues se estaban solicitando datos adicionales, como la georreferenciación de la dirección del usuario, que no eran necesarios para el objeto de la aplicación.

También fue implementada en Pichincha la "Plataforma Digital COVID-19,"[30] desarrollada en colaboración entre el gobierno y empresas privadas Claro, Grupo Link, Kin Analytics, y Movistar. Esta plataforma fue creada con el objetivo de "…controlar la cuarentena para que no se rompa el aislamiento, definir cercos epidemiológicos, efectuar pruebas masivas de COVID-19 de registrados en el 171 y Salud Ec, vigilar aglomeraciones, fumigaciones en zonas de contagio y aplicar sanciones a quienes hayan incumplido el toque de queda".

Esta plataforma fue diseñada para:

1. Gestionar la cuarentena y los cercos epidemiológicos, realizando el seguimiento de las personas, a través de Apps, centros de contacto y herramientas georreferenciales;
2. Gestionar la aplicación de tests masivos, a través de la información obtenida de las llamadas realizadas por los usuarios al número telefónico 171; y,
3. Controlar las aglomeraciones y la movilidad, mediante la geolocalización de reuniones de más de 30 personas, a través del uso de cámaras del 911 y el Big Data de las empresas de Telecomunicaciones.

Sobre esta plataforma, la principal alerta tiene que ver con la enorme cantidad de datos que se recopilaron a través de la integración de múltiples bases de datos. Debería haber existido un tratamiento lo suficientemente robusto para asegurar la integridad de los datos ahí resguardados; para que éstos no fueran usados indebidamente y no representaran un riesgo para la privacidad y la autodeterminación informativa de las personas.

Finalmente, fue desarrollada la aplicación "Ecuador Así", por la empresa Link, en colaboración con el Banco Interamericano de Desarrollo (BID), para la notificación de contactos por proximidad física, a través de tecnología *bluetooth*. De acuerdo con los términos de privacidad, tanto la descarga de la aplicación como la notificación de resultado positivo o sospecha de contagio por COVID-19, eran voluntarias. No eran

30 https://www.telecomunicaciones.gob.ec/el-gobierno-nacional-pone-al-servicio-de-la-capital-de-la-republica-un-nuevo-instrumento-tecnologico-para-enfrenar-el-coronavirus-la-plataforma-digital-covid-19/

requeridos, para su instalación o uso, el registro de información del usuario sobre su identidad, domicilio, correo electrónico o número de teléfono; según el documento, la aplicación tampoco accedía a los datos almacenados en los teléfonos donde la aplicación era instalada, ni rastreaba la ubicación del usuario.

Como puntos cuestionables, puede señalarse que en los términos de uso no existe ningún tipo de orientación a los usuarios para el ejercicio de los derechos de acceso, rectificación, cancelación u oposición; por otro lado, en un análisis de la aplicación del Observatorio Ciberderechos & Tecnosociedad de la Universidad Andina Simón Bolivar[31], se presentaron observaciones informativas, jurídicas y técnicas, que deberían haber sido tomadas en cuenta para la protección de los datos personales de los ecuatorianos, sobre todo tomando en cuenta que:

a. Ecuador, en ese momento, era uno de los pocos países que no contaba con una Ley especializada para la protección de los datos personales; y,
b. La fuga masiva de datos ocurrida en septiembre de 2019.

En un análisis de la aplicación "Ecuador Así", del Observatorio Ciberderechos & Tecnosociedad de la Universidad Andina Simón Bolivar, se presentaron observaciones informativas, jurídicas y técnicas, que deberían haber sido tomadas en cuenta para la protección de los datos personales de los ecuatorianos.

Destaca, dentro de estas observaciones, lo señalado en el numeral 4 de las observaciones informativas: "Para la promoción de la aplicación se envían mensajes SMS de emergencia (SNGRE) sin haber requerido el consentimiento de los usuarios. Cabe mencionar que recibir estos SMS directamente de SNGRE es una mala práctica de seguridad. Atacantes maliciosos podrían utilizar el mismo sistema para realizar ataques de ingeniería social (*phishing*) contra los usuarios como medio para propagar *malware*."

EL SALVADOR

Durante la emergencia nacional, se implementaron algunas medidas tecnológicas, que serán detalladas a continuación:

1. El *chatbot* "SIVI,"[32] que fue desarrollado entre la Secretaría de Innovación, Facebook y la empresa Infobip. El *chatbot* funcionaba así: a través de un menú con seis opciones, el

31 https://www.uasb.edu.ec/web/ciberderechos/analisis-de-la-aplicacion-asi-ecuador
32 https://diario.elmundo.sv/sivi-respondera-dudas-sobre-covid-19-desde-messenger-de-facebook/

usuario podía: realizar un auto-test (respondiendo preguntas sobre síntomas), conocer los principales síntomas y vías de contagio, conocer en qué consistía la cuarentena domiciliar, recibir consejos para la prevención, conocer la existencia de mitos y rumores sobre el virus y generar denuncias (no se conoce sobre qué se podía denunciar y cuál era este proceso).

Este *chatbot* estaba alojado primeramente en la página de Facebook del Ministerio de Salud, para luego mudar a WhatsApp. Aunque la herramienta únicamente pedía ingresar el nombre para interactuar y luego, si el usuario lo deseaba, introducir datos sobre su salud (síntomas), lo que podría clasificarse como un uso proporcional en el tratamiento de los datos, no podemos olvidar que esta herramienta, al estar ligada al uso de un teléfono celular, también es susceptible de generar otro tipo de datos, como la geolocalización del usuario y la identificación del mismo a través de las bases de datos de las empresas de telefonía.

Esto es importante ponerlo en consideración, si consideramos que los operadores telefónicos deben mantener un registro de los usuarios (Art. 30-A Ley de Telecomunicaciones), que deberá mantener a disposición de las autoridades sin especificación del tiempo para su resguardo. En la misma línea, la Ley Especial para la Intervención de las Telecomunicaciones en su artículo 47 establece que los operadores deberán entregar a la Fiscalía General de la República, en caso sea requerido, "… los informes relativos a los datos de registro de la línea o líneas telefónicas investigadas y los registros de llamadas, correos electrónicos y otros medios de telecomunicaciones…" Tampoco puede ignorarse que la aplicación WhatsApp, propiedad de Facebook, tiene sus propios procesos para tratar datos, por lo que el riesgo de creación de perfiles para la publicidad o cualquier otra actividad fuera del objetivo para el que fue utilizado el *chatbot* no puede descartarse.

Con todo, no es posible afirmar que haya existido un tratamiento indebido de datos personales, en la medida en que no se tuvo conocimiento de ninguna denuncia sobre este particular, en los tres meses en que funcionó, ni en noticias, ni en los círculos de profesionales de las tecnologías.

2. La página web para consultar sobre el beneficio económico otorgado por el gobierno en el marco de la cuarentena. La consulta se hacía ingresando el número de Documento Único de Identidad; si resultaba beneficiado, tenía que dirigirse a uno de los bancos del sistema bancario para retirar el importe asignado (USD $300). El primer sitio no poseía certificado de seguridad, una falla recurrente en los sitios gubernamentales. Cuando este sitio colapsó, éste fue mudado a otro servidor. No se tiene conocimiento de algún incidente que afectara los datos personales de los beneficiarios, al mismo tiempo que se desconoce el tratamiento que se haya realizado a la base de datos (subsidio del gas licuado) que alimentó el sitio en cuestión.

   Aunque no existe documento alguno que reporte casos de filtraciones de datos o vulnerabilidades de sistemas, se lograron identificar algunas debilidades respecto de algunas herramientas tecnológicas que el gobierno implementó como parte de la respuesta a la emergencia por COVID-19; la más recurrente fue la falta de certificados de seguridad en las plataformas y páginas web. Entre estos sitios sin certificado de seguridad, se encontraba

la plataforma que fue habilitada para consultar, introduciendo el número de Documento Único de Identidad, si una persona era beneficiaria de la ayuda económica que el gobierno entregó en los primeros días de la cuarentena; este sitio, que colapsó en cuestión de minutos, no tenía certificado SSL[33]. Otro caso fue la implementación de un "carnet de inmunidad" alimentado con la base de datos de recuperados de la enfermedad, que contenía un código QR, que llevaba a un sitio web que tampoco contaba con certificado de seguridad.[34]

En el caso de El Salvador se lograron identificar algunas debilidades respecto de algunas herramientas tecnológicas que el gobierno implementó como parte de la respuesta a la emergencia por COVID-19.

Este asunto cobra mayor relevancia si se analiza en conjunto con otros casos fuera de la temática de COVID-19, que ponen en evidencia la falta de medidas básicas de seguridad en las páginas web de instituciones gubernamentales. En primer lugar, el caso de la publicación de datos confidenciales de más de cinco millones de salvadoreños en el sitio web del Ministerio de Hacienda[35], En segundo lugar, el hackeo a la página web de la estatal Universidad de El Salvador, mediante el cual las notas de los estudiantes fueron cambiadas[36]. En tercer lugar, de manera general, la falta de certificados de seguridad en páginas web de Ministerios del gobierno salvadoreño.

Finalmente, uno de los casos más delicados sobre seguridad de la información está relacionado con el envío de los resultados de las pruebas COVID-19. Según un artículo periodístico, los resultados de los análisis de las pruebas COVID-19 son enviados en formato Excel, a través de WhatsApp, al Ministro de Salud y a asesores del presidente, teniendo además prohibido que los resultados se incorporen a la plataforma en línea del Sistema de Vigilancia Epidemiológica.[37]

33 https://www.elsalvador.com/noticias/nacional/web-subsidio-coronavirus-colapsa/700662/2020/
34 https://diario.elmundo.sv/gobierno-inicia-con-la-entrega-de-carnes-de-inmunidad-a-recuperados-de-covid-19/
35 https://gatoencerrado.news/2020/07/10/hacienda-publico-datos-privados-de-millones-de-salvadorenos/
36 https://www.elsalvador.com/noticias/nacional/hackean-sistema-web-universidad-el-salvador/732239/2020/
37 https://www.elsalvador.com/noticias/nacional/venezolanos-dirigen-mesa-toma-muestras-covid-19el-salvador/722087/2020/

2.2. MARCO LEGAL DE LA PROTECCIÓN DE LOS DATOS PERSONALES

En la presente sección, para los seis países en estudio, se hace una recopilación de la normativa, jurisprudencia, lineamientos o convenios nacionales relativos al tratamiento de datos personales y datos de salud, tanto en el momento previo a la pandemia, como aquellos emitidos durante el contexto de emergencia y pandemia por COVID-19. Se incluye lo relativo a las autoridades encargadas de la protección de los datos personales y sus competencias/facultades en materia de protección de datos.

Para una lectura más amigable, la información sobre la legislación será presentada en forma de tabla y se realizarán los comentarios pertinentes a continuación de esta.

TABLA I. MARCO LEGAL DE LA PROTECCIÓN DE LOS DATOS PERSONALES

Constitución	Ley de protección de datos personales	Tratados internacionales	Otras leyes secundarias	Jurisprudencia
Argentina				
Art. 43. Regula el Hábeas Data.[38]	Ley de Protección de Datos Personales (LDP) N° 25.326.[39]	Convenio 108 para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal[40], incorporado a través de la Ley Nº 27.483. Pacto Internacional de Derechos Civiles y Políticos de las Naciones Unidas (Art. 17); Declaración Universal de los Derechos Humanos (Art. 12) y Convención Americana sobre Derechos Humanos (Art. 11).	Decreto 1,558 de 2001 que reglamente la Ley de Protección de Datos Personales No. 25,326. "Guía en el tratamiento de datos personales en el uso de herramientas de geolocalización"[41] emitidos por la Agencia de Acceso a la Información Pública (AAIP) En el contexto de la pandemia, la AAIP publicó la "Guía sobre el tratamiento de los datos personales ante el coronavirus COVID-19."[42]	Sentencia de la Corte Suprema de Justicia de la Nación, del 15 de octubre de 1998, conocida como caso "Urteaga" en la que se dispuso al Estado la obligación de poner a disposición de los particulares la información contenida en sus bancos de datos o archivos.

38 http://servicios.infoleg.gob.ar/infolegInternet/anexos/0-4999/804/norma.htm
39 https://www.argentina.gob.ar/normativa/nacional/ley-25326-64790/texto
40 https://www.oas.org/es/sla/ddi/docs/U12%20convenio%20n%20108.pdf
41 https://www.argentina.gob.ar/sites/default/files/guia_geolocalizacion_0.pdf
42 https://www.argentina.gob.ar/sites/default/files/guia_coronavirus_0.pdf

Constitución	Ley de protección de datos personales	Tratados internacionales	Otras leyes secundarias	Jurisprudencia
Bolivia				
Art. 21. Establece el derecho a la privacidad, intimidad, honra, propia imagen y dignidad.[43] Art. 130. Regula la denominada Acción de Protección de Privacidad, desarrollada en el Art. 58 del Código Procesal Constitucional.	No existe	Pacto Internacional de Derechos Civiles y Políticos de las Naciones Unidas (Art. 17); Declaración Universal de los Derechos Humanos (Art. 12) y Convención Americana sobre Derechos Humanos (Art. 11).	Art. 56 Ley General de Telecomunicaciones y Tecnologías de la Información y Comunicación. Reforma al Art. 79 de la Ley del Órgano Electoral, refiriéndose a la interoperabilidad entre el Servicio de Registro Cívico (SERECI) y el Servicio General de Identificación (SEGIP). Art. 12 de la Ley de Ciudadanía Digital. Art. 19 del Decreto Supremo Nº 28168, de 18 de mayo de 2005. Regula el Habeas Data	El derecho a la autodeterminación informativa fue introducido como un derecho humano, por medio de la Sentencia Constitucional Plurinacional 0090/2014-S1.[44]
Brasil				
Art. 5 inciso X de la Constitución, que regula la inviolabilidad de la intimidad, la vida privada, la honra y la imagen de las personas. Inciso XII, que regula la inviolabilidad de las comunicaciones; y, el inciso LXXII que regula el Hábeas Data.[45]	Ley General de Protección de Datos Personales (LGDP, Ley 13.709/18)[46]	Pacto Internacional de Derechos Civiles y Políticos de las Naciones Unidas (Art. 17); Declaración Universal de los Derechos Humanos (Art. 12) y Convención Americana sobre Derechos Humanos (Art. 11).	Marco Civil de Internet (Ley Nro. 12,965 de 2014)[47] Ley No. 9,507 de 1997 que regula el Habeas Data. Código de Defensa del Consumidor (Ley Nro. 8,078 de 1990)	

43 https://www.oas.org/dil/esp/constitucion_bolivia.pdf
44 https://jurisprudenciaconstitucional.com/resolucion/13467-sentencia-constitucional-plurinacional-0090-2014-s1
45 http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm
46 http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm
47 http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm

Constitución	Ley de protección de datos personales	Tratados internacionales	Otras leyes secundarias	Jurisprudencia
Colombia				
Art. 15 de la Constitución Política[48] establece el derecho de las personas a "...conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas."	Ley Nº 1581 del año 2012, que dicta las disposiciones generales para la protección de los datos personales.[49]	Pacto Internacional de Derechos Civiles y Políticos de las Naciones Unidas (Art. 17); Declaración Universal de los Derechos Humanos (Art. 12) y Convención Americana sobre Derechos Humanos (Art. 11).	Marco Civil de Internet (Ley Nro. 12,965 de 2014) Ley No. 9,507 de 1997 que regula el Habeas Data. Código de Defensa del Consumidor (Ley Nro. 8,078 de 1990) Ley 1266 del año 2008 que regula el habeas data. Decreto 1377 del año 2013, que reglamenta parcialmente la Ley Nº 1581.	Sentencia T-414 de 1992[50], que desarrolla el derecho al Habeas Data como una garantía del derecho a la intimidad. Esta línea ha evolucionado y desde la Sentencia SU-082 de 1995 se considera al HD como un derecho autónomo; esta consideración es reiterada con la Sentencia C-1011 de 2008[51] dictada por la Corte Constitucional.
Ecuador				
Art. 66, numeral 19 de la Constitución de la República[52] garantiza el derecho de las personas a que sus datos de carácter personal sean protegidos y que para el tratamiento de estos sea requerido su consentimiento o sea mandado por Ley. Art. 92 regula el Habeas Data.	Ley Orgánica de Protección de Datos Personales, R.O. Nro. 459, de 26 de mayo de 2021.[53]	Pacto Internacional de Derechos Civiles y Políticos de las Naciones Unidas (Art. 17); Declaración Universal de los Derechos Humanos (Art. 12) y Convención Americana sobre Derechos Humanos (Art. 11).	Art. 21 de la Ley de Estadística. Art. 2 de La Ley Orgánica de la Gestión de la Identidad y Datos Civiles.	Sentencia No. 001-14-PO-CC de 3 de julio de 2014[54], de la Corte Constitucional que establece el criterio referencial para la protección de un dato y de la información de carácter personal.

48 https://pdba.georgetown.edu/Constitutions/Colombia/colombia91.pdf
49 https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981
50 https://www.corteconstitucional.gov.co/relatoria/1992/t-414-92.htm
51 https://www.corteconstitucional.gov.co/relatoria/2008/C-1011-08.htm
52 https://www.oas.org/juridico/pdfs/mesicic4_ecu_const.pdf
53 https://bit.ly/3c3wipJ
54 https://www.coronelyperez.com/wp-content/uploads/2019/10/5.-Habeas-Data-jurisprudencia-vinculante.pdf

Constitución	Ley de protección de datos personales	Tratados internacionales	Otras leyes secundarias	Jurisprudencia
El Salvador				
Art. 2 que regula el derecho al honor y la dignidad, de donde se deriva el derecho a la autodeterminación informativa.[55]	No	Pacto Internacional de Derechos Civiles y Políticos de las Naciones Unidas (Art. 17); Declaración Universal de los Derechos Humanos (Art. 12) y Convención Americana sobre Derechos Humanos (Art. 11).	Título III de la Ley de Acceso a la Información Pública (LAIP)[56] y su Reglamento (RELAIP).	Jurisprudencia de la Sala de lo Constitucional ha reconocido el Habeas Data y el derecho a la autodeterminación informativa, como un derecho fundamental, basado en art. 2 de la Constitución, que señala que el Estado garantiza la protección del honor y la dignidad de los salvadoreños.

Fuente: Elaboración propia.

De la información contenida en la Tabla 1, se puede observar que de los seis países en estudio, cuatro poseen una ley específica para la protección de los datos personales y 2 realizan esta tarea recurriendo a un entramado jurídico de normas constitucionales, convenios internacionales, leyes secundarias y jurisprudencia.

Los países que poseen una ley de protección de datos personales son Argentina, Brasil, Colombia y recientemente Ecuador. Los países que no cuentan con una ley en la materia son Bolivia y El Salvador. Sobre estos dos últimos países, se debe señalar que en El Salvador fue aprobada la Ley de Protección de Datos Personales, pero esta fue vetada por el presidente[57], por lo que continúa careciendo de una ley específica en la materia. En Bolivia, se han presentado, al menos, dos anteproyectos de ley para la protección de datos personales, sin que a la fecha haya habido algún avance en la sede legislativa para su aprobación.

55 https://www.asamblea.gob.sv/sites/default/files/documents/decretos/171117_072857074_archivo_documento_legislativo.pdf
56 https://www.asamblea.gob.sv/sites/default/files/documents/decretos/171117_073009410_archivo_documento_legislativo.pdf
57 https://bit.ly/3fW0rZ8

En aspectos más puntuales, vale la pena señalar, en primer lugar, la regulación de la entidad encargada de la protección de los datos personales; y, en segundo lugar, la forma en la que son considerados los datos de salud en los respectivos países.

Sobre las autoridades de protección de datos personales, en Argentina, la Autoridad encargada del control de la Ley de Datos Personales es la Agencia de Acceso a la Información Pública (AAIP); la cual, a través del decreto N° 899/2017 subsumió las funciones de la Dirección Nacional de Protección de Datos Personales, que antiguamente cumplía las funciones establecidas en el Art. 29 de la Ley N° 25.326. La AAIP tiene competencia sobre los datos en poder de entidades públicas y privadas (Art. 21, 22 y 24). En tal sentido, a la Agencia le corresponde, entre otras, la facultad de sancionar las violaciones a la LDP, conforme al Art. 31 de dicha Ley.

En Bolivia, al carecer de una ley específica para la protección de datos personales, tampoco tiene una autoridad encargada de esta protección, por lo que la única vía es la de la acción de protección de privacidad, que se realiza en sede judicial.

En Brasil, la protección de los datos personales corresponde a la Autoridad Nacional de Protección de Datos (ANPD), de acuerdo con el Art. 55-J, romano I de la LGDP. La Autoridad, que es parte de la Presidencia de la República (Art. 55-A) y que recién fue constituida, posee facultades sancionatorias de carácter administrativo (Art. 55-J, romano IV); estas sanciones se encuentran en el Art. 52 de la Ley.

En Colombia, de acuerdo con el Art. 19 de la Ley Nº 1581, la autoridad encargada de la protección de los datos personales es la Superindentencia de Industria y Comercio (SIC), que tiene la facultad de imponer las sanciones contempladas en el Art. 23 de la misma normativa.

En Ecuador, de acuerdo con el Art. 75 de la Ley Orgánica de Protección de Datos Personales, la autoridad encargada es la Autoridad de Protección de Datos Personales, con potestades de vigilancia y sancionatorias, conforme a los literales “a” y “b” del mismo artículo.

En El Salvador, tampoco hay una ley específica sobre esta materia. La protección de los datos personales está encargada al Instituto de Acceso a la Información Pública (IAIP), de acuerdo con el Art. 51 de la Ley de Acceso a la Información Pública (LAIP). De manera más específica, los Lineamientos Generales de Protección de Datos Personales para Instituciones del Sector Público, en su Art. 45 señala las atribuciones del IAIP en materia de protección de datos personales; entre ellas, está la de ordenar, de oficio o a petición de parte, la supresión, rectificación, adición o restricción en la circulación de la información contenida en los archivos y las bases de datos, cuando éstas contravengan las normas sobre protección de los datos personales. Las facultades sancionatorias del

IAIP, otorgadas en el mismo artículo, se encuentran reguladas en el Título VIII de la LAIP, en el cual se establecen, tanto las infracciones, como las sanciones (Arts. 76 y 77, respectivamente).

En referencia a la forma en la que son considerados los datos de salud, en Argentina, por ejemplo, de acuerdo a la Ley N° 25.326, los datos relativos a la salud son considerados como datos sensibles, de acuerdo al Art. 2; guardando para ellos la protección especial del Art. 7, que establece que una persona no está obligada a proporcionar datos sensibles y que el tratamiento de estos datos sólo puede hacerse si media interés general autorizadas por ley o si son tratados con finalidades científicas y estadísticas, cuidando que los titulares no puedan ser identificados. Además, el Art. 8 señala específicamente para los datos de salud, que pueden ser recolectados y tratados, respetando siempre los principios del secreto profesional.

De los seis países en estudio, cuatro poseen una ley específica para la protección de los datos personales.

En Bolivia, por su parte, en cuanto a la protección de datos personales sensibles, entre los que se incluyen los datos de salud, hay que establecer como parte del marco legal para la protección de los datos personales, las siguientes referencias: a) la Sentencia Constitucional 0965/2004-R, que señaló, al establecer el ámbito de aplicación del habeas data que la protección que este mecanismo brinda incluye los siguientes ámbitos: "…e) Derecho de exclusión de la llamada 'información sensible' relacionada al ámbito de la intimidad de la persona…"; b) la Ley Nº 3131 del Ejercicio Profesional Médico, en la cual, si bien no se habla concretamente de datos personales sensibles, regula como derechos de los pacientes: la confidencialidad, el secreto médico y el respeto a su intimidad.

En Brasil, los datos personales de salud son considerados datos sensibles por la Ley Nro. 13.709/18 (Art. 5, romano II). Así, los datos sensibles pueden ser tratados, por regla general, únicamente cuando el titular o su tutor legal consientan, de manera específica y destacada, su tratamiento para fines específicos (Art. 11, romano I). Es decir, no sólo basta el mero consentimiento; sino que este debe ser específico, destacado y otorgado para un fin específico. Las excepciones a la necesidad de este consentimiento están reguladas en el romano II del mismo artículo.

En Colombia, los datos de salud, según el Art. 5 de la Ley Nº 1581, se incluyen en la categoría de datos sensibles, los cuales, por regla general no pueden ser tratados, pero que, como excepción, pueden ser tratados si se cumplen los supuestos del Art. 6.

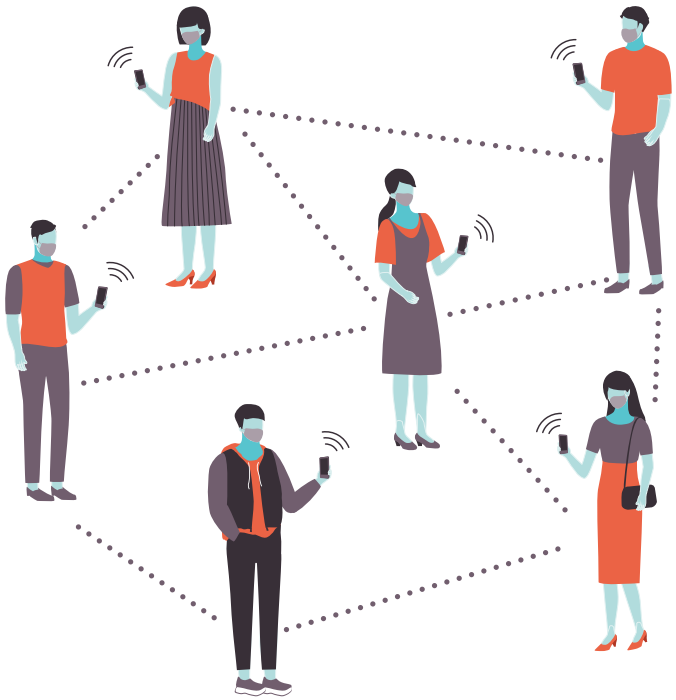
En Ecuador, los datos de salud se encuentran incluidos en las categorías especiales de datos personales que señala el Art. 25 de la Ley Orgánica de Protección de Datos

Personales, por lo que para su recolección y tratamiento se deberá atender lo dispuesto en los Arts. 30, 31 y 31 de la referida Ley. En tales artículos se regula la autorización para la colecta de estos datos, teniendo como límite la confidencialidad y la seguridad de los datos, así como las excepciones a la solicitud de consentimiento para colectarlos. Asimismo, se regulan los parámetros mínimos para el tratamiento de esta categoría de datos, en la que destaca la recomendación de anonimizar o seudonimizar los datos con el fin de que no sea posible la identificación del titular de los datos.

En el caso salvadoreño, la referencia a los datos de salud como datos sensibles se encuentra en el Art. 6 de la LAIP, que es la normativa que escuetamente desarrolla un capítulo sobre la materia. Sin embargo, el Instituto de Acceso a la Información Pública emitió en 2018 los "Lineamientos de normalización de la gestión y de protección de datos personales en los expedientes clínicos del Sistema Integrado de Salud de El Salvador" que, entre otras cosas, establece directrices para que los entes obligados que tratan información médica, adopten medidas para proteger los datos personales contra la alteración, pérdida, transmisión y acceso no autorizado, así como directrices para garantizar la reserva de los datos sensibles referentes a la salud física y mental de las personas y para la adopción de procesos para la recepción y respuesta de solicitudes de acceso, rectificación y supresión de datos personales. Por otra parte, en el año 2019, el Ministerio de Salud emitió la "Norma Técnica para la Conformación, Custodia y Consulta de Expediente Clínico", que regula la gestión documental y la protección de datos personales del expediente clínico y otros documentos relacionados con la atención de personas en las instituciones de salud. Esta norma establece el derecho de las personas al acceso, a la rectificación y a la supresión de la información del expediente clínico, así como las normas para la seguridad física e informática del expediente, según sea el caso.

2.3. SOLICITUD GUBERNAMENTAL PARA ACCEDER A LOS DATOS EN PODER DE OPERADORES MÓVILES

En la presente sección se presentarán los casos de Brasil, Colombia y Ecuador, en donde se habilitó a las compañías de telefonía móvil a compartir los datos de sus usuarios con instituciones gubernamentales y cómo fueron resueltas estas peticiones. No fue posible obtener información adicional sobre Argentina, Bolivia y El Salvador.



BRASIL

En el contexto de la pandemia, el gobierno emitió la Medida Provisoria 954, que pretendía que las operadoras telefónicas compartieran los nombres, números telefónicos y dirección de sus usuarios con el Instituto Brasileño de Geografía y Estadística (IBGE), debido a la imposibilidad que el instituto enfrentaba para realizar visitas domiciliarias que alimentarían la producción de estadísticas oficiales durante la emergencia. Esta medida fue suspendida por el Supremo Tribunal Federal, que consideró que la medida no definía cómo y para qué iban a ser usados los datos colectados, además de no especificar qué tipo de mecanismos técnicos se implementarían para evitar fugas accidentales o mal uso de los datos.

Sin embargo, algunas herramientas desarrolladas en estados y municipios de Brasil sí usaron datos de los operadores de telefonía para su funcionamiento. Estas fueron desarrolladas al amparo de la Ley 13.979, la cual obligaba a los organismos de la administración pública federal, estatal, distrital y municipal, a compartir entre sí, datos esenciales para la identificación de personas infectadas o sospechosas de tener una infección por coronavirus.

En ese escenario, la Prefectura de Río de Janeiro y la empresa TIM firmaron un acuerdo en el cual la empresa ofrecía los datos de conexión con las torres de telefonía, en tiempo real, con lo cual se podrían monitorear las aglomeraciones y los movimientos de la población. Con base en la concentración de usuarios en una localidad en un determinado momento, se generaba un "mapa de calor". Según la empresa, la información preservaría el anonimato de los clientes[58].

Por su parte, el Estado de Sao Paulo implementó el Sistema de Monitoreo Inteligente (SIMI), desarrollado en colaboración con las empresas de telefonía, Claro, Oi, TIM y Vivo. Este sistema también usaba los datos vinculados a las antenas de telefonía móvil de las operadoras para identificar aglomeraciones y para enviar mensajes con orientaciones a los usuarios. Según las autoridades del Estado, no existía riesgo a la privacidad de los usuarios, pues no se analizaba la trayectoria individual y además los datos eran anonimizados y presentados de manera agregada respectando las disposiciones de la LGPD.[59]

Con el fin de evitar la creación de nuevas plataformas para el mismo objetivo, las operadoras telefónicas Claro, Oi, TIM y Vivo crearon un servicio único para que los gobiernos estatales, municipales y federal pudieran monitorear aglomeraciones a través de mapas de calor generados con los datos de los celulares de los usuarios[60]. En el momento del anuncio, 15 estados y dos ciudades mostraron interés en el servicio. De acuerdo con el presidente de Sindicato Nacional de las Empresas de Telefonía y de Servicio Móvil Celular y Personal, no habría riesgo a la privacidad, en tanto los datos son anonimizados.

EL GOBIERNO CENTRAL TENÍA LA INTENCIÓN DE REALIZAR ESTE TIPO DE MONITOREO A ESCALA NACIONAL, PERO FINALMENTE DESISITIÓ[61]

En este contexto, la Agencia Nacional de Telecomunicaciones (ANATEL) se pronunció sobre estas soluciones, señalando que "…la adopción de cualquier medida de la naturaleza de las anteriores debe resultar de una decisión motivada, con respaldo legal y la debida transparencia para los órganos de control y para la sociedad".[62] En ese sentido, para la ANATEL, la colecta de datos debe estar sujeta a la legislación vigente y a los dictámenes de la Constitución Federal. La ponderación de la tutela de la salud

58 https://www.tim.com.br/sp/sobre-a-tim/sala-de-imprensa/press-releases/institucional/prefeitura-do-rio-fecha-parceria-com-a-tim-para-montar-mapa-de-deslocamento-na-cidade-durante-a-pandemia_
59 https://www.saopaulo.sp.gov.br/noticias-coronavirus/governo-de-sp-apresenta-sistema-de-monitoramento-inteligente-contra-coronavirus/
60 https://www.uol.com.br/tilt/noticias/redacao/2020/04/23/teles-criam-site-para-governos-monitorarem-isolamento-com-dados-de-celular.htm
61 https://www.uol.com.br/tilt/noticias/redacao/2020/04/13/bolsonaro-veta-uso-de-dados-de-celulares-para-monitorar-isolamento.htm
62 https://www.gov.br/anatel/pt-br/assuntos/noticias/posicionamento-da-anatel-a-respeito-da-utilizacao-de-rastreamento-de-usuarios-de-telecomunicacoes-no-ambito-de-medidas-no-combate-a-pandemia-de-covid-19

y la privacidad, aún en época de crisis, debe considerar la armonización entre ambos bienes jurídicos, de manera motivada y transparente; en el juicio de proporcionalidad deben valorarse otras opciones menos invasivas a la privacidad de las personas y el consentimiento debe ser abordado de alguna manera.

COLOMBIA

Durante los primeros días de la emergencia, la SIC emitió la Circular Externa 001,[63] la cual facultaba a los operadores de telefonía móvil y a las entidades privadas a suministrar al Departamento Nacional de Planeación (DNP) y "demás entidades públicas" los datos personales necesarios para atender, prevenir, tratar o controlar la propagación del coronavirus. Como sustento, la SIC hizo referencia a la excepción a la autorización previa e informada del titular para el tratamiento de los datos personales, contenida en la letra "c" del Art. 10 de la Ley Nº 1581 (casos de urgencia médica o sanitaria); además, basó su justificación en el Art. 13 de la referida Ley, por medio del cual los datos pueden ser entregados "b) A las entidades públicas o administrativas en ejercicio de sus funciones legales…"

> La Circular Externa 001 de la SIC de Colombia se trataba de un acto de autoridad que pretendía ir más allá de habilitaciones legales para impulsar la entrega de información de personas.

Sobre esta Circular, diversas organizaciones de la sociedad civil a nivel nacional e internacional alertaron sobre los peligros que el amplio alcance del documento podía generar[64], facilitando la entrega de información personal de manera desproporcionada a las necesidades surgidas del control de la pandemia. Así, por ejemplo, señalaron que **la información sobre localización, identificación y comunicación de los usuarios que estas empresas poseen, representa un riesgo de "…discriminación, de vigilancia indebida, de invasión de la privacidad y de protección de las fuentes periodísticas". Además, se señaló que la Circular no detalla los requisitos y condiciones legales que deben cumplir las entidades privadas para entregar datos personales y sensibles; tampoco señala el límite temporal para la entrega de la información o el tipo de datos que pueden ser requeridos, en el entendido que para la atención de la emergencia, no son necesarios todos los datos que recopilan estas empresas.**[65] En síntesis, se trata de un acto de autoridad que pretendía ir más

63 https://www.sic.gov.co/sites/default/files/normatividad/032020/Circular%20001.pdf.pdf
64 https://flip.org.co/index.php/es/informacion/pronunciamientos/item/2486-organizaciones-de-la-sociedad-civil-rechazan-circular-de-la-sic-sobre-uso-de-datos-personales-para-controlar-la-pandemia
65 Ídem.

allá de habilitaciones legales para impulsar la entrega de información de personas. No tenemos evidencia de que esa información haya sido entregada. No obstante, la medida por sí misma resulta un ejercicio que no puede considerarse sujeto a los principios de legalidad, necesidad o proporcionalidad para la restricción sobre la autodeterminación informativa.

Uno de los casos de colaboración entre gobierno, academia y empresas de telefonía fue el Sistema de Inteligencia de Epidemiologia del COVID-19 (SISCOVID)[66]. Este proyecto, financiado por el Ministerio de Ciencia Tecnología e Innovación, fue trabajado en conjunto entre investigadores de la Universidad de Los Andes, el Centro Nacional de Consultoría (CNC) y la Universidad de Ibagué, junto a empresas como Movistar, LUCA Data Unit, y Facebook Geoinsights quienes proveyeron datos agregados de la movilidad de los ciudadanos a partir del uso de teléfonos celulares.

El objetivo declarado del proyecto fue "...estudiar la dinámica del virus a través de modelos de simulación matemática y computacional apoyados por datos de movilidad (incluyendo datos MNO) y encuestas, para proporcionar evidencia para la toma de decisiones en cinco ciudades del país: Barranquilla, Bogotá, Cali, Cartagena y Medellín."[67] De acuerdo a un reporte de la Fundación Karisma "Cómo se utilizaron exactamente... los conocimientos ofrecidos por los grupos académicos por los gobiernos es menos claro."[68]

ECUADOR

En el marco de la pandemia, se declaró el estado de excepción por calamidad pública mediante Decreto Ejecutivo Nº 1017. En virtud de este decreto, se permitía "... usar plataformas satelitales y de telefonía móvil para monitorear la ubicación de personas en estado de cuarentena sanitaria y/o aislamiento obligatorio [...]" (Art. 11); es decir, que mediante el GPS del teléfono celular, el gobierno podía monitorear a aquellas personas con diagnóstico positivo del virus, quienes estuvieron en contacto con casos positivos o personas que ingresaron al país desde el extranjero, quienes debían cumplir el periodo obligatorio de 14 días de aislamiento.

Esta medida, en tanto permitía el acceso a información sensible de los ciudadanos, despertó cuestionamientos sobre su legalidad, necesidad y proporcionalidad y la afectación a los derechos humanos de las personas, como el derecho a la privacidad.

66 https://www.researchgate.net/publication/348950496_SISCOVID_modelos_de_sistemas_complejos_para_contribuir_a_disminuir_la_transmision_de_SARS-COV-2_en_contextos_urbanos_de_Colombia
67 https://descubre.movistar.co/informe-de-gestion-responsable-2020/gestion-2020-4-2.html
68 https://web.karisma.org.co/wp-content/uploads/2021/05/Useless-and-Dangerous-A-Critical-Exploration-of-Covid-Applications-and-Their-Human-Rights-Impacts-in-Colombia.pdf

En este contexto, la Corte Constitucional emitió un dictamen favorable a la medida, en términos generales. No obstante, la Corte sí tuvo pronunciamiento sobre el ámbito de aplicación. En el número 1 letras c) y d) del dictamen, respecto de las medidas tecnológicas permitidas en el Art. 11 del DE Nº 1017, la Corte señaló que estas medidas deberían ser usadas únicamente en el marco de actuación de la declaratoria de emergencia, señalando como limitante clara que no podrían ser usadas para menoscabar el derecho a la privacidad y a la no discriminación; recalcando, además, la obligatoriedad de la protección de los datos personales por parte del Estado. También manifestó que estas medidas sólo debían ser aplicadas a las personas a las que se les haya señalado cumplir aislamiento voluntario u otras medidas de similar naturaleza, quienes debían ser informadas sobre el posible uso de estas medidas y su alcance.[69] Desde la perspectiva del derecho internacional de los derechos humanos, esto plantea un par de consecuencias relevantes. Independientemente de habilitaciones o restricciones expresas a nivel de legislación, la utilización de esta clase de medidas puede ser eventualmente constitutiva de actos infractores de derechos fundamentales consagrados a nivel supralegal. Por la inversa, es un dictamen de carácter prospectivo, manteniéndose en general las limitaciones del sistema ecuatoriano para cuestionar la aplicación fuera del ámbito constitucional.

La utilización de esta clase de medidas puede ser eventualmente constitutiva de actos infractores de derechos fundamentales.

En este contexto, a inicios de abril del 2020, el gobierno presentó la plataforma ecuador.analiticacovid.com, en la cual, mediante la presentación de mapas de calor, entre otras funcionalidades, se pueden conocer los lugares con mayor concentración de personas. Estos mapas, de acuerdo con especialistas, son elaborados con datos provenientes de las empresas de telefonía celular, a través de la conexión del dispositivo con las antenas repetidoras de telefonía.[70] Si bien no es inédita esta forma de obtención y presentación de información sobre cúmulos de personas, **la ausencia de resguardos legales expresos en Ecuador plantea un factor de gran preocupación sobre el procesamiento de información de teléfonos móviles que puede representar información personal, inclusive de carácter sensible.**

69 http://doc.corteconstitucional.gob.ec:8080/alfresco/d/d/workspace/SpacesStore/0753708f-17ba-4a7b-a818-d93769a77b3a/Dictamen_1-20-EE-20_(0001-20-EE).pdf

70 https://www.planv.com.ec/historias/sociedad/asi-funcionan-monitoreos-celulares-que-el-gobierno-usa-vigilar-la-epidemia

3. DISCUSIÓN

Tomando como base la opinión de los expertos en derechos humanos de la Organización de la Naciones Unidas (ONU) emitida en marzo de 2020[71] a propósito de la respuesta de los Estados a la emergencia sanitaria, que instaba a recordar "...urgentemente a los Estados que cualquier respuesta de emergencia al coronavirus debe ser proporcionada, necesaria y no discriminatoria", serán analizadas las particularidades de la respuesta que los países seleccionados para este estudio generaron, con la finalidad de comprender el grado de adecuación a tales exigencias. Desde esa perspectiva, siguiendo de cerca el lenguaje de la ONU, la recomendación apunta a medidas que por naturaleza resultan restrictivas del ejercicio de derechos fundamentales, con el propósito de resguardo de la salud pública.

Sin embargo, como puede observarse, no todos los países abordaron de manera similar el combate a la pandemia mediante el uso de tecnologías, ni dieron de forma clara prioridad a un análisis o una evaluación de legalidad, necesidad, proporcionalidad y no discriminación. De todos los países, El Salvador no desarrolló ninguna aplicación, ni solicitó, hasta donde sabemos, datos en poder de las operadoras telefónicas para alimentar alguna estrategia de seguimiento de contagios. Su único auxilio fue un *chatbot* que presentaba las opciones de auto evaluación y de información sobre el virus. Y, aunque esta medida pueda representar un riesgo, debido a los metadatos de los teléfonos en los que el *chatbot* era utilizado y porque además se compartían datos sensibles, la ausencia de respuesta a solicitudes de información realizadas, impide conocer más detalles sobre esta herramienta que fue desactualizada en agosto de 2020.

No todos los países abordaron de manera similar el combate a la pandemia mediante el uso de tecnologías, ni dieron de forma clara prioridad a un análisis o una evaluación de legalidad, necesidad, proporcionalidad y no discriminación.

También es necesario apuntar que, para poder realizar una ponderación más adecuada de la respuesta de los Estados en Latinoamérica, debe hacerse referencia a las condiciones sociales y económicas de la región.

71 https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=25722&LangID=E

Esto es así en el caso de las medidas en las que era necesario un alto grado de implicación de la población, como las aplicaciones de rastreo. Por un lado, hay que entender que en la mayoría de los países de la región, una buena parte de su población no tiene acceso a una estructura digital confiable, a pesar de los esfuerzos de los gobiernos por llevar este servicio a toda la población. Manifestaciones de esta desigualdad fueron evidentes al implementarse las clases a distancia, las cuales requerían que los alumnos tuvieran acceso a internet y a dispositivos informáticos para tomar las clases.

Para el caso, el acceso a internet en los países estudiados es disímil y en algunos casos, aún es bajo. En Argentina, por ejemplo, del total de la población, el 82.9% cuenta con acceso a internet; mientras que, en Bolivia, es el 44.2% el porcentaje de la población con acceso a internet. Por su parte, Brasil tiene un porcentaje de 79%, mientras que en Colombia, Ecuador y El Salvador, el porcentaje es de 64.6%, 59.2% y 59%, respectivamente.[72]

No obstante, en este contexto de emergencia, hubo esfuerzos por parte de los operadores de telefonía por ayudar a superar los desafíos de conectividad, mediante distintas actividades como el incremento de la velocidad de internet sin costo para los usuarios y las alianzas con Ministerios de Educación de algunos países para la implementación de plataformas educativas.[73] La eficacia de tales actividades deberá ser evaluada en un futuro.

Respecto del criterio de finalidad, existe un dilema que debe ser abordado inmediatamente. Es cierto que las aplicaciones estudiadas hacen alusión (unas mejor que otras) a la finalidad para la cual se solicita a una persona que otorgue sus datos personales. Esto estaría bien si sólo se evaluara si la aplicación cumple con ese requisito y si, además, todas las aplicaciones pidieran los datos estrictamente necesarios para esa finalidad. Sin embargo, la aplicación por sí sola no resuelve el problema del avance del virus; más bien, es una herramienta; y, como tal, debería ser parte de una estrategia de salud más amplia. En este sentido, una de las principales críticas a estas aplicaciones es que no se explica a la población cómo esta herramienta forma parte de una estrategia de combate más amplia. Esto podría limitar que más gente se comprometa con la medida; ya que entre más información tenga la población, mayor seguridad tendrá del por qué está cediendo sus datos.

Otro aspecto sobre la finalidad, ligado a lo explicado anteriormente, se refiere a la proliferación excesiva de aplicaciones, que muchas veces ofrecen finalidades que se

72 https://covid.alsur.lat/es/
73 https://www.thedialogue.org/blogs/2020/07/desafios-de-conectividad/?lang=es

solapan, lo que vuelve aún más confuso determinar qué es lo que exactamente se está persiguiendo con esas herramientas. No puede asegurarse con total certeza que esta proliferación desmedida de aplicaciones tenga relación causal con la ausencia de una ley específica de protección de datos personales; para el caso del presente estudio, de los países analizados puede observarse que este fenómeno ocurrió, tanto en Argentina y Brasil, que son países que sí cuentan con esta normativa, como en Bolivia, país que no cuenta con una ley en la materia.

Respecto de la proporcionalidad, habría que señalar que, más allá de los problemas de excesiva recopilación de datos que fueran reportados en algunas aplicaciones en sus estadios iniciales, habría que plantearse seriamente el escenario en el cual las operadoras de telefonía comparten los datos de sus usuarios con los gobiernos.

En el momento en el que un gobierno hace partícipe a una compañía privada de telefonía de la estrategia de monitoreo de personas infectadas, expone los datos sensibles de salud de esas personas.

Esto no sólo tiene que ver con el asunto de los riesgos de que esta vigilancia exceda los fines epidemiológicos. El problema añadido es que, en el momento en el que un gobierno hace partícipe a una compañía privada de telefonía de la estrategia de monitoreo de personas infectadas, expone los datos sensibles de salud de esas personas. Aunque las compañías tengan sus propias políticas de privacidad y los datos que entregan a los gobiernos deberían ser anonimizados, no hay que olvidar que estas empresas conocen la identidad de sus usuarios, por lo que pueden perfectamente asociar un dato sensible (contagio por el virus) a los datos que previamente han recolectado.

Sería una forma de exponer datos de manera involuntaria, si se quiere, pero precisamente este tipo de riesgos debe obligar a los Estados a evaluar previamente si la medida que proponen es necesaria y proporcional; si el objetivo que se persigue puede ser alcanzado mediante otro procedimiento menos intrusivo; y, si esta medida conserva el equilibrio entre el derecho a la salud y el derecho a la privacidad de las personas.

Siempre referido al requerimiento de datos personales en poder de las operadoras telefónicas por parte de los gobiernos, no hay que olvidar algunos aspectos que deben ser ampliamente considerados. Por un lado, aunque el aspecto de la anonimización en un proceso exitoso, la posibilidad de re identificar a una persona es muy complicado, hay que señalar que no basta con borrar nombres o números telefónicos, como muchas veces es interpretado por algunos funcionarios. El uso de otras fuentes de datos para

triangular la información personal de una persona y así lograr la desanonimización, es plausible. Por ello, los encargados de la ciberseguridad en las instituciones públicas y privadas deben ser muy cuidadosas a la hora de realizar este proceso.

Por otro lado, este tipo de colaboraciones debe ser transparente con el público. Se debe tener acceso a los convenios que los Estados firman con las compañías. No existe justificación suficiente a la luz del derecho internacional de los derechos humanos, ni como restricción al derecho de acceso a la información consagrado en la Convención Americana sobre Derechos Humanos, para mantener esta clase de acuerdos fuera del conocimiento público.

En sistemas de vigilancia más complejos, la transparencia debe ser una de las más importantes condiciones a cumplir desde la perspectiva del derecho de acceso a la información. En estos casos, debe ponerse a disposición del público la suficiente cantidad de información que permita un correcto entendimiento de la arquitectura de vigilancia.

En este apartado no puede dejar de mencionarse algunas observaciones referentes a las aplicaciones y sistemas informáticos creados por los Estados. En primer lugar, se debe señalar la arriesgada apuesta de países como Bolivia y Ecuador que, sin tener una Ley de Protección de Datos Personales, crearon aplicaciones y sistemas de monitoreo de movilización de la población que necesitan de entramados jurídicos sólidos para garantizar la privacidad y la protección de los datos personales y datos sensibles de las personas, no sólo en su aspecto correctivo, sino en el preventivo. En estos casos, el marco del derecho internacional de los derechos humanos cobra un valor adicional, como ámbito de protección de los derechos fundamentales operativizados en otros países a través de la ley. Es decir, las preocupaciones sobre la información personal y sobre la dignidad de las personas se vinculan directamente a su consagración como derechos fundamentales en la conjunción entre protección constitucional y reconocimiento por tratados internacionales ratificados por cada país.

Lo señalado anteriormente no implica señalar que en los países con Leyes específicas para la protección de los datos personales, la tutela efectiva del derecho a la autodeterminación informativa esté asegurada y que todos los actores del entramado digital en la sociedad cumplan a cabalidad esa normativa. Basta poner atención a las evaluaciones que realizan distintas organizaciones de defensa de los derechos humanos en el ámbito digital, principalmente en Argentina, Brasil y Colombia, para corroborar que el problema no estriba en que un país tenga o no una Ley sobre el tema; sino, sobre las facultades contraloras y sancionatorias que pueda tener la autoridad encargada para la protección de los datos personales, así como el grado de interiorización sobre la importancia de esta protección que la sociedad en general alcance.

Otro problema que fue reportado en el diseño de estas aplicaciones fue su escasa seguridad, por lo menos en sus versiones iniciales. Como puede constatarse en el presente informe, organizaciones de la sociedad civil que trabajan en la protección de los derechos humanos en el ambiente digital reportaron vulnerabilidades en las aplicaciones, con la potencialidad de exponer datos personales de buena parte de la población. En alguna medida, la urgencia de las medidas de sanidad pública parecía justificar despliegues rápidos de mecanismos de auxilio. Sin embargo, el riesgo representado para la información personal por la carencia de condiciones razonables de seguridad representa a la vez un abandono del principio de seguridad en la protección de datos personales, que pone en riesgo información sensible que puede afectar desde la dignidad hasta el trato en condiciones de no discriminación de las personas.

La urgencia parecía justificar despliegues rápidos de mecanismos de auxilio. Sin embargo, la carencia de condiciones razonables de seguridad representa un abandono del principio de seguridad en la protección de datos personales.

Esto debe servir para que los Estados no dejen que la urgencia de respuestas provoque una reacción apresurada. Cada Estado debería evaluar si la implementación de ciertas tecnologías es necesaria e idónea; si se tiene la suficiente capacidad para mantener el equilibrio entre la salud y la privacidad; y, si se tiene suficiente evidencia sobre la eficacia de la herramienta propuesta respecto del fin que se pretende alcanzar. En otras palabras, el desarrollo y el despliegue de tecnologías deben pasar por un análisis previo, acorde con el impacto en las personas que la operación correcta y la operación incorrecta del sistema pueden tener. Se trata de un análisis de adecuación, como parte del cumplimiento del estándar de necesidad y el de proporcionalidad, exigidos dentro de la pandemia por los organismos internacionales, y fuera de la pandemia por la vigencia habitual de los instrumentos sobre derechos humanos.

También fueron identificados problemas referentes al consentimiento que debía ser solicitado para la colecta de datos personales. Los casos de Argentina y Colombia en el que existieron declaraciones y disposiciones contradictorias en las que, por un lado se obligaba a usar la aplicación en ciertas circunstancias, pero se señalaba que no era obligación descargarla, deben poner en perspectiva la necesidad de guiarse por las exigencias de protección de los derechos humanos desde el diseño de estas herramientas; sobre todo, porque el consentimiento para el tratamiento de datos personales sensibles es obligatorio en la mayoría de legislaciones en la materia.

Asimismo, de las aplicaciones estudiadas no hay una certeza sobre cuánto tiempo las bases de datos serán conservadas; o si los datos serán destruidos después de la emergencia; o, si estos datos no serán usados posteriormente para fines distintos del monitoreo epidemiológico. Aunque los términos de uso de las aplicaciones hacen referencia a las Leyes que protegen los datos personales en los respectivos países, no hay que perder de vista que, por tratarse de una categoría de datos que requiere protección especial, las cláusulas referidas al tratamiento de datos sensibles deberían ser lo más específicas posibles en cuanto al aseguramiento del respeto a la privacidad de los usuarios antes, durante y después de la emergencia.

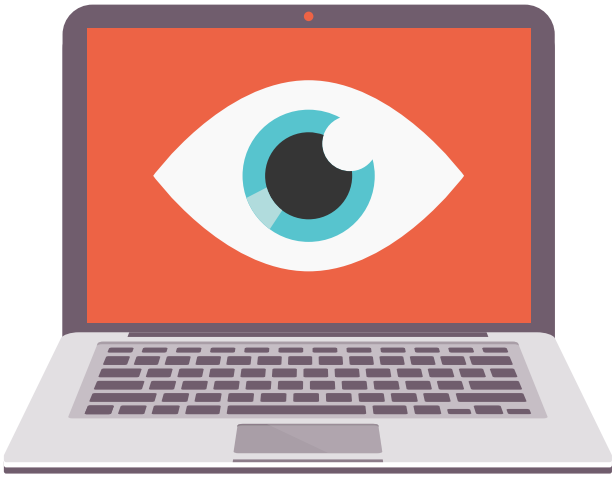
4. CONCLUSIONES Y RECOMENDACIONES

La emergencia por el coronavirus puso a prueba a los sistemas de salud de todo el mundo y ha tenido repercusiones en todos los ámbitos de nuestra vida. Para afrontar los embates de la pandemia, los gobiernos de la mayoría de los países en el mundo implementaron medidas tecnológicas en el afán de contrarrestar los contagios y América Latina no fue la excepción.

De las respuestas tecnológicas estudiadas salen a la luz algunos problemas que deben ser revisados, si las futuras estrategias de salud echarán mano, nuevamente, de ellas:

- Problemas de seguridad y riesgos a la privacidad en el diseño de aplicaciones; idoneidad frente a la realidad socioeconómica de los países de la región;
- problemas de apego irrestricto a la normativa de protección de datos personales y ausencia de normas especializadas en algunos países;
- limitada transparencia respecto del desarrollo y la implementación de las soluciones tecnológicas, así como en los convenios firmados entre empresas privadas y administración pública; y
- falta de coherencia en el uso de aplicaciones con una estrategia general de salud

Estas son algunas de las falencias que se han podido constatar a través de la función de contraloría que ejercen numerosas organizaciones en la región.



Queda claro que el derecho a la privacidad no es absoluto y que, en el marco de la emergencia, algunas intrusiones a este derecho, cuando está en juego la salud de la población, son tolerables. Sin embargo, eso no quiere decir que estas intromisiones deban socavar la privacidad y el derecho de autodeterminación informativa

de las personas. Para ello, es necesario que cualquier respuesta en el combate a la pandemia y a cualquier futura emergencia, sea adecuada, proporcional, con una finalidad clara, delimitada en el tiempo, consentida y necesaria. Aunque parezca evidente, debe también contar con habilitaciones legales suficientes, respeto al principio de legalidad. En tal sentido, serán expuestas algunas recomendaciones generales para abordar el uso de tecnologías desde las buenas prácticas:

1. Toda medida de emergencia por parte de autoridades estatales, incluyendo las que integren componentes tecnológicos, debe estar provista de mecanismos de análisis previo y evaluación posterior de impacto en derechos fundamentales.
2. Toda medida de autoridad debe estar expresamente sustentada en las disposiciones constitucionales y legales que las autorizan y justifican, así como deben hacer expresa mención de sus propios límites;
    - Para una mejor solución, los gobiernos deberían consultar con las autoridades encargadas de proteger los datos personales de cada país, previo a la implementación de cualquier tecnología que pueda infringir los principios de privacidad y protección de datos, para mantener el balance entre las intromisiones a la privacidad y el respeto a los derechos humanos.
3. Los convenios firmados entre empresas privadas e instituciones gubernamentales deben ser de carácter público, tanto vía transparencia activa como mediante el ejercicio del derecho de acceso a la información, para que las personas conozcan con detalle el tipo de información que está siendo recolectada, para qué está siendo recolectada, en qué le beneficia que la información esté siendo recopilada y con quién se está compartiendo, así como también para permitir mecanismos de reclamación.
    - Fomentar la participación de amplios sectores de la sociedad, con diversos intereses, en las discusiones sobre el procesamiento de datos, así como garantizar mecanismos de seguimiento y evaluación, que permitan conocer si se han cumplido los propósitos de interés público o si existe algún impacto negativo derivado del uso de estas tecnologías y de la colecta y tratamiento de los datos.
4. Todo desarrollo tecnológico y toda adquisición de tecnología debe poner a disposición el código fuente de las aplicaciones, de tal forma que se permita la auditoría externa, se sepa con claridad el funcionamiento de la herramienta, y se puedan identificar y reparar vulnerabilidades.
5. Sin perjuicio de las medidas sanitarias aplicables a la totalidad de la población, por regla general las aplicaciones tecnológicas deben ser de utilización voluntaria.
6. Cualquier análisis debe considerar, antes de implementar una solución tecnológica, el contexto socioeconómico en el que va a desplegarse, a fin de evitar discriminación en sectores de la población.

7. Toda medida que involucre la recolección de información de las personas, incluyendo a las que hacen uso de tecnologías de comunicación, debe estar ceñida exclusivamente a los propósitos de combate a la pandemia e integrarse en una estrategia clara de salud.
8. Toda política estatal en contexto de emergencia sanitaria debe mantener compromisos explícitos de tratamiento de información personal, incluyendo mediante la publicación de políticas de privacidad y tratamiento de datos personales en el caso de medidas tecnológicas, con pleno respeto a los principios de protección de datos personales independientemente de la existencia de leyes generales de protección en cada país.
9. Toda política estatal en contexto de emergencia, incluidos sus componentes tecnológicos, deben fijar de forma clara y específica sus propios términos de finalización de su recolección y mantenimiento de información de las personas, así como el destino de los datos una vez la emergencia haya finalizado.
10. Toda herramienta tecnológica creada para hacer frente a una emergencia debería cumplir con el requisito de privacidad desde el diseño.

Las recomendaciones contenidas en los numerales vii, viii y ix adquieren una mayor importancia para países con situaciones sociopolíticas convulsas en desarrollo, como Colombia y El Salvador, por el riesgo que representa la recolección desproporcionada de datos personales en un contexto en el que los datos recolectados pueden servir para la persecución de rivales políticos, defensores de derechos humanos o para mantener el control de la libertad de expresión de la población en general.

Finalmente, sería de mucho provecho la realización de un meta análisis sobre del uso de tecnologías como parte de las herramientas de combate a la epidemia de la COVID-19 desde una perspectiva de derechos humanos. En segundo lugar, sería conveniente realizar un estudio que provea evidencia robusta sobre la diferencia, si existió, en los impactos de la recolección de datos personales en países con leyes específicas de protección de datos personales y en aquellos donde no existe esta legislación. En tercer lugar, sería provechoso un abordaje multidisciplinario en el que pueda ser evaluada la eficacia de estas herramientas como medida para detener el avance de la enfermedad y luego sea ponderada con mayor certeza la intrusión a la privacidad que estas herramientas generan.

En la medida en que más estudios se desarrollen sobre esta temática, mejor información generará y mejores recomendaciones podrán ser elevadas a las autoridades y a los encargados de las políticas públicas en América Latina.

ANEXO I. LISTA DE LAS PRINCIPALES APLICACIONES UTILIZADAS EN EL CONTEXTO DE LA COVID-19

Nombre de la Aplicación	Novedad de la Aplicación	Instrumento jurídico base	Descripción	Principales objeciones
Argentina				
Cuidar App	La aplicación fue creada para la emergencia por COVID-19.	Decisión Administrativa 432 / 2020, de 24 de marzo de 2020.	Creada con el fin de servir para el autodiagnóstico de síntomas compatibles con Covid-19 y brindar información de salud a la población, además de servir para portar el certificado habilitante de circulación.	Críticas a la versión para Android incluyen: 1) solicitud de una gran cantidad de permisos para el teléfono, como por ejemplo: acceso a la geolocalización (aproximada y precisa), calendario, contactos, micrófono, cámara, acceso completo a la red con la capacidad de ver las conexiones de red, configuración de audio, inicio cuando se enciende el dispositivo y prevenir que el teléfono se duerma. 2) Se reportó una vulnerabilidad en la generación del token de validación de un solo uso asociado al dispositivo.
Bolivia				
Bolivia Segura	La aplicación fue creada para la emergencia por COVID-19.	Ley para la prevención, contención y tratamiento de la infección por el coronavirus. Ley Nro. 1.293 de 01 de abril de 2020.	La aplicación oficial del Gobierno para brindar información, estadísticas de la evolución de la pandemia y ser una herramienta de autoevaluación de salud en línea.	1) permitía el acceso a los datos por parte de terceros para fines lícitos, sin detallar quiénes podían ser esos terceros y qué se entendería por “fines lícitos”; 2) la ausencia de medidas de seguridad para la protección de los datos personales; 3) la ausencia de un proceso para acceder a los datos que el usuario ingresa; y, 4) la interoperabilidad con otras instituciones como el SEGIP y el Ministerio de Salud, sin contar con una Ley de Protección de Datos Personales que garantice el uso adecuado de los datos y los mecanismos de seguridad apropiados.
Brasil				
Coronavirus-SUS	La aplicación fue creada para la emergencia por COVID-19.	Ley Nro. 13.979 de 06 de febrero de 2020.	Originalmente tenía funciones informativas. Luego incorporó funciones de trazabilidad de contactos.	1) falta de certeza sobre la no recopilación de datos personales que la política de privacidad indica; 2) falta de claridad sobre el papel que desempeña Amazon Web Services, con quien comparte datos; 3) parte de la información no es encriptada.

Colombia				
CoronApp	Aplicación construida sobre la base del código fuente de una aplicación ya existente desde el año 2017.	Decreto 417 de 17 de marzo de 2020.	Una herramienta para informar a las personas sobre el Covid-19 en Colombia, permitir el auto-reporte de síntomas, generar un pasaporte de movilidad y realizar la trazabilidad de contactos.	1) falta de información sobre cómo se gestiona la seguridad y privacidad de los datos; 2) falta de certeza sobre la temporalidad del tratamiento y sobre lo que ocurrirá con los datos una vez finalizada la emergencia; 3) referencias muy generales al cumplimiento de las obligaciones legales para la protección de datos en los términos de uso; 4) el protocolo usado, aunque parecía centralizado, no atacaba el problema de privacidad, pues los identificadores de los dispositivos cercanos al usuario, que se guardaban en una base local en el aparato, eran generados por un servidor que podía desanonimizar los identificadores, volviendo identificable al usuario.
Ecuador				
Ecuador ASI	La aplicación fue creada para la emergencia por COVID-19	Decreto Ejecutivo 1.017 de 16 de marzo de 2020.	Una herramienta para notificación de contactos por proximidad física, a través de la tecnología *bluetooth*.	1) no hay suficiente información sobre qué datos serán usados, por quién y en qué condiciones; 2) no hay suficiente información sobre las medidas de seguridad; 3) se envían mensajes de emergencia del Servicio Nacional de Gestión de Riesgos y Emergencias (SNGRE) sin el consentimiento del usuario.
El Salvador				
No desarrolló aplicación. Únicamente un chat bot llamado SIVI.				