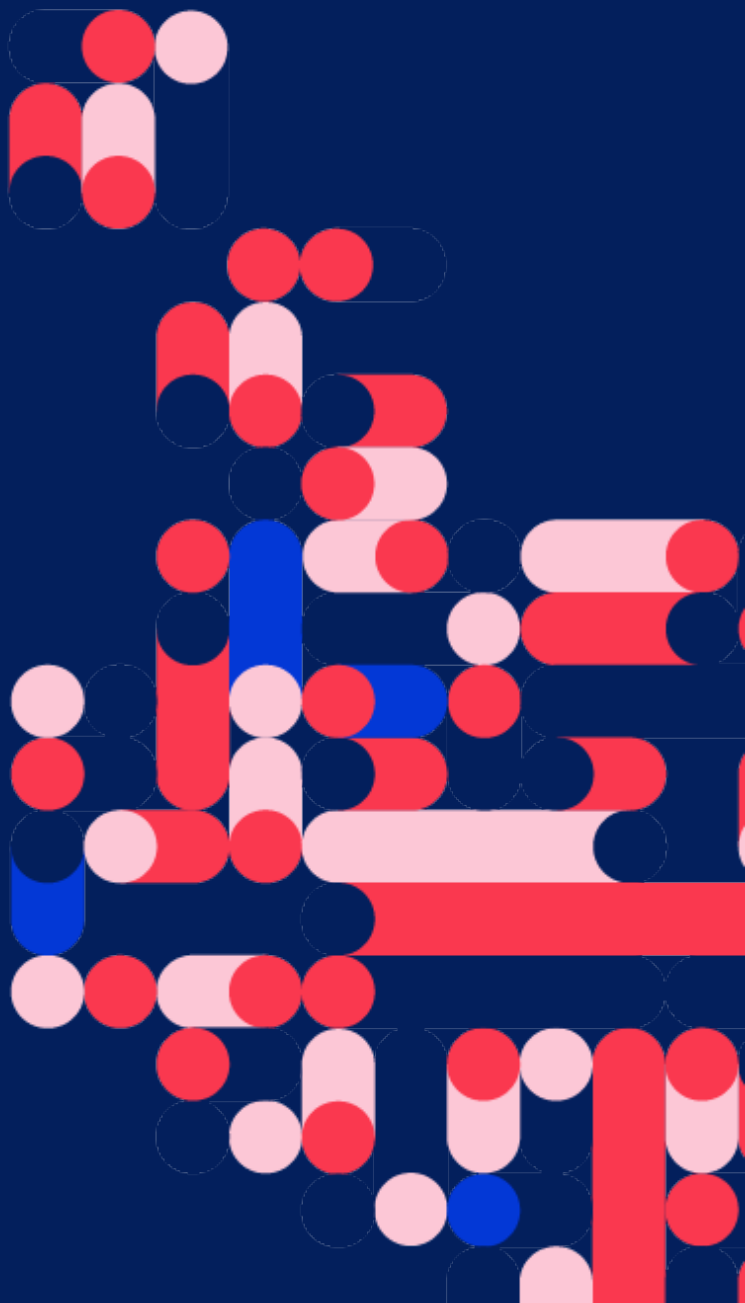
Informe Observatorio Covid-19 del Consorcio AI Sur:

Un análisis crítico de las tecnologías desplegadas en América Latina contra la pandemia



AlSur

AlSur

Observatorio de tecnologías de vigilancia y pandemia

Al Sur es un consorcio de organizaciones que trabajan en la sociedad civil y en el ámbito académico en América Latina y que buscan con su trabajo conjunto fortalecer los derechos humanos en el entorno digital de la región. Para más información sobre Al Sur y sus miembros, visite https://www.alsur.lat/

Informe Observatorio Covid-19 del Consorcio Al Sur: Un análisis crítico de las tecnologías desplegadas en América Latina contra la pandemia

Junio, 2021.

Autores: Jamila Venturini & Maria Paz Canales (Derechos Digitales), Morena Schatzky & Agustina del Campo, Centro de Estudios en Libertad de Expresión y Acceso a la Información (CELE), Olga Lucía Camacho, Carolina Botero (Fundación Karisma) y Bárbara Simão (InternetLab).

Diagramación: Lorena Marks

Agradecemos las revisiones de la Asociación por los Derechos Civiles (ADC) y de la Red en Defensa de los Derechos Digitales (R3D).

Índice

Resumen Ejecutivo

Las respuestas gubernamentales frente al SARS-Cov 2 varían significativamente de un país a otro, y como cualquier política pública, su intención depende mucho de la coyuntura política y social local. Para dar cuenta de ello, el Observatorio Covid-19 del Consorcio Al Sur (OCCA) recoge y estandariza la información disponible para facilitar la comparación de las respuestas tecnológicas implementadas en América Latina.

El presente reporte presenta un análisis cualitativo en base a los hallazgos del relevamiento de información llevado a cabo en 14 países durante la primera etapa de desarrollo del proyecto, que se extendió durante la segunda mitad de 2020 e inicios de 2021. Nuestro objetivo es que este reporte permita abrir la conversación desde la sociedad civil, la academia y los Estados acerca de la implementación de soluciones tecnológicas como parte de las políticas públicas y prácticas estatales en contexto de pandemia.

En la última parte de este informe se avanza hacia las consideraciones normativas de las iniciativas cuya información se ha relevado, sometiéndolas a análisis desde la perspectiva de la normativa local vigente (o la ausencia de ella) así como el marco institucional en que ellas se han insertado.

El reporte cierra con una perspectiva regional que reflexiona en torno a los hallazgos acerca de las soluciones tecnológicas investigadas evaluadas desde el punto de vista de los estándares propuestos por el sistema interamericano de derechos humanos, con particular consideración a los principios de legalidad, necesidad y proporcionalidad.

La pandemia ha reforzado la ubicuidad de la tecnología en nuestras vidas, no solo para su contención, sino en todo aspecto. Es por ello una excelente oportunidad para sentar principios y procedimientos robustos, respetuosos de estándares internacionales de derechos humanos, acerca de cómo la tecnología debe ser presentada y comunicada por los Estados a la ciudadanía como parte de las políticas públicas, de forma tal que le permitan reclamar y mantener el control individual y colectivo del uso de sus datos en función de objetivos de política pública enunciados en su nombre.

Las conclusiones ofrecidas por este informe proponen un punto de partida para explorar oportunidades de mejora en el diseño e implementación de tecnologías en el contexto de pandemia. Además, propone reflexionar sobre el futuro del rol de la tecnología en el control social y el desarrollo de relaciones entre los Estados y la ciudadanía en nuestra región.

En ese sentido, proponemos explorar los siguientes puntos críticos que deberían ser tomados en cuenta en las políticas públicas de la región que consideren el despliegue de tecnología:

- Atención reforzada a los niveles de conectividad;
- Evaluaciones de impacto en derechos humanos para garantizar toma de decisiones responsables por gobiernos y empresas;
- Gobernanza de datos bien definida; y
- Transparencia hacia la ciudadanía en selección y despliegue de la tecnología.

Introducción

Desde que la Organización Mundial de la Salud (OMS) declaró la pandemia de la Covid-19 el 11 de marzo de 2020, e hizo un llamado enfático al desarrollo de capacidad de respuesta y prevención en todo el mundo[1], muchos actores gubernamentales y no gubernamentales han intentado aprovechar el uso de la tecnología para combatir la propagación del virus. A tales fines, se han desplegado herramientas para hacer entrega de información confiable a la población; hacer uso de información en tiempo real de la evolución de casos y movilidad para el diseño de políticas para contener la expansión del virus; mejorar las capacidades de seguimiento epidemiológico existentes; y monitorear el cumplimiento de cuarentenas[2].

Lo que tienen en común todos los despliegues tecnológicos que se han intentado es que se encuentran basados en un uso intensivo de datos. La motivación del despliegue tecnológico como parte del ejercicio de contención de la pandemia exacerba una tendencia que ya venía registrándose en América Latina con anterioridad respecto del uso creciente de tecnología para la digitalización de la acción del Estado y servicios prestados por privados.

En este contexto, el diseño de tecnologías que se integren a la estrategia de freno de la pandemia pasa por el acceso a datos, ya sea a través de la recolección directa desde la ciudadanía, o a través del acceso a datos previamente disponibles en manos de actores públicos y privados, recopilados con anterioridad para propósitos diferentes. Ambas alternativas presentan oportunidades y riesgos, que se avienen a distintas estructuras de gobernanza para gestionarlos de manera tal que permitan la satisfacción de su propósito -freno a la expansión de la pandemia-, pero a la vez prevengan impactos negativos en el ejercicio de derechos de la ciudadanía.

El atractivo de los datos -ya sea en manos privadas o públicas, o recolectados directamente de los ciudadanos con ocasión de la pandemia- es indudable para los gobiernos que buscan hacer su acción más efectiva. Sin embargo, aún en el contexto de la pandemia, su tratamiento por parte de actores estatales y privados debe manejarse con estrictos compromisos de derechos humanos para asegurar que persiga un propósito legítimo e impedir usos alejados de esos objetivos durante, y luego de terminada la emergencia sanitaria.

---

1 OMS, *"Cronología de la respuesta de la OMS a la COVID-19"*, 29 de septiembre, 2020, disponible en: <https://www.who.int/es/news/item/29-06-2020-covidtimeline>

2 Acerca del rol de la tecnología que se ha desarrollado en el contexto de pandemia y sus impactos en el ejercicio de derechos ver Canales, Maria Paz. "La herejía tecno-optimista florece en pandemia Un repaso crítico a las tecnologías disponibles", Derechos Digitales, Junio 2020, disponible en: <https://www.derechosdigitales.org/wp-content/uploads/herejia-tecno-optimista.pdf>

Algunas de las tecnologías desplegadas en nuestra región fueron rápidamente implementadas por parte de iniciativas públicas, privadas o una combinación de ambas; otras se han basado en la reorientación del propósito de tecnologías previamente existentes, o la expansión de éstas a nuevos usos en los sectores de la salud o la seguridad social[3]. El sentido de urgencia para su implementación, que ha sido acompañado en nuestra región por la declaratoria de estados de emergencia constitucional, plantea importantes preguntas acerca de cuáles son los marcos de gobernanza adecuados, así como las evaluaciones de contexto e impacto previo a las que deben ser sometidas estas tecnologías a lo largo de su implementación durante la emergencia. También plantean interrogantes en torno a su efectividad y qué sucederá con ellas al finalizar la emergencia.

América Latina cuenta con un contexto que se manifiesta particularmente relevante durante la pandemia de Covid-19, y esto es debido a la carencia o insuficiencia de marcos normativos e institucionales para la adecuada protección de los datos personales, materia prima de la tecnología en despliegue. Se han desarrollado esfuerzos desde el Banco Interamericano de Desarrollo (BID) para acompañar el diseño e implementación de tales soluciones y abordar algunas de las cuestiones referidas a su gobernanza, incluyendo iniciativas de acompañamiento para evaluación externa de acuerdo con estándares internacionales[4]. Tales esfuerzos resultan relevantes ante la ausencia de contextos regulatorios claros y completos en materia de manejo de datos a través de la región.

A lo anterior se suma la falta de transparencia en el que se han adoptado muchas de las políticas y medidas que incorporan el uso de tecnologías en la región en el contexto de emergencia sanitaria (y constitucional en la mayoría de los casos). Esta realidad ha sido la fuente de motivación de la creación del Observatorio Covid-19 del Consorcio Al Sur (OCCA)[5], que se planteó como desafío recolectar información relevante de la caracterización de las tecnologías desplegadas con la finalidad de identificar estas medidas y crear un repositorio público y abierto que permita unificar el acceso a fichas descriptivas de las diferentes iniciativas tecnológicas implementadas en la región dentro de la estrategia de combate a la pandemia. Creemos que hacer disponible esta información permitirá con posterioridad realizar un análisis pormenorizado de las tecnologías descritas y facilitar el

3 Ver Aguerre, Carolina. "*La delgada y móvil frontera de las Corona-Apps en América Latina*", Análisis Carolina 30/2020, 19 de mayo de 2020, disponible en: <https://www.fundacioncarolina.es/wp-content/uploads/2020/05/AC-30.-2020.pdf>
Ver Venturini, Jamila et al. "Tecnologias e Covid-19 no Brasil: vigilância e desigualdade social na periferia do capitalismo", 2020, disponible en: <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>

4 Ramirez Rufino, Smeldy et al. "*COVID-19 y el uso responsable de datos: Análisis de iniciativas apoyadas por BID Lab*", BID, Noviembre 2020, disponible en: <https://publications.iadb.org/es/covid-19-y-el-uso-responsable-de-datos-analisis-de-iniciativas-apoyadas-por-bid-lab>

5 Ver <https://covid.alsur.lat/es/>

desarrollo de estudios comparados por parte de activistas, académicas, medios de prensa, organizaciones de la sociedad civil y organismos internacionales, entre otros actores.

Así la estructura del presente informe es la siguiente, luego de esta introducción (I), se describe la metodología desarrollada para el levantamiento del OCCA y su informe final (II); enseguida se introduce una referencia al marco normativo vigente desde una perspectiva de instrumentos internacionales de derechos humanos a los cuales la mayor parte de países estudiados se han obligado, y las guías y estándares específicamente emanadas de órganos internacionales, particularmente del Sistema Interamericano de Derechos Humanos, ya sea generales o específicamente desarrollados durante la pandemia para orientar las medidas estatales, que serán utilizados como marco del análisis normativo a lo largo del informe (III); a continuación se avanza en la descripción factual de las tecnologías estudiadas para relevar algunas tendencias regionales, indicadores críticos para su funcionalidad y aspectos de transparencia evaluados en ellas (IV); la sección siguiente aborda un análisis del marco legal de implementación de las tecnologías estudiadas desde la perspectiva de la normativa de protección de datos personales y de acceso a la información vigente a nivel nacional durante el contexto de pandemia (V). La última sección tiene por objeto preciso entregar una evaluación inicial del desempeño de los marcos normativos en los cuales tuvieron lugar las implementaciones tecnológicas estudiadas, de cara a las guías y estándares provistos por el sistema interamericano de derechos humanos en relación a los principios de legalidad, necesidad y proporcionalidad en la afectación del ejercicio de derechos (VI); para cerrar con nuestras conclusiones que invitan a futura reflexión más allá del contexto de pandemia (VII).

Metodología

La metodología del OCCA está basada en 18 conceptos centrales que dieron origen a un conjunto de atributos e indicadores. Estos posibilitan la comparación y determinación de tendencias entre las tecnologías intensivas en el uso de datos desarrolladas en los países de América Latina durante la pandemia. La adopción de una metodología estandarizada por medio de una ficha común de análisis tuvo como objetivos facilitar el levantamiento de información, así como la comparación entre las iniciativas y permitir la visualización de las características principales de cada una. Además, para algunos de los indicadores se ofrecieron definiciones adicionales que permitieran armonizar la interpretación de elementos como el concepto de consentimiento expreso, libre e informado; los derechos involucrados en el control efectivo de los usos de datos personales por parte de las titulares y la naturaleza pública, privada o público-privada de una iniciativa.

Si bien la metodología se desarrolló de modo de dar cuenta de iniciativas tecnológicas de distinto carácter que eran de conocimiento previo del Consorcio Al Sur (soluciones basadas en la web, aplicaciones para dispositivos móviles, acuerdos con empresas de telecomunicaciones, etc.), para la primera fase del proyecto se priorizó el análisis de las aplicaciones de carácter nacional disponibles para descarga en dispositivos móviles. Con eso se buscó facilitar la comparación entre sus principales características, por ejemplo, en lo relacionado a las funcionalidades implementadas, los datos recogidos, el modo de obtención del consentimiento de las titulares para el uso de datos – algo que podría variar mucho a depender del tipo de iniciativa en análisis – y los derechos garantizados en relación al control de datos personales.

La propuesta metodológica contempló tanto el levantamiento de datos cuantitativos, como un análisis cualitativo orientado a sistematizar información atingente a la implementación de soluciones tecnológicas como parte de las políticas públicas y prácticas estatales en contexto de pandemia. La recolección de información quedó a cargo de las organizaciones miembro de Al Sur y de una colaboradora local en el caso de Bolivia (bajo la guía de Derechos Digitales). En general, cada organización pudo analizar una o más iniciativas desarrolladas en su país de actuación, con excepción de Derechos Digitales y el Instituto Panameño de Derecho y Nuevas Tecnologías (Ipandetec), que quedaron a cargo de analizar también iniciativas de otros países con el apoyo de informantes locales. En total fueron analizadas 16 aplicaciones de 14 países de la región, siendo una de implementación nacional de cada país, y dos adicionales en el caso de Bolivia. Una segunda etapa de análisis incluirá aplicaciones adicionales de Argentina, Colombia, Costa Rica y México.

Cada organización desarrolló sus propias estrategias para la obtención de información dependiendo de su experiencia, la disponibilidad de información pública y del contexto local de relacionamiento con autoridades y empresas a cargo de las iniciativas. Las fuentes incluyeron encuestas nacionales para la definición del contexto de implementación de las iniciativas en términos de conectividad, contratos de adhesión reflejados en los Términos y Condiciones y Políticas de Privacidad – entre otras denominaciones dadas a éstos – por los encargados del despliegue de las tecnologías, solicitudes de acceso a la información pública, documentos y declaraciones oficiales, información de la prensa, entrevistas directas con los desarrolladores de las tecnologías, entre otras.

Los análisis pasaron por tres procesos de revisión liderados por Derechos Digitales y el Centro de Estudios en Libertad de Expresión y Acceso a la Información (CELE) de la Universidad de Palermo, que también quedaron a cargo del desarrollo y aplicación de un manual de estilo a los contenidos finales.

Finalmente para la elaboración del presente reporte y el análisis del marco normativo específico de implementación de las iniciativas, se formularon solicitudes adicionales de información a cada una de las organizaciones de Al Sur, para verificar las condiciones normativas en materia de protección de datos personales y de acceso a la información en las cuales tuvieron lugar las implementaciones tecnológicas. Esta información fue procesada por Derechos Digitales para brindar un panorama general por país, y con posterioridad fue agregado el análisis conducido por el CELE, Fundación Karisma, InternetLab y Derechos Digitales para evaluar la normativa examinada y la implementación tecnológica desarrollada, respecto de los principios de legalidad, necesidad, proporcionalidad y transparencia conforme a los estándares del Sistema Interamericano de Derechos Humanos. Este análisis final permite contrastar las implementaciones tecnológicas desarrolladas durante la emergencia con los lineamientos más relevantes en nuestra región en materia de derechos humanos, y en particular aquellos especialmente provistos por la Comisión Interamericana de Derechos Humanos con ocasión de la pandemia.

Estándares y orientaciones de derechos humanos para el uso de tecnologías durante la pandemia

Múltiples actores locales, internacionales y regionales, en particular aquellos preocupados por el desarrollo de políticas y prácticas que respeten y garanticen los derechos humanos por todos los sectores, han emitido declaraciones, directrices, compilado estándares y promovido una mejor comprensión de las implicancias de los desarrollos tecnológicos en los derechos humanos de sus usuarias. Creemos que resulta útil tener a la vista estos estándares internacionales y directrices ofrecidos específicamente para garantizar la protección del ejercicio de derechos humanos en el contexto de pandemia, de manera de establecer el claro vínculo de cada uno de los aspectos de las tecnologías desplegadas cuya información se ha levantado con impactos directos en el ejercicio de derechos de la ciudadanía en nuestra región.

Temporalmente los primeros en advertir acerca de las implicancias del uso de la tecnología en el ejercicio de derechos en pandemia fueron los Expertos de la Organización de las Naciones Unidas (ONU), quienes emitieron una comunicación específica pidiendo a los Estados que respeten los derechos humanos en sus esfuerzos por combatir la pandemia y que eviten restricciones desproporcionadas e innecesarias al ejercicio de ciertos derechos. Además recordaron urgentemente a los Estados que cualquier respuesta de emergencia al Covid-19 debe ser proporcionada al riesgo evaluado, necesaria y no discriminatoria[6].

Ante las iniciativas que comenzaban a desarrollarse en la región, las organizaciones pertenecientes a Al Sur emitieron una declaración haciendo eco de las preocupaciones expresadas por los Expertos de la ONU, solicitando a los gobiernos de América Latina y el Caribe que las tecnologías digitales aplicadas ante la pandemia de Covid-19 respeten los Derechos Humanos[7].

Por su parte, la Comisión Interamericana de Derechos Humanos (CIDH) ha emitido hasta el momento dos documentos, la Resolución 01/20 "Pandemia y Derechos Humanos en las Américas[8]", y la Resolución 4/20 que "***Establece Lineamientos Interamericanos sobre Derechos Humanos de Personas con***

6 UN experts, "COVID-19: States should not abuse emergency measures to suppress human rights", 16 de marzo, 2020, disponible en: <https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=25722&LangID=E>

7 Al Sur, "Sociedad civil pide a gobiernos de América Latina y el Caribe que tecnologías digitales aplicadas ante la pandemia COVID-19 respeten los DDHH", Al Sur, 18 de marzo, 2020, disponible en: <https://www.alsur.lat/sites/default/files/2020-04/Sociedad%20civil%20pide%20a%20gobiernos%20de%20Am%C3%A9rica%20Latina%20que%20posibles%20tecnolog%C3%ADas%20digitales%20aplicadas%20ante%20la%20pandemia%20COVID.pdf>

8 Comisión Interamericana de Derechos Humanos, "*Resolución 1/20. Pandemia y Derechos Humanos en las Américas*", 10 de abril, 2020, disponible en: <https://www.oas.org/es/cidh/decisiones/pdf/Resolucion-1-20-es.pdf>

Covid-19[9]". En el primer instrumento, la CIDH enfatiza que los Estados deben "asegurar que, en caso de recurrir a herramientas de vigilancia digital para determinar, acompañar o contener la expansión de la epidemia y el seguimiento de personas afectadas, éstas deben ser estrictamente limitadas, tanto en términos de propósito como de tiempo, y proteger rigurosamente los derechos individuales, el principio de no discriminación y las libertades fundamentales. Los Estados deben transparentar las herramientas de vigilancia que están utilizando y su finalidad, así como poner en marcha mecanismos de supervisión independientes del uso de estas tecnologías de vigilancia, y los canales y mecanismos seguros para recepción de denuncias y reclamaciones[10]".

En tanto en su Resolución 4/20 la CIDH avanza un paso más en la precisión de sus directrices respecto de la evaluación del rol de algunas tecnologías en la pandemia para señalar: "*Los Estados deberán realizar una evaluación previa y pública del impacto que tienen en la privacidad de las personas afectadas por el virus las aplicaciones tecnológicas y herramientas de georreferenciación que se proyecten desarrollar para preservar la salud, a los efectos de justificar de forma fundada el beneficio de esas herramientas frente a otras alternativas que afecten en menor medida la privacidad. Asimismo, deberán prevenir la identificación selectiva de las personas y cuidar de que se recaben y utilicen los datos personales estrictamente necesarios para combatir la propagación de la Covid-19[11]*".

En línea con esto último, la Organización Mundial de la Salud (OMS) desarrolló un trabajo en esta materia con un comité multidisciplinario de expertos, con los cuales elaboró una guía de principios éticos, consideraciones técnicas y requisitos que son consistentes con estos principios para lograr el uso equitativo y apropiado de estas tecnologías con el propósito de informar a los programas de salud pública y a los gobiernos que están considerando desarrollar o implementar tecnologías digitales de trazabilidad para el seguimiento de contactos Covid-19[12].

Tales principios resultan útiles y orientadores para la toma de decisiones y fueron elaborados teniendo en cuenta las diferentes alternativas técnicas disponibles, de acuerdo a los distintos proyectos técnicos que, contra reloj, se han desarrollado alrededor del mundo para responder a los

9 Comisión Interamericana de Derechos Humanos, "Resolución 4/20. Establece Lineamientos Interamericanos sobre Derechos Humanos de Personas con COVID-19", 27 de julio, 2020, disponible en: <https://www.oas.org/es/cidh/decisiones/pdf/Resolucion-4-20-es.pdf>

10 CIDH, *Resolución 1/20*. Párrafo 36.

11 CIDH, *Resolución 4/20.* Párrafo 35.

12 World Health Organization, "*Ethical considerations to guide the use of digital proximity tracking technologies for COVID-19 contact tracing*", 28 de mayo 2020, disponible en: <https://apps.who.int/iris/bitstream/handle/10665/332200/WHO-2019-nCoV-Ethics_Contact_tracing_apps-2020.1-eng.pdf>

desafíos de la pandemia. Sin embargo, hasta ahora no ha sido posible levantar evidencia de que los casos específicos de tecnologías de esta naturaleza desarrolladas en nuestra región hayan considerado estas directrices, demostrando la necesidad de acercar estos esfuerzos técnicos multidisciplinarios a los espacios de toma de decisión política, más allá de las autoridades de salud que constituyen normalmente la audiencia natural de las guías emanadas de la OMS.

Otro tanto cabe afirmarse respecto de las directrices de la CIDH en materia de respeto de los estándares de legalidad, necesidad y proporcionalidad en el despliegue de tecnologías que impactan en el ejercicio de derechos fundamentales. Estos estándares son vinculantes para los Estados en todos los niveles de diseño e implementación de políticas públicas a fin de cumplir con su obligación de promover y proteger el ejercicio de los derechos humanos de su población, aún en momentos de crisis sanitaria.

Finalmente, durante el período de pandemia el Comité Jurídico Interamericano de la OEA emitió una actualización de sus principios sobre la privacidad y la protección de datos personales, con anotaciones[13], de los cuales también resulta posible derivar orientaciones para la implementación de tecnologías respetuosas de la protección de datos personales.

13 Ver http://www.oas.org/es/sla/cji/docs/CJI-RES_266_XCVIII-O-21.pdf

Una revisión de la tecnología desplegada y las estrategias para su despliegue

A.Tendencias regionales

Las estrategias digitales para la respuesta a la pandemia del Covid-19 en América Latina encuentran una importante barrera relacionada a la desigualdad en el acceso a internet y a las tecnologías por parte de la población. Si bien es posible observar una tendencia de aumento en la penetración de dispositivos móviles, el acceso a computadoras sigue limitado o decreciente en algunos países y las brechas en términos de conectividad persisten. Muchas usuarias de internet en la región disponen únicamente de conexiones móviles y muchas veces bajo servicios que les permiten acceder a una cantidad muy limitada de datos en forma mensual o sobre la base de programas de cero rating que aseguran sólo el acceso permanente a determinadas aplicaciones, por ejemplo.

Según datos recopilados por el Banco Mundial, el 65,8% de las latinoamericanas tenía acceso a internet en 2018, mientras que la cifra llega a 88% en América del Norte y 81,5% en la Unión Europea[14]. En Corea del Sur, país considerado pionero en el uso tecnológico para el combate al Covid-19, la penetración de acceso a internet en la población era de 96% en 2018[15].

Aún esos índice de conectividad global de la región, el contexto de implementación de las iniciativas analizadas en cuanto a la conectividad disponible varía en cada país. Mientras en países como Argentina, Chile, Costa Rica y Uruguay el porcentaje de usuarias de internet es muy superior a la media regional, alcanzando a más del 80% de la población, en Bolivia[16], Ecuador, El Salvador[17], y Paraguay no llega al 60% de la población. Brasil, Colombia, Guatemala, México, Panamá y Perú tienen entre 60 y 80% de la población con acceso a internet.

Esto afecta la penetración y efectividad que algunas de las tecnologías propuestas durante la pandemia pueden tener para cumplir con sus objetivos. En particular, la efectividad de las tecnologías de trazabilidad de contactos descansa en alcanzar un alto nivel de penetración en la población, lo cual resulta poco realista en contextos de conectividad

14 Banco Mundial, 2018, disponible en: <https://data.worldbank.org/indicator/IT.NET.USER.ZS?end=2018&locations=EU-ZJ-XU&start=1990&view=chart>

15 Banco Mundial, 2018, disponible en: <https://data.worldbank.org/indicator/IT.NET.USER.ZS?end=2018&locations=KR&start=1990&view=chart>

16 Banco Mundial, 2018, disponible en: <https://datos.bancomundial.org/indicador/IT.NET.USER.ZS?locations=BO>

17 Según datos del Banco Mundial, El Salvador tenía solo 33% de su población como usuaria de internet en 2018: https://data.worldbank.org/indicator/IT.NET.USER.ZS?end=2018&locations=SV&start=1990&view=chart.
Para 2020, la penetración de internet llegaba a 59% en el país según informaciones del reporte Digital 2020: https://datareportal.com/reports/digital-2020-el-salvador.

limitada. Conforme han mostrado estudios internacionales en la materia, para que sean realmente efectivas y produzcan un impacto relevante en la estrategia sanitaria[18], se requiere una alta adopción de entre por lo menos un 40% y un 60% de la población, sin perjuicio de que tasas menores serían útiles en casos de que sean aplicadas en conjunto con otras estrategias tradicionales.

18 Luca Ferretti, Chris Wymant, Michelle Kendall, Lele Zhao, Anel Nurtay, Lucie Abeler-Dörner, Michael Parker, David Bonsall, Christophe Fraser, Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing, Science08, Mayo 2020, disponible en: <https://science.sciencemag.org/content/early/2020/03/30/science.abb6936/tab-pdf>

19 Patrick Howell O'Neill, No, coronavirus apps don't need 60% adoption to be effective, MIT Technology Review, 5 de junio 2020, disponible en: <https://www.technologyreview.com/2020/06/05/1002775/covid-apps-effective-at-less-than-60-percent-download/>

Tabla 1: Número de usuarias de las aplicaciones de combate a Covid-19 analizadas y representatividad en la población

País	Número de usuarias	Porcentaje de la población (aproximado)
Argentina	Más de 10 millones (Google Play Store)	22,12
Bolivia[20]	Más de 50 mil (Google Play Store)	0,43
Brasil	Más de 1 millón (Google Play Store)	0,47
Chile	Más de 100 mil (Google Play Store)	0,52
Colombia	11 millones (Presidencia de la República)	21,62
Costa Rica	500 mil (Google Play Store)	10,27
Ecuador	Más de 500 mil (Google Play Store)	2,83
El Salvador	No se aplica[21]	Sin datos
Guatemala	Más de 100 mil (fuentes no oficiales)	1,68
México	Más de 500 mil (Google Play Store)	0,4
Panamá	2.300 (Autoridad Nacional para la Innovación Gubernamental)	0,06
Paraguay	5.473 (Ministerio de Salud)	0,08
Perú	Más de 1 millón (Google Play Store)	3,03
Uruguay	616 mil (Ministerio de Industria, Energía y Minería)	17,73

Fuente: elaboración propia datos a diciembre de 2020.

20 Considerando solamente la aplicación Bolivia Segura, disponibilizada desde el poder público, a nivel nacional.

21 No se trata de una aplicación independiente que puede ser descargada, sino de un chatbot disponible para Facebook y Whatsapp.

Además de las brechas existentes, otros factores pueden influir en la adopción de las aplicaciones disponibles al público para el control del Covid-19. Su nivel de difusión por parte de las autoridades gubernamentales seguramente cumple un rol decisivo en ese sentido y está intrínsecamente relacionado con el contexto político de cada país. En Brasil, por ejemplo, la aplicación "Coronavírus - SUS" fue implementada por un Ministerio de Salud afectado por sucesivos cambios de gestión[22]. En Bolivia, las respuestas a la pandemia fueron desarrolladas por un gobierno de transición de relativa legitimidad y en medio a una profunda crisis política. Allí también se presentaron iniciativas a nivel subnacional -como Salud En Cochabamba y Sammy Bot-, que terminan por competir con la solución propuesta desde el gobierno central[23].

En Colombia, CoronApp fue promocionada como una herramienta "salva vidas" destinada a impactar positivamente en la gestión de la pandemia, sin embargo como ha dado cuenta la sociedad civil local, a un año de estas promesas persisten las dudas sobre su utilidad real para mitigar o contener la pandemia. Se le exige a nivel interno mayor transparencia del Estado para permitir evaluar críticamente sus resultados, identificar cuáles son las enseñanzas a futuro y pensar qué estándares deben orientar el despliegue de herramientas de este tipo, y cómo podrían fortalecerse los procesos democráticos de rendición de cuentas a cargo de sus impulsores[24].

Distinto parece haber sido el caso uruguayo en que el nuevo gobierno publicitó la estrategia digital adoptada para responder al avance de la pandemia como pionera. En el caso de la incorporación de la función de alertas de exposición por medio de la interfaz de programación de aplicaciones (API, por la sigla en inglés referente a ***Application Programming Interface***) desarrollada por Apple y Google, el propio Presidente comunicó públicamente por su cuenta de Twitter agradeciendo a las empresas globales de tecnologías por su colaboración[25]. De igual manera en el caso de Ecuador la iniciativa desplegada por una empresa privada con el apoyo de BID Lab recibió respaldo institucional y comunicacional de parte de las autoridades públicas y empresas privadas del país que se sumaron a su promoción[26]. Conforme a la información compartida por sus desarrolladores, la aplicación es hoy la aplicación pública con más descargas en la historia de Ecuador.

22 Ver: Venturini, Jamila et al. Op. Cit.
23 Ver: Molina, Fernando. "La parálisis institucional enfrenta a Bolivia a un profundo conflicto social", El País, 26 de julio, 2020. Disponible en: https://elpais.com/internacional/2020-07-26/la-paralisis-institucional-enfrenta-a-bolivia-a-un-profundo-conflicto-social.html
24 Índice Coronavirus y derechos digitales en Colombia, ver: https://cv19.karisma.org.co/
25 Ver: https://twitter.com/LuisLacallePou/status/1271559039814709251.
26 Ver Lenin Moreno realizó la presentación del aplicativo móvil así ecuador, Youtube, 18 de agosto 2020, disponible en: <https://youtu.be/POHYfgmo4M8>

Por otro lado, la existencia de distintas soluciones al interior de un mismo país también pudo afectar el grado de adhesión a la aplicación desplegada a nivel nacional. En muchos países, particularmente aquellos federales, se observa una multiplicación de iniciativas a nivel departamental o provincial e incluso municipal en algunos casos. En México, por ejemplo, han sido identificadas nueve aplicaciones. En Bolivia, como vimos, fueron identificadas al menos cuatro[27], incluso una aplicación implementada de manera autónoma por una empresa privada[28].

Otro factor relevante es el carácter voluntario u obligatorio de la descarga. En el caso de América Latina, la tendencia parece apuntar a que se dio preferencia a soluciones de uso voluntario por la ciudadanía: no se registró ninguna aplicación cuyo uso fuera obligatorio en el análisis desarrollado. Sin embargo, en algunos casos ciertos grupos sí fueron obligados a instalarla. Algunos casos salientes en ese sentido son el de Argentina, Panamá y Uruguay, donde se requiere a las personas que quieran ingresar al país instalar la aplicación para hacer un monitoreo de síntomas. Del mismo modo, en el caso colombiano una resolución del Ministerio de Salud y Protección Social exige que algunos sectores de la población hagan uso de la aplicación "CoronApp", como trabajadores, contratistas, cooperados, sector aeronáutico, entre otros[29]. Lo mismo pasaría en Uruguay con profesionales del deporte, según informaciones publicadas en la prensa y en Argentina con ciertos trabajadores esenciales para el uso de transporte público, por ejemplo.

Entre las aplicaciones analizadas en la región fueron identificadas las siguientes funcionalidades: información de salud (incluso en tiempo real, en el caso de emergencias), autodiagnóstico, datos integrados para la toma de decisiones de salud pública, trazabilidad de contactos, pasaportes de movilidad y trabajo, telemedicina y vigilancia de confinamiento[30]. Se analizaron también dos chatbots implementados en aplicaciones de redes sociales y mensajería[31].

En algunos casos, frente a la escasez de tests suficientes y las dificultades de monitoreo del avance de la pandemia en los países, los objetivos de las aplicaciones –particularmente las de auto-diagnóstico– incluyen la producción de informaciones para apoyar la toma de decisiones del

27 Las aplicaciones Bolivia Segura, Salud en Cochabamba y Sammy Bot fueron analizadas en el marco del OCCA y están incluidas en los análisis que siguen.

28 Ver: Opinión. "Héroes en casa, la nueva plataforma boliviana de autoevaluación de Covid-19", 8 de abril, 2020. Disponible en: https://www.opinion.com.bo/articulo/tecnologia/heroes-casa-nueva-plataforma-boliviana-autoevaluacion-covid-19/20200408150910761074.html.

29 Ministerio de Salud y Protección Social, 2020, disponible en: <https://www.minsalud.gov.co/Normatividad_Nuevo/Resoluci%C3%B3n%20No.%20666%20de%202020.pdf>

30 Ver: Canales, Maria Paz. Op. Cit.

31 Sammy Bot (Bolivia) y Sivi (El Salvador).

Estado. Es el caso de México, por ejemplo, donde la información estadística recabada mediante la aplicación "COVID19-MX" es utilizada para orientar las políticas de las autoridades de salud. Algo similar menciona la página web de la aplicación "CUIDAR" de Argentina: "*[l]a app Cuidar complementa y asiste las políticas de prevención y cuidado de la población y, en particular, brinda elementos e insumos concretos para la intervención sanitaria de los ministerios de Salud en todo el territorio nacional*[32]".

B. Derechos afectados

El derecho a la protección de datos personales se encuentra afectado por todas las aplicaciones analizadas. Muy estrechamente conectado a este, se afecta en la mayor parte de los casos el derecho a la privacidad, reconocido por tratados de derechos humanos firmados por todos los países donde se implementan estas iniciativas y la mayor parte de sus Constituciones Nacionales.

La protección de datos se refiere a la capacidad de autodeterminación informativa de las titulares de datos, o sea, su capacidad de ejercer un efectivo control sobre el uso de sus informaciones personales, mientras la privacidad se caracteriza por la posibilidad de excluir, quedar exento e inmune a invasiones arbitrarias por parte de terceros o de la autoridad pública en la esfera íntima. Esta última se ve afectada en el caso de estos despliegues tecnológicos, por ejemplo, por la ausencia de medidas de seguridad que impidan un acceso indebido a la información recolectada, y la posibilidad de vigilancia por parte de agentes estatales o privados.

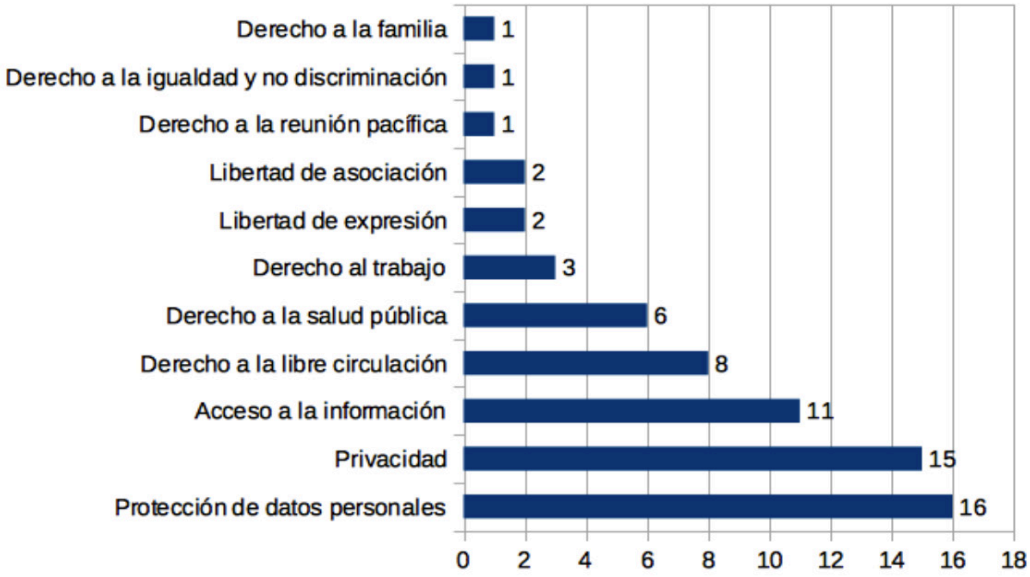
El derecho de acceso a la información se ve afectado en 11 de las iniciativas, principalmente debido a que se encuentra condicionado a la entrega de ciertos datos personales – sea por medio de registros, sean metadatos recolectados de manera automática con la instalación. En ese sentido, se observa como una mala práctica la exigencia de suscripción para acceder a informaciones de interés público sobre la evolución de la pandemia, la ubicación de centros de salud, entre otras que deberían estar disponibles abiertamente. Este tipo de práctica puede afectar también el derecho a la salud pública, como se ha detectado en seis de las aplicaciones analizadas.

Ocho aplicaciones afectan también el derecho a la libre circulación, especialmente en los casos en que incorporan funcionalidades como la emisión de permisos o de denuncia de aglomeraciones, por ejemplo, como en el caso chileno. Ahí también se puede ver afectado el derecho de reunión pacífica.

El derecho al trabajo también puede verse afectado por este tipo de aplicaciones, como se ha apuntado en tres de los casos analizados: Argentina, Colombia y México.

32 Jefatura de Gabinete de Ministros, 2020, disponible en: <https://www.argentina.gob.ar/jefatura/innovacion-publica/acciones-coronavirus/aplicacion-y-tableros-de-gestion/que-es>

Gráfico 1: Número de aplicaciones por derecho afectado



Fuente: elaboración propia.

El indicador de afectación de derechos por las tecnologías identificadas en el OCCA constituye la pieza articuladora que permitirá luego expandir el análisis factual aquí presentado al análisis de la satisfacción (o no) de las distintas iniciativas con los estándares establecidos por la CIDH y los ordenamientos Constitucionales nacionales.

C. Análisis comparado de indicadores críticos de funcionalidad

I. Funcionalidades y datos recolectados

Las aplicaciones analizadas incorporan una gran variedad de funcionalidades. En algunos casos donde las soluciones de oferta de información de interés público y auto-diagnóstico fueron lanzadas poco tiempo después de la identificación de los primeros casos de Covid-19, se realizaron actualizaciones a fin de incorporar funcionalidades adicionales. Es el caso de la función de trazabilidad de contactos en Brasil y Uruguay, por ejemplo, cuyos protocolos para implementación a nivel nacional se fueron desarrollando entre los meses de abril y mayo, cuando varias de las iniciativas analizadas ya se habían lanzado[33].

La función que promete facilitar el monitoreo de la exposición de las usuarias al nuevo coronavirus se encuentra también disponible en las aplicaciones de Colombia, Ecuador y Panamá, totalizando cinco de las 16 aplicaciones analizadas. Es importante hacer notar que en algunos países

33 Entre las 16 aplicaciones móviles o chatbots analizados, la gran mayoría fue lanzada en el mes de marzo de 2020, al mismo tiempo en que se empezaban a detectar los primeros casos de COVID-19 en la región. Del total, una fue disponibilizada en el mes de febrero, siete en marzo, tres en abril, dos en mayo, dos en junio y una en agosto (en este caso una versión piloto había sido lanzada en marzo).

donde la aplicación de cobertura nacional no incorpora esta funcionalidad, eventualmente surgen otras soluciones a nivel subnacional que sí la incorporan. En México existen tres aplicaciones de nivel provincial que incorporan la trazabilidad de contactos. En el caso de Bolivia, ninguna de las tres iniciativas analizadas incorpora la función, aunque fuentes locales afirman que hubo discusiones al respecto.

En la presente investigación también se analizó la disponibilidad de las siguientes funciones en las aplicaciones: geolocalización, base de datos, reconocimiento facial y brazalete electrónico. Entre esos factores, la aplicación "Ecuador ASI" y el chatbot Sivi, de El Salvador son las únicas iniciativas que no incluyen una funcionalidad de geolocalización. Todas las demás aplicaciones analizadas prevén este tipo de función, aunque en la mayoría de los casos por opt-in -la usuaria tiene la opción de activarla o no. Es interesante observar cómo la funcionalidad es incorporada al chatbot Sammy Bot, de Bolivia: se pide el envío de la ubicación actual por medio de las opciones de la aplicación de mensajería Whatsapp de manera obligatoria para hacer el pre-diagnóstico, lo que constituye una muestra de recolección excesiva de datos, ya que difícilmente tal información podría ser considerada necesaria para el diagnóstico[34].

Ninguna aplicación incorpora funcionalidades asociadas al uso de brazaletes electrónicos y solo la panameña "Protégete con Salud" incluye reconocimiento facial. "Protégete con Salud" es la plataforma oficial del Gobierno de Panamá que permite a los pacientes positivos de Covid-19 mantenerse en comunicación con los expertos de la salud, sobretodo en posibles momentos de urgencia. Aún con relación al uso de informaciones biométricas, la aplicación "Bolivia Segura" ofrece la posibilidad de validación en el sistema por medio de huella digital.

La aplicación chilena, por su parte, ofrece la posibilidad de reportar incidentes y aglomeraciones, así como de conectarse con una comisaría virtual para solicitud de permisos de salida y otros servicios públicos. La aplicación colombiana por su vez incluye la posibilidad de emitir pasaportes de movilidad, algo también presente en la aplicación argentina, que emite certificados de permiso de circulación. En Perú, la aplicación "Perú en tus manos" incluye un mapa con indicaciones de riesgo de contagio por zonas. Finalmente, la "Coronavirus UY", de Uruguay, incluye la función de telemedicina y la posibilidad de emisión de un certificado de salud para ingreso de personas extranjeras al país. Una función interesante en términos de accesibilidad en el caso uruguayo es la posibilidad de uso de la

34 Sammy Bot, es un chatbot de WhatsApp que ofrece asistencia médica con la posibilidad de realizar pre-diagnósticos del COVID-19, tests con un PsicoBot, solicitar la entrega de Pruebas Rápidas y agendar una cita con un médico por telemedicina. Es la solución tecnológica oficial del Servicio Departamental de Salud de La Paz y de la ciudad de Santa Cruz.

aplicación por más de una persona en un único dispositivo.

Con relación a los datos recolectados, once de las aplicaciones solicitan de las usuarias información sobre el número de documento nacional de identidad (DNI), doce el nombre, doce la edad, diez el género, nueve la dirección, catorce la ubicación, catorce recolectan datos de sintomatología y diez sobre enfermedades pre-existentes[35]. Solamente la aplicación de Panamá solicita una fotografía de la usuaria, posiblemente para habilitar la funcionalidad de reconocimiento facial incorporada.

II. Características del consentimiento para el tratamiento de datos personales

Con relación al otorgamiento del consentimiento por parte de las titulares para el tratamiento de sus datos personales, se analizó si se trataba de un consentimiento expreso, libre e informado a partir de la siguiente definición estándar:

> "El consentimiento debe cumplir con los siguientes elementos: (i) la aplicación solicita marcar activamente el consentimiento para el uso de datos, como un acto distinto de la instalación y antes de empezar a operar, (ii) la aplicación no recopila ni procesa datos antes de que se marque la aceptación, (iii) la solicitud de aceptación viene acompañada de un texto, o un enlace a un texto, que puede leerse de manera previa a la aceptación, que indique los datos que serán usados, por quiénes y en qué condiciones".

Menos de la mitad de las aplicaciones analizadas (seis) cumplen con todos los requisitos en la recolección del consentimiento. Las demás no lo hacen por distintas razones. En el caso de la aplicación brasileña, por ejemplo, hay inconsistencias relevantes entre los términos de solicitud del consentimiento presentes en su Política de Privacidad y los datos que son efectivamente recolectados.

La gran mayoría de las aplicaciones solicita el consentimiento de manera activa por medio de un click o un botón. Solo tres de ellas asumen el consentimiento por el uso de aplicación. En el caso de los chatbots analizados, ambos asumen el consentimiento por el uso. Cuando se trata de la retirada del consentimiento por parte de la titular, la mayoría lo permite y ofrece una dirección de correo o medios de contacto para que se haga la solicitud. Sin embargo, de manera preocupante se observa que siete

35 En el caso de Sivi, el chatbot implementado en El Salvador, aunque los datos como documento de identidad y ubicación no sean requeridos directamente de las usuarias, pueden ser obtenidos por el cruce de bases de datos o los permisos requeridos por la aplicación sobre la cual opera (por ejemplo Messenger o WhatsApp, ambas controladas por la empresa Facebook). Aún así, ese caso no está contabilizado en los números presentados arriba.

aplicaciones no permiten la retirada del consentimiento para el tratamiento de datos en cualquier momento.

Es el caso de la aplicación Bolivia Segura, cuyos términos y condiciones informan que "***los datos serán conservados y tratados mientras sean necesarios para las finalidades indicadas en el inciso c) anterior, y durante el período que el Usuario haga uso de los Servicios Digitales y que dure la situación de emergencia sanitaria. En el momento en que finalice el periodo de conservación de tus datos personales será anonimizados para evitar una posterior identificación***". De hecho, las tres aplicaciones bolivianas no explicitan mecanismos para la retirada del consentimiento. Las demás son: Coronavírus SUS, de Brasil; CoronApp, de Colombia; Alerta Guate, de Guatemala; y Protégete con Salud, de Panamá.

D. Análisis de transparencia

La cuestión de la transparencia es transversal al análisis de las tecnologías implementadas, siendo un factor fundamental para facilitar información no sólo sobre cuestiones prácticas y técnicas de las aplicaciones -cuestiones relativas a sus funcionalidades, términos de privacidad y seguridad, por ejemplo- sino también para conocer cuáles son las autoridades gubernamentales y/o empresas detrás de su desarrollo y cuál es el uso dado a los datos recolectados. En este sentido, a los fines del análisis comparativo, nos concentramos principalmente en dos tipos de transparencia: por un lado, en aquella derivada del derecho de acceso a la información pública: la información en poder del Estado a la que las ciudadanas deben poder acceder -con la salvedad de una restricción legítima-, inherentemente asociado al ejercicio de su derecho de libertad de expresión. Por otro lado, en la transparencia relativa al tratamiento y uso de los datos personales, fundamental para el ejercicio de la autodeterminación informativa por parte de las usuarias, que debe estar en concordancia con los estándares internacionales de protección de datos y consistentes con consideraciones de privacidad en tratados internacionales de Derechos Humanos.

En el ámbito regional, la Corte Interamericana de Derechos Humanos ha interpretado el artículo 13 de la Convención Americana de Derechos Humanos (CADH) de manera amplia, otorgándole al derecho a la libertad de pensamiento y de expresión una dimensión individual y social, de la cual se desprende el derecho de acceso a la información. En este sentido, la Corte ha indicado que el derecho a la libertad de pensamiento y de expresión consagrado en la CADH comprende "***no sólo el derecho y la libertad de expresar su propio pensamiento, sino también el derecho y la libertad de buscar, recibir y difundir informaciones e ideas de toda índole***[36]". En el caso Claude Reyes y Otros vs. Chile, la Corte establece que

36 Caso López Álvarez, supra nota 72, párr. 163; Caso Ricardo Canese, supra nota 72, párr. 77; y Caso Herrera Ulloa, supra nota 72, párr. 108

el artículo 13 ampara el derecho de las personas a recibir la información bajo el control del Estado, al mismo tiempo que ampara "***la obligación positiva del Estado de suministrarla, de forma tal que la persona pueda tener acceso a conocer esa información o reciba una respuesta fundamentada cuando por algún motivo permitido por la Convención el Estado pueda limitar el acceso a la misma para el caso concreto***[37]". Al igual que en la CADH, la Declaración Universal de Derechos Humanos y el Pacto Internacional de Derechos Civiles y Políticos también disponen un derecho positivo a buscar y recibir información.

La transparencia pública es fundamental para garantizar el correcto funcionamiento de la democracia: el acceso a la información pública por parte de las ciudadanas permite aunar esfuerzos para combatir la corrupción y abusos de poder[38]. En lo que respecta a las aplicaciones tecnológicas desplegadas en razón de la pandemia, el acceso a la información y la transparencia son cruciales para verificar que el balance entre la protección del derecho a la salud y la afectación de otros derechos fundamentales como la privacidad y protección de datos, se realice en concordancia con las normas de derechos humanos.

Además de la jurisprudencia en materia de acceso a la información en el marco del Sistema Interamericano de Derechos Humanos, la CIDH en su Resolución 1/20 formula la siguiente recomendación a los Estados miembros: "(…) ***Los Estados deben transparentar las herramientas de vigilancia que están utilizando y su finalidad, así como poner en marcha mecanismos de supervisión independientes del uso de estas tecnologías de vigilancia, y los canales y mecanismos seguros para recepción de denuncias y reclamaciones***[39]".

Sumado a ello, la OMS en su Guía de consideraciones éticas para el uso de dispositivos de trazabilidad de Covid-19[40] dispone entre los principios sugeridos el de "transparencia y explicabilidad", indicando lo siguiente: "L***a recolección y el tratamiento de los datos será transparente, y se le brindará a las personas información concisa y de fácil lectura, en un lenguaje claro e inequívoco, sobre el propósito de la recolección, los tipos de datos***

37 Caso Claude Reyes y Otros Vs. Chile, disponible en: https://www.corteidh.or.cr/docs/casos/articulos/seriec_151_esp.pdf

38 La Carta Democrática Interamericana, en su artículo 4, establece que son componentes fundamentales del ejercicio de la democracia "la transparencia de las actividades gubernamentales, la probidad, la responsabilidad de los gobiernos en la gestión pública, el respeto por los derechos sociales y la libertad de expresión y de prensa". Disponible en: https://www.oas.org/charter/docs_es/resolucion1_es.htm

39 Resolución 1/20 CIDH, Par.36.

40 World Health Organization, "Ethical considerations to guide the use of digital proximity tracking technologies for COVID-19 contact tracing", 28 de mayo 2020, disponible en: <https://apps.who.int/iris/bitstream/handle/10665/332200/WHO-2019-nCoV-Ethics_Contact_tracing_apps-2020.1-eng.pdf>

recogidos, cómo se almacenarán y compartirán los datos y cuánto tiempo se conservarán. Debe haber total transparencia sobre cómo funcionan las aplicaciones y las interfaces de programación de aplicaciones (API), y publicación de los códigos de código abierto y de libre acceso. También se debe proporcionar a las personas información significativa sobre la existencia de tomas de decisiones automatizadas y cómo se realizan las predicciones de riesgo, incluyendo cómo se ha desarrollado el modelo algorítmico y los datos utilizados para entrenar el mismo. Además, debe haber información sobre la utilidad del modelo y sobre los tipos de errores que un modelo de este tipo puede cometer" (la traducción es propia).

La medida dialoga con lo establecido en el Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (Convenio 108)[41], firmado por algunos países de la región, que determina que los datos personales deben ser tratados de manera transparente (artículo 5.4). La transparencia es así entendida como un principio básico de la protección de datos y el Convenio detalla en el artículo 8 que los países deberán garantizar que las entidades que actúen como controladores informen sobre su dirección, la base legal para el tratamiento de datos, las categorías de datos procesadas, los recipientes de cada categoría de datos y las maneras en las personas afectadas pueden ejercer sus derechos en relación al procesamiento de los datos.

En función de estos principios y recomendaciones, el análisis sobre la transparencia de las aplicaciones desplegadas en este reporte incluye los siguientes ejes: i) transparencia en el diseño de las aplicaciones; ii) participación de la ciudadanía en el diseño y evaluación de las aplicaciones; iii) transparencia en cuanto a la información que se hace disponible a las usuarias; iv) derechos de las titulares de los datos personales; v) cuáles son los organismos gubernamentales que tienen acceso a los datos recolectados; vi) información sobre el carácter público, privado o público-privado de la aplicación.

I. Diseño y seguridad de las aplicaciones

De modo general podemos concluir que ninguna de las aplicaciones informa las medidas de seguridad adoptadas en forma detallada. Algunas de ellas ni siquiera hacen mención a políticas de seguridad, es el caso de aquellas desarrolladas en Paraguay, Perú, Colombia, México, Panamá y El Salvador.

Aquellas aplicaciones que sí hacen mención a las medidas de seguridad adoptadas para su desarrollo y uso, proveen información a título general, indicando que se ha asumido el compromiso de proteger los datos allí

41 Ver: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108.

recabados, se han implementado medidas técnicas adecuadas (por ejemplo en los casos de Uruguay, Bolivia Salud en Cochabamba, Ecuador y Guatemala), y/o que se cumplen con certificaciones de seguridad reconocidos a nivel internacional como las normas ISO (por ejemplo, Argentina menciona esto en un sitio web externo a la app). Lo mismo sucede en el caso de Brasil, con excepción de las medidas de seguridad involucradas en el uso de la trazabilidad de contacto, las cuales son explicadas en mayor profundidad con una infografía. En el caso de Chile, la aplicación prevé un enlace que lleva al sitio web oficial del Ministerio de Salud donde se encuentran las políticas de protección de datos y de seguridad en el desarrollo de sistemas que, si bien podrían aplicarse a esta app, no están exclusivamente diseñadas para ella.

En el otro extremo, un caso interesante para mencionar es el de Costa Rica. En la política de privacidad de la aplicación, se informa lo siguiente: ***"Hemos implementado medidas de seguridad técnicas y organizativas apropiadas diseñadas para proteger la seguridad de cualquier información personal que procesemos. Sin embargo, recuerde también que no podemos garantizar que Internet sea 100% seguro. Aunque haremos todo lo posible para proteger su información personal, la transmisión de información personal hacia nuestras aplicaciones es bajo su propio riesgo. Solo debe acceder a los servicios dentro de un entorno seguro".***

Sin perjuicio de cómo informan las medidas de seguridad adoptadas, todas las aplicaciones parecen transferir los datos de forma segura a través de protocolos HTTPS.

II. Participación de la ciudadanía

Cuando se trata de las instancias de participación ciudadana en la implementación de las iniciativas analizadas, el escenario regional es también preocupante.

En relación a los aportes de la sociedad civil al diseño o implementación de las iniciativas, solamente Ecuador contempló una instancia de participación de académicos antes de la implementación de su aplicación. Particularmente, se solicitó la revisión de tres componentes de la aplicación por parte de los académicos, que pertenecían a tres diferentes universidades: la Pontificia Universidad Católica del Ecuador (PUCE), la Universidad de las Fuerzas Armadas y la Escuela Superior Politécnica del Litoral. Se requirieron sus comentarios en las distintas etapas del desarrollo de la aplicación, incluso se les compartió el acceso al código previo a su publicación y se hizo un seguimiento de las opiniones recibidas.

Se observa con preocupación la poca participación de la sociedad civil en la evaluación de las aplicaciones después de su despliegue. Nuevamente

Ecuador representa una buena práctica en ese sentido por medio del seguimiento de los comentarios al código de la aplicación, que es abierto. Otro país donde fueron considerados los aportes de la sociedad civil fue Argentina: luego del lanzamiento de la primera versión de "CUIDAR", se realizaron varias críticas a la cantidad de permisos solicitados y cuestiones generales del funcionamiento. Algunas de ellas fueron consideradas e incorporadas como mejoras en las versiones siguientes. La Secretaría de Innovación abrió además un canal de comentarios y consultas mediante un formulario en su página web y por correo electrónico.

La mayoría de las iniciativas no hace disponible su código de manera abierta. En aquellos casos en los que sí lo hace, los desarrolladores lo han presentado como medida explícita para permitir el desarrollo de auditorías ciudadanas, como en Uruguay -aunque para acceder al código completo de la aplicación es necesario presentar una solicitud institucional y justificar su fundamento y propósitos-. Conforme el comunicado del Ministerio de Salud Pública, ***"con el objetivo de brindar una total transparencia y garantías sobre el manejo de la información recolectada, en esta primera etapa, se pone a disposición de instituciones nacionales (academia, industria, sociedad civil organizada), la posibilidad de auditar la documentación y código fuente de la aplicación Coronavirus UY, incluyendo sus funcionalidades de alerta de exposición***[42]".

Además de Uruguay, en lo que respecta a la realización de evaluaciones y auditorías técnicas externas, solo las aplicaciones desplegadas en Colombia y Ecuador prevén este tipo de mecanismo. El caso argentino es llamativo, pero esta vez desde el punto de vista negativo: las primeras versiones de los Términos y Condiciones de la aplicación incluían cláusulas prohibiendo auditorías independientes por investigadores de seguridad, por ejemplo, por medio de técnicas de ingeniería inversa. Estas cláusulas fueron eliminadas de las nuevas versiones de la aplicación.

III. Información disponible para las usuarias

La información se presenta en un lenguaje claro y accesible en la mayoría de las iniciativas desarrolladas, con excepción de cuatro de ellas (Colombia, Panamá, Ecuador y el Sammy Bot de Bolivia), según la siguiente definición ofrecida para el análisis:

> "La información se entrega usando oraciones cortas y de estructura simple, con vocabulario sencillo, indicando qué personas adoptarán qué acciones. La información no usa lenguaje excesivamente técnico, del ámbito jurídico ni tecnológico, y cuando lo hace provee ejemplos

42 Fuente: Ministerio de Salud Pública, 2020, disponible en: https://www.gub.uy/ministerio-salud-publica/politicas-y-gestion/informacion-sobre-aplicacion-coronavirus

> o definiciones simples para facilitar la comprensión".

En cuanto a la información entregada, solo la aplicación mexicana y el chatbot de El Salvador no informan a las titulares el propósito del tratamiento de sus datos personales.

La mayoría de ellas, a su vez, informa cuáles son las autoridades y/o empresas que se encargan de la recopilación y procesamiento de los datos personales, con excepción de Paraguay, El Salvador y Sammy Bot de Bolivia. En este caso directamente no cuenta con términos y condiciones ni explica cuál es la institución que procesa los datos.

En algunos casos, las empresas y organismos detrás de las aplicaciones fueron revelados por investigaciones privadas llevadas a cabo por la sociedad civil y la prensa. En el caso de Brasil, por ejemplo, a pesar de que se indique que el procesamiento de datos lo realiza el Ministerio de Salud, la organización InternetLab encontró que existe un intercambio de datos con la empresa Amazon (descubrimiento posible gracias a la herramienta Lumen). En el caso de Guatemala, a su vez, la información sobre la empresa detrás del procesamiento de datos y sus vínculos con el gobierno fue revelada por investigaciones técnicas y periodísticas, luego de que las críticas sobre el despliegue de la tecnología se volvieran públicas.

IV. Derechos de las titulares

Solo en la mitad de las aplicaciones analizadas garantiza un control efectivo sobre el uso de datos personales, considerando el siguiente criterio:

> "Las garantías previstas por los términos y condiciones de la aplicación, o las normas legales a que ellos hacen referencia, incluyen la posibilidad de ejercicio por las titulares de datos de los derechos de acceso, rectificación, cancelación y oposición".

Ocho aplicaciones cumplen con este estándar, disponiendo mecanismos por los cuales las usuarias pueden ejercer el derecho de acceso, rectificación y cancelación o supresión de sus datos personales. En el caso de Bolivia, los Términos y Condiciones de "Bolivia Segura" solo hacen referencia al uso y acceso a la información pública disponible en la aplicación, sin mención a los datos introducidos por la usuaria. Lo mismo pasa con Ecuador, donde no hay referencias u orientaciones sobre la posibilidad de acceso, rectificación, cancelación y oposición por parte de las titulares de datos en la documentación analizada.

En el caso de Colombia, la Política de Privacidad reconoce a la titular su derecho a conocer, actualizar y rectificar sus datos personales, así como de requerir que se le informe sobre los usos hechos de ellos y de presentar

quejas ante la autoridad de protección de datos. Sin embargo, cuando se trata de la cancelación, las informaciones no son claras y hay una serie de condicionantes al ejercicio de este derecho.

Entre las aplicaciones que permiten el acceso, de modo general se ofrecen canales de comunicación oficiales (correo, teléfono o dirección de una oficina física) para el ejercicio del derecho de acceso, así como de cancelación, rectificación y oposición.

V. Acceso gubernamental a datos

Comprender la posibilidad de acceso a las informaciones recolectadas por la aplicación por parte de otras instituciones gubernamentales no siempre es fácil. Aunque en algunos casos las hipótesis de acceso compartido son explicitadas en los contratos de adhesión asociados a las plataformas, en otros es necesario hacer una revisión de la normativa aplicable tanto de manera general, como en la situación excepcional de pandemia. Como resultado, en muchas situaciones no es totalmente claro para las usuarias cuáles son las entidades que podrían acceder a los datos y las situaciones y condiciones de acceso. Aún así, como se nota en los ejemplos a continuación, en muchos de los casos está previsto tal tipo de acceso.

En Argentina, a pesar de que en la administración de la app se encuentra involucrada la Subsecretaría de Gobierno Abierto, el Estado no publica información sobre el uso de informaciones como datos estadísticos o casos positivos identificados. En este caso, los Términos y Condiciones son claros en explicitar que los datos pueden ser cedidos a cualquier organismo estatal en el contexto de la emergencia sanitaria: "***El Usuario presta su consentimiento expreso para que la Subsecretaría de Gobierno Abierto ceda la información personal del Usuario recolectada por la Aplicación únicamente a otras entidades estatales y/o establecimientos sanitarios nacionales, provinciales o municipales, para que estos puedan contener y/o mitigar la propagación del virus COVID19, ayudar a prevenir la sobreocupación del sistema sanitario argentino.***" A pesar de la autorización genérica, la aplicación establece una buena práctica al garantizar a las usuarias la posibilidad de requerir información sobre cesiones realizadas de forma no disociada de los datos.

Cuando se trata de la normativa aplicable, es importante llamar la atención al artículo 2 de la decisión administrativa 431/2020 de la Jefatura de Gabinete de Ministros que determina que la Dirección Nacional de Migraciones deberá transferir o ceder datos o informaciones a las jurisdicciones provinciales y de la Ciudad de Buenos Aires para contribuir a la identificación y localización de las personas que puedan reunir la condición de “caso sospechoso”, así como de quienes hubieran estado en contacto estrecho con ellas.

En el caso de Brasil, la Política de Privacidad de la aplicación "Coronavírus SUS" afirma que el consentimiento sólo cubre el tratamiento de sus datos por el Ministerio de Salud de Brasil. Sin embargo, según la legislación brasileña, los datos recolectados por el Estado pueden utilizarse libremente por otros órganos públicos si son anonimizados (es decir, si es imposible volver a identificar a su titular) o si son "***necesarios para la ejecución de políticas públicas previstas en leyes, acuerdos o similares***", "para la protección de la vida o la seguridad física del propietario o de terceros", entre otras hipótesis. Además, no existe una disposición clara en la legislación brasileña sobre el uso de datos para la seguridad pública de modo que existen varias hipótesis en las que otros organismos públicos podrían tener acceso a los datos reunidos por la aplicación.

En Colombia, además de la Agencia Nacional Digital y el Instituto Nacional de Salud responsables respectivamente por el desarrollo de la aplicación y por la gestión de la información recolectada, cualquier órgano público puede tener acceso a los datos si ellos son considerados necesarios para el ejercicio de sus funciones o por orden judicial.

En México, el aviso de privacidad declara que se podrán transferir datos al Sistema Nacional de Salud, el cual está constituido por las dependencias y entidades de la Administración Pública a nivel federal y local, por las personas físicas o morales de los sectores social y privado que presten servicios de salud, así como por los mecanismos de coordinación de acciones.

En Panamá, la Fuerza de Tarea Conjunta puede tener acceso a los datos en el contexto de la pandemia. Ella está constituida por un equipo de médicos del Ministerio de Salud apostados en el Centro de Operaciones de Emergencia (COE) del Sistema Nacional de Protección Civil (Sinaproc). El COE por su vez está conformado por la Gobernación de la Provincia, Ministerio de Salud, CSS, Policía Nacional, Ministerio de Desarrollo Social y líderes comunitarios.

En Paraguay, mientras los datos de salud son considerados sensibles y, entre ellos, los datos médicos son confidenciales, los datos personales incluyendo nombre, número de cédula, teléfono, dirección y ubicación georeferencial pueden ser accedidos por cualquier autoridad competente, según informa la Política de Privacidad de la aplicación. Un comunicado oficial agrega que puede haber participación de Migraciones y Policía Nacional en la gestión y tratamiento de los datos: "***a través del Servicio del Sistema de Intercambio de Informaciones del MITIC esta aplicación cruzará por primera vez las bases de datos de Migraciones, (de quienes ingresaron al país), de la Policía Nacional (que valida los datos personales de los ciudadanos), y***

los datos de Salud, (del cumplimiento de la cuarentena), para el envío de reportes médicos y las instrucciones de no salir de la casa, etc"[43].

VI. Carácter de las iniciativas

La mayoría de las iniciativas analizadas fueron desarrolladas por el sector público (siete) y con presupuesto estatal (siete). Todas las demás (nueve) fueron viabilizadas por medio de iniciativas público-privadas.

Entre las iniciativas público-privadas, un modelo que se repite en los casos de Argentina, Guatemala, El Salvador, Panamá, Perú y Uruguay es el de donación de las aplicaciones por el sector privado. En el caso argentino y uruguayo, las donaciones se realizaron por empresas de tecnología nacionales organizadas alrededor de entidades industriales, pertenecientes a la Cámara de la Industria Argentina del Software y la Cámara Uruguaya de Tecnologías de la Información, respectivamente. Desde la perspectiva de desarrollo local, este es un modelo interesante en tanto evidencia la preparación de la industria para responder a los desafíos tecnológicos que presenta la implementación de las aplicaciones bajo análisis. A la vez, muestra la existencia de un ecosistema de colaboración previo a la pandemia.

El caso de El Salvador es interesante dado que el chatbot Sivi fue una donación de la empresa de tecnologías global Facebook. También en Guatemala la aplicación habría sido financiada por el grupo multinacional Tenlot[44], que maneja una lotería en el país[45]. En Panamá, la donación provino de una única empresa de operación regional en Centroamérica (GBM Panamá) y en Perú de un conjunto de seis empresas y una universidad.

El caso de Ecuador es particular: la iniciativa es considerada privada porque una empresa (Link Digital) recibió apoyo del Banco Interamericano de Desarrollo (BID) para desarrollar la aplicación "Ecuador ASI" y luego la ofreció al gobierno local.

Ante la ausencia de informaciones más detalladas sobre los términos de este tipo de cooperación entre empresas y gobiernos, surgen dudas sobre los eventuales beneficios que estas empresas podrían tener, tales como el acceso a determinados tipos de datos.

Cabe mencionar que además de las empresas involucradas en el desarrollo, varias de las aplicaciones cuentan con servicios privados para

43 Mintic, 2020, disponible en: <https://www.mitic.gov.py/noticias/control-de-personas-en-cuarentena-se-realizara-con-app-que-facilita-datos-clinicos-y-localizacion>

44 Ver: http://www.sp-tenlot.com/category/Sobre-Tenlot.

45 Fuente: https://www.no-ficcion.com/project/empresas-ciberseguridad-app-covid-19-giammattei.

el almacenamiento de los datos recolectados. Nueve de las iniciativas analizadas usan servidores privados para ello. Se identificó la utilización de los servicios de Amazon en cuatro aplicaciones y en una los de Google. En cuatro casos no fue posible identificar cuál era la empresa proveedora de los servicios de almacenamiento. Tres aplicaciones tienen sus datos almacenados en data centers públicos y en dos casos no se encontraron informaciones disponibles sobre la ubicación del almacenamiento de los datos.

Análisis jurídico por país

Presentamos aquí los principales aspectos de los marcos normativos vigentes en cada país durante el período analizado por el OCCA en relación a la protección de datos personales y el acceso a la información[46]. También se identifican, cuando resulta relevante para la vigencia de tales marcos generales identificados, normativa específica implementada durante la emergencia sanitaria con potencial afectación a tales derechos.

Argentina

Argentina ha asumido importantes compromisos con la protección de los derechos humanos, que en particular incluyen garantías para el acceso a la información y la privacidad. Además de adherir a la Declaración Internacional de los Derechos Humanos, el Pacto Internacional de Derechos Civiles y Políticos, el Pacto Internacional de Derechos Económicos, Sociales y Culturales y la CADH, Argentina es parte del Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (Convenio 108) y ha adoptado los Principios de la Organización para la Cooperación y el Desarrollo Económicos (OCDE) sobre Inteligencia Artificial. El país también ha firmado el Protocolo Adicional que modifica el Convenio 108 (conocido como "Convenio 108+"), pero este aún no ha sido aprobado por el Congreso, y por tanto se encuentra pendiente de entrada en vigencia.

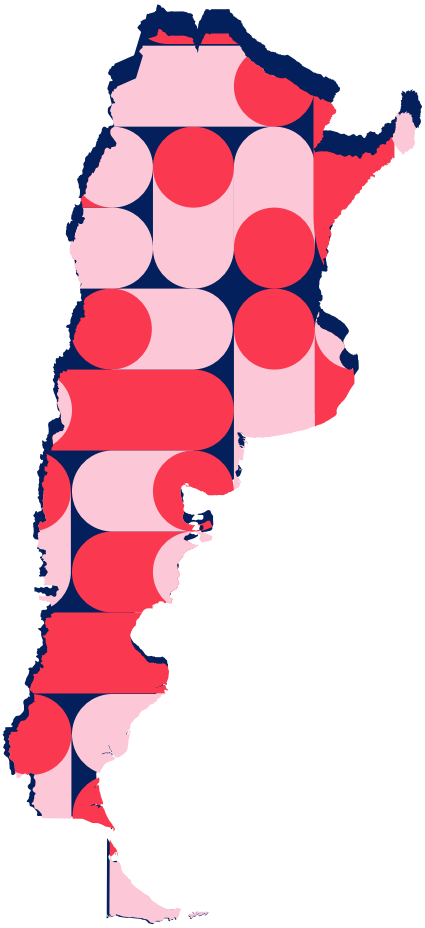
A nivel nacional, la protección de datos personales está prevista en la Constitución Nacional y en la Ley Nº 25.326 de Protección de Datos Personales, con su consecuente reglamentación en el Decreto Nº 1558/2001. El órgano de supervisión de la ley es la Agencia de Acceso a la Información Pública (AAIP)[47], un ente con autonomía funcional en el ámbito de la Jefatura de Gabinete de Ministros que también es responsable por controlar la

46 La información presentada en el análisis de cada país fue ofrecida por las mismas organizaciones encargadas de la recolección de información sobre las iniciativas tecnológicas desplegadas durante la pandemia de COVID-19 en cada país.

47 Desde enero de 2021, el cargo de Director de la AAIP se encuentra vacante. El 23 de marzo de 2021 se realizó una audiencia pública en la que se discutió la candidatura propuesta por el Poder Ejecutivo para ocupar el cargo. Ante críticas e impugnaciones recibidas por organismos de la sociedad civil alegando falta de idoneidad del candidato, el Ejecutivo no confirmó su designación, por lo que deberá presentar una nueva candidatura.

implementación de la Ley N° 27.275 de Acceso a la Información Pública y su Decreto Reglamentario N° 206/2017. La autoridad forma parte de la Red Iberoamericana de Protección de Datos (RIPD), que desde 2003 agrupa a representantes de las autoridades de control en materia de protección de datos personales y áreas afines de los gobiernos nacionales y subnacionales de los países de Iberoamérica. La RIPD cuenta con 16 autoridades de protección de datos nacionales miembro, 18 autoridades observadoras, entre estas últimas el Supervisor Europeo de Protección de Datos (EDPS); Organización de Estados Americanos (OEA) y Comité Consultivo del Convenio 108 del Consejo de Europa[48]. En 2017 fueron elaborados por la red los Estándares de Protección de Datos Personales para los Estados Iberoamericanos, que han servido desde entonces como marco de referencia en los procesos legislativos de la región.

En relación al procesamiento de datos personales por parte de entes públicos, la normativa al respecto determina que el consentimiento no será necesario cuando los datos se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal (artículo 5 inciso 2.b). Además, el consentimiento para ceder el tratamiento de datos personales no será exigible cuando se realice entre dependencias de los órganos del Estado en forma directa, en la medida del cumplimiento de sus respectivas competencias.



La Ley N° 25.326 también indica que ninguna persona puede ser obligada a proporcionar datos sensibles, y que éstos sólo pueden ser recolectados y objeto de tratamiento cuando medien razones de interés general autorizadas por ley (artículo 7 incisos 1 y 2). Lo mismo se aplica para razones de salud pública, de emergencia o para la realización de estudios epidemiológicos cuando se trata de datos personales relativos a la salud. En este caso, es necesario que se preserve la identidad de las titulares de los datos mediante mecanismos de disociación (artículo 11 incisos 3.c y 3.d).

48 Composición a marzo de 2021.

Durante la pandemia fueron dictadas algunas normas administrativas relacionadas a la protección de datos personales, como la Decisión Administrativa N° 431 del 22 de marzo de 2020 de Jefatura de Gabinete de Ministros, que requiere a las distintas jurisdicciones, entidades y organismos de la Administración Pública Nacional que transfieran, cedan o intercambien entre sí datos e información con fin de realizar acciones útiles para la protección de la salud pública, durante la vigencia de la emergencia sanitaria.

La Resolución N° 48 de fecha 28 de marzo de 2020, del Ministerio del Interior, implementó el "***Certificado Único Habilitante para Circulación – Emergencia COVID19", y señala que se "efectuarán los intercambios de información que resulten necesarios con organismos y entidades públicas y privadas para corroborar la veracidad de los datos consignados al momento de tramitar el 'Certificado Único Habilitante para Circulación – Emergencia COVID19', requiriendo el consentimiento del solicitante cuando fuera pertinente en el marco de lo previsto por la Ley N° 25.326 y modificatorias"*** (artículo 3). Si bien la implementación del certificado se mantiene, a través de la Decisión Administrativa N° 446 de fecha 1 de abril de 2020 de Jefatura de Gabinete de Ministros se deroga el citado artículo 3°.

Un marco normativo específico también acompañó el despliegue de la aplicación Cuidar, analizada en el marco de este informe, que tuvo por objeto obligar a su descarga por personas que ingresaran al país (Decisión Administrativa n.° 432 de 20 de marzo de 2020 y Disposición n.° 1771/20 de la Dirección Nacional de Migraciones) e incluyó la creación de una base de datos centralizada con los datos recogidos por la aplicación (Disposición N° 3 de 5 de mayo de 2020 de la Subsecretaría de Gobierno Abierto y País Digital).

Entre las normas administrativas dictadas durante la pandemia por Covid-19, podemos mencionar las siguientes:

La Decisión Administrativa N° 431 del 22 de marzo de 2020 de Jefatura de Gabinete de Ministros, requiere a las distintas jurisdicciones, entidades y organismos de la Administración Pública Nacional que transfieran, cedan o intercambien entre sí y bajo la supervisión de la "Unidad de Coordinación General del Plan Integral para la Prevención de Eventos de Salud Pública de Importancia Internacional", los datos e información que, por sus competencias, obren en sus archivos, registros, bases, o bancos de datos, con el único fin de realizar acciones útiles para la protección de la salud pública, durante la vigencia de la emergencia en materia sanitaria con motivo de la pandemia por coronavirus COVID-19.

Cabe destacar también la Disposición N° 10 de fecha 23 de julio de 2020 de

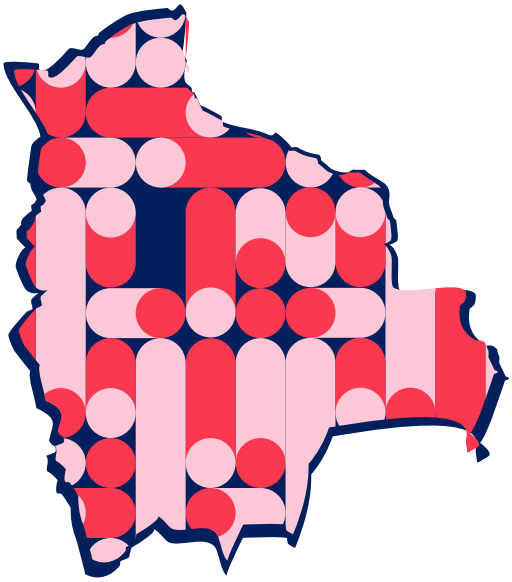
la Subsecretaría de Gobierno Abierto y País Digital que, entre otras medidas, crea cuatro bases de datos con relación a los respectivos Convenios suscritos entre el gobierno de la Provincia de Buenos Aires y de la Ciudad Autónoma de Buenos Aires, con el objeto de intercambiar información relacionada con casos sospechosos, confirmados o descartados de COVID-19 producida por la App, las aplicaciones provinciales y/o demás aplicaciones y/o sistemas de aplicación telefónica.
Con respecto a los plazos en materia de solicitud de acceso a la información pública, en un principio los plazos administrativos se encontraron suspendidos, en razón de lo dispuesto por el Decreto 298/2020, de fecha 19 de marzo de 2020 y sus prórrogas. Sin embargo, a través de la Resolución Nº 70/2020 con fecha 14 de abril de 2020, la Agencia de Acceso a la Información Pública exceptuó de la suspensión de los plazos a los pedidos de acceso a la información pública y a las acciones tendientes a la protección de datos personales.

Desde el ámbito judicial, se destaca en el marco de la pandemia la decisión del Superior Tribunal de Justicia de la Provincia de Jujuy del 9 de junio de 2020, por la que se suspende un Decreto provincial que autorizaba la recolección de datos personales mediante escaneo de documentos nacionales de identidad (DNI), la utilización de aplicaciones o "cualquier otro mecanismo de control" en razón de la pandemia.

La obligatoriedad del uso de aplicación móvil Cuidar hasta el momento no ha sido judicializada.

Bolivia

Bolivia es signataria de la mayor parte de los estándares internacionales de derechos humanos, como la Declaración Internacional de los Derechos Humanos, el Pacto Internacional de Derechos Civiles y Políticos, el Pacto Internacional de Derechos Económicos, Sociales y Culturales y la CADH. Sin embargo, no ha establecido otros compromisos específicos en materia de protección de datos personales.



Lo anterior es consistente con el hecho de que es uno de los pocos países de América Latina que carece de un marco normativo general a nivel nacional para la materia. Las disposiciones que se utilizan para garantizar la protección de datos personales derivan del derecho a la privacidad reconocido constitucionalmente

y de su jurisprudencia relacionada a la autodeterminación informativa. Algún nivel de protección a los datos personales se garantiza por medio del habeas data, también conocida como Acción de Protección de Privacidad. En todo caso, no existe una normativa que se encargue de establecer un régimen general de consentimiento para el tratamiento de datos desde el sector público.

En relación a datos de salud, se aplica lo dispuesto en la Norma Técnica para el Manejo del Expediente Clínico[49], contenida en la Resolución Ministerial N° 90 del 26 de febrero de 2008, que determina qué documentos relacionados al historial clínico de personas atendidas en los establecimientos de salud deben tener un manejo "escrupuloso" (artículo 5.1)". El artículo 21 de la misma norma establece que los expedientes clínicos son confidenciales y de manejo restringido "***al grupo de personas que tienen la responsabilidad directa del paciente y que deben estar claramente especificados***".

Con relación al derecho de acceso a la información pública, Bolivia lo reconoce constitucionalmente en el artículo 8.II, que concibe la transparencia como un valor del Estado. La transparencia es también un principio de la jurisdicción ordinaria conforme lo previsto en el *f* 180 de la Constitución y de la administración pública, de acuerdo al artículo 232 de la misma norma fundamental. La Constitución también prevé en el artículo 235 la obligación de "rendir cuentas sobre las responsabilidades económicas, políticas, técnicas y administrativas en el ejercicio de la función pública". Hay además diversas normas jurídicas que desarrollan el principio de transparencia, tales como: la Ley N° 341 de Participación y Control Social, que en su artículos 8.9 reconoce a la rendición de cuentas como parte del derecho de participación y control social; la Política Nacional de Transparencia y Lucha contra la Corrupción, aprobada mediante Decreto Supremo 0214 de 22 de julio de 2009, que en el artículo 2 dispone que todas las entidades e instituciones públicas deben trabajar por la transparencia en sus instituciones para prevenir y sancionar actos de corrupción, y el Decreto Supremo N.° 28.168 sobre la Transparencia en la Gestión Pública del Poder Ejecutivo[50].

Bolivia enfrentó sus primeros meses de pandemia bajo un gobierno interino que se encargó de tomar medidas para frenar la diseminación del COVID-19 en el país. Entre otras disposiciones preocupantes desde una perspectiva de derechos humanos, se dispuso la criminalización de la difusión de informaciones que pusieran en riesgo o afectara la salud pública[51]. De acuerdo con datos de organizaciones de la sociedad civil[52],

49 Ver http://saludpublica.bvsp.org.bo/cc/BOX.79/documentos/01049.pdf
50 Ver https://www.comunicacion.gob.bo/sites/default/files/docs/Decreto%20Supremo%20N%C2%BA%2028168%20Acceso%20a%20la%20Informacion_0.pdf

la medida derivó en la imputación de al menos 781 personas por delitos contra la salud pública y 273 procesos penales solamente en mes de abril del 2020. Al menos 83 de estos procesos, terminaron en condenas a partir de juicios abreviados, obteniendo sanciones de entre uno (1) y tres (3) años de prisión. Si bien estas disposiciones fueron derogadas más adelante como consecuencia de diversos pronunciamientos de organismos internacionales, el Estado no logró con ello revertir las vulneraciones causadas por la vigencia de los decretos, siendo para esto necesario revisar las condenas emitidas.

Brasil

Brasil reconoce los derechos a la privacidad y acceso a la información, así como los demás derechos humanos previstos en la Declaración Internacional de los Derechos Humanos, el Pacto Internacional de Derechos Civiles y Políticos, el Pacto Internacional de Derechos Económicos, Sociales y Culturales y la Convención Americana de Derechos Humanos. El país no ha firmado el Convenio 108, pero los Principios de la OCDE sobre Inteligencia Artificial.

sí

A nivel nacional, la Ley General de Protección de Datos[53] aprobada en el 2018 entró en vigencia en septiembre de 2020, ya durante la pandemia, e incluso estuvo en discusión su posible postergación hasta 2021[54]. La autoridad nacional de protección de datos recientemente creada por la ley aún no adhiere a la RIPD.

Los artículos 23 a 30 de la Ley N° 13.709/2018 disciplinan el procesamiento de datos personales por el sector público, que sólo puede ocurrir de acuerdo con las bases de tratamiento del artículo 7 y 11 de esta ley. Esto significa que el sector público puede procesar datos personales mediante el consentimiento, pero también en otros casos, como el de implementación de políticas públicas, sin necesidad de consentimiento –incluso para datos sensibles-. Hay un régimen especial en relación a la comunicación, o uso

51 Ver https://www.derechosdigitales.org/14611/in-support-of-freedom-of-expression-in-bolivia-we-request-the-abrogation-of-the-ds-4231/

52 Ver https://www.fundacionconstruir.org/wp-content/uploads/2020/10/Informe-Ind-Jud-y-Acceso-a-la-info-Bolivia-COVID-19.pdf

53 Ver https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

54 La Medida Provisional N° 959/2020 presentada por el Poder Ejecutivo intentó retrasar la entrada en vigor de la Ley hasta mayo de 2021, pero la propuesta no fue finalmente aprobada por el Congreso.

compartido, de datos personales entre entes públicos y privados.

De acuerdo con el artículo 5.II de la Ley General de Protección de Datos brasileña, los datos de salud son considerados datos personales sensibles. Eso significa que reciben una protección especial y solo pueden ser tratados mediante consentimiento de la titular o en los siguientes casos: a) para el cumplimiento de una obligación legal o reglamentaria por parte del responsable del tratamiento; b) para la ejecución, por parte de la administración pública, de políticas públicas previstas en leyes o reglamentos; c) para la realización de estudios por un organismo de investigación; d) para el ejercicio regular de derechos, incluso contractuales y en procedimientos judiciales, administrativos y de arbitraje. La ley también prevé que el tratamiento de datos –incluso sensibles– es legítimo cuando busque la protección de la vida o la seguridad física de la titular o de un tercero y para la tutela de la salud.

Durante la pandemia, el gobierno federal determinó, por medio de la Medida Provisional Nº 954/2020[55], que datos de consumidores de servicios de telecomunicaciones fueran compartidos con la autoridad estadística nacional, el Instituto Brasileño de Geografía y Estadística (IBGE), argumentando que la medida era necesaria para que el órgano pudiera desarrollar encuestas en el periodo. Sin embargo, expertos apuntaron a que la medida debilitaba los estándares de protección de datos adoptados en el país y exponía informaciones de millones de ciudadanos a medidas de vigilancia. La Suprema Corte Federal suspendió la vigencia de la medida, que finalmente tampoco fue aprobada por el Congreso. Según la Suprema Corte, a pesar de la gravedad de la pandemia de COVID-19, es necesario salvaguardar los derechos fundamentales consagrados en la Constitución. La decisión hizo referencia al Decreto 10.212/2020, que incorporó al ordenamiento jurídico brasileño la normativa sanitaria internacional de la Organización Mundial de la Salud (OMS), que impide el tratamiento de datos prescriptivos incompatibles con la finalidad de evaluación y gestión de riesgos sanitarios.

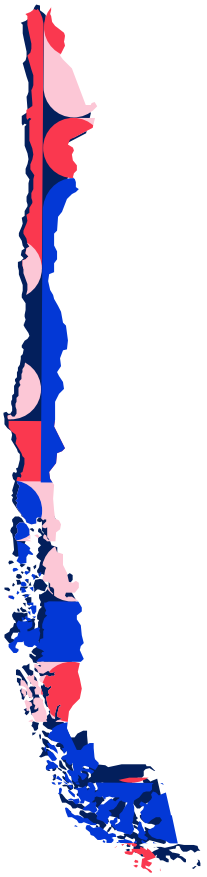
En relación al acceso a la información, la principal norma aplicable es la Ley de Acceso a la Información[56], Nº 12.527/2011. Durante la pandemia, el gobierno federal intentó restringir las reglas establecidas por la ley, suspendiendo el periodo legal de respuesta a solicitudes de acceso y restringiendo la posibilidad de cuestionamiento a respuestas negativas durante la emergencia sanitaria[57]. Sin embargo, fue impedido por una decisión de la Suprema Corte Federal de abril de 2020 que consideró que la medida iba en contra de los principios constitucionales de publicidad y

55 En Brasil, las medidas provisionales son actos del Poder Ejecutivo que posteriormente deben ser transformadas en ley por el Poder Legislativo.
56 Ver: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm.
57 Ver: https://br.okfn.org/2020/03/24/so-venceremos-a-pandemia-com-transparencia/.

transparencia[58]. En todo caso, el intento puede ser interpretado como parte de una serie de medidas del gobierno federal de Brasil por fragilizar las garantías de acceso a la información desde 2019.

Chile

Chile adhiere a los principales estándares internacionales de derechos humanos, como son la Declaración Internacional de los Derechos Humanos, el Pacto Internacional de Derechos Civiles y Políticos, el Pacto Internacional de Derechos Económicos, Sociales y Culturales y la CADH. El país no ha firmado a la fecha el Convenio 108 del Consejo de Europa sobre protección de datos personales, pero ha adoptado los Principios de la OCDE sobre Inteligencia Artificial.

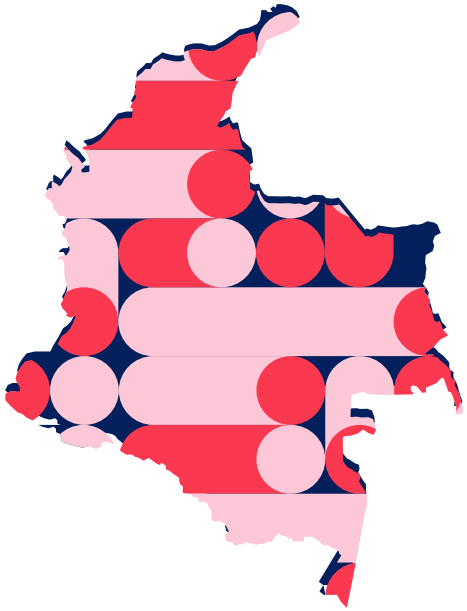


El país posee desde 1999 una normativa general de datos personales, la Ley N° 19.628 sobre protección de la vida privada, pero no cuenta con una autoridad de protección de datos personales. El Consejo para la Transparencia, órgano encargado del acceso a la Información Pública, tiene una competencia limitada de supervisión y recomendación respecto del uso de datos personales por los órganos públicos y es miembro de la RIPD. El régimen general para el tratamiento de datos por parte del sector público consta del artículo 20 de la ley de protección de datos personales, que determina que solamente es procedente respecto de las materias de competencia del servicio público y respetando las reglas de la ley (incluyendo los principios de finalidad, calidad, necesidad y legalidad). No se requiere consentimiento en esos casos. Fuera de ellos, aplican las reglas generales. Cuando se trata de datos de salud, como en otros países, ellos son considerados sensibles y como tales no pueden ser objeto de tratamiento salvo si hay autorización legal expresa, consentimiento, o para el otorgamiento de beneficios de salud (artículo 10).

En materia de acceso a la información, Chile dispone de la Ley N° 20.285 sobre acceso a la información pública, también conocida como "Ley de transparencia". Durante la pandemia, el Consejo para la Transparencia reguló la forma de responder como órgano a las obligaciones de transparencia flexibilizando los plazos de respuesta[59].

58 Ver: https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=442475&ori=1.
59 Ver: https://www.consejotransparencia.cl/ante-emergencia-sanitaria-cplt-flexibiliza-plazos-de-cumplimiento-de-obligaciones-de-transparencia/

Colombia



Colombia adhiere a la Declaración Internacional de los Derechos Humanos, el Pacto Internacional de Derechos Civiles y Políticos, el Pacto Internacional de Derechos Económicos, Sociales y Culturales y la CADH. El país también ha firmado los Principios de la OCDE sobre Inteligencia Artificial, aunque no ha adoptado el Convenio 108 del Consejo de Europa.

A nivel nacional la Ley Estatutaria de Protección de Datos[60], Ley N° 1.581 de 2012, y el Decreto Reglamentario N° 1.377 de 2013[61] definen las reglas para la protección de datos personales. La autoridad nacional responsable por supervisar la aplicación del marco normativo en la materia es miembro de la RIPD.

La autorización para el procesamiento de datos personales debe, por regla general, ser expresa. Salvo en los casos en que el consentimiento no sea necesario, lo que puede incluir varios escenarios en los que la persona se relaciona con el Estado (artículo 10), entre ellos el registro civil, cuando así lo requiere una entidad pública en ejercicio de sus funciones legales, cuando así lo ordena una autoridad judicial o cuando el tratamiento está autorizado por la ley para fines históricos, estadísticos o científicos. Lo mismo también es válido en casos de urgencia médica o sanitaria.

Durante la pandemia, las disposiciones anteriores han sido interpretadas en forma distorsionada por diversas entidades públicas para ampliar los ámbitos de excepción, y no pedir el consentimiento para proceder directamente al tratamiento de datos personales. Sin embargo, expertos apuntan[62] que la interpretación debe ser restrictiva, lo que quiere decir que se aplicada caso a caso y no como regla general.

Con relación al acceso a la información las leyes N° 1.712 de 2014[63] y N° 1.755 de 2015[64] sobre el derecho de petición regulan la materia. Durante la pandemia se expidió por el Ejecutivo el Decreto Legislativo N° 491 de 2020[65],

60 Ver: http://www.secretariasenado.gov.co/senado/basedoc/ley_1581_2012.html 59
61 Ver: http://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Decretos/1276081
62 Ver: https://www.ambitojuridico.com/noticias/analisis/constitucional-y-derechos-humanos/la-excepcion-que-fue-regla-el-consentimiento-en
63 Ver: http://www.secretariasenado.gov.co/senado/basedoc/ley_1712_2014.html
64 Ver: https://secretariageneral.gov.co/transparencia/marco-legal/normatividad/ley-1755-2015
65 Ver: https://dapre.presidencia.gov.co/normativa/normativa/Decreto-491-28-marzo-2020.pdf

que en su artículo 6 amplió los plazos para dar respuestas a peticiones ciudadanas mientras dure la emergencia sanitaria. El Decreto fue analizado por la Corte Constitucional que declaró la constitucionalidad de la extensión de plazos[66].

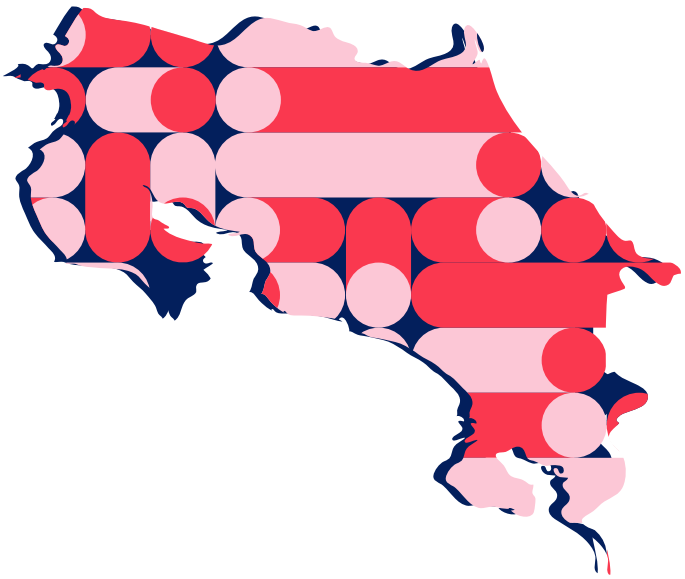
Costa Rica

Costa Rica, como otros países, adhiere a la Declaración Internacional de los Derechos Humanos, el Pacto Internacional de Derechos Civiles y Políticos, el Pacto Internacional de Derechos Económicos, Sociales y Culturales y la CADH, así como ha firmado los Principios de la OCDE sobre Inteligencia Artificial.

El país cuenta con la Ley Nº 8.968, de Protección de la Persona frente al Tratamiento de sus Datos Personales, y con la Agencia de Protección de Datos de los Habitantes que es miembro de la RIPD. No hay medidas específicas relacionadas al tratamiento de datos por parte del sector público o al tratamiento de datos de salud.

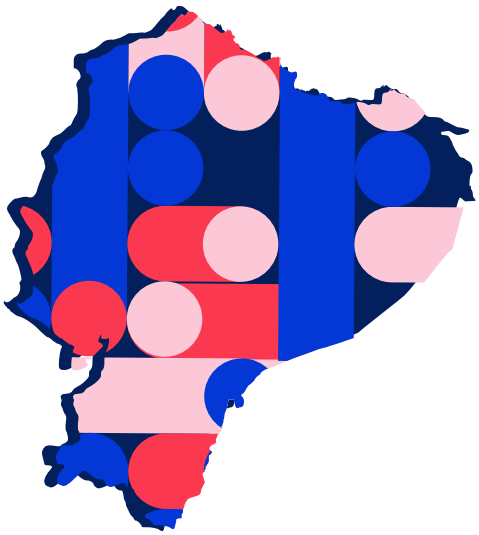
Por otro lado, no existe una normativa general de acceso a la información pública, aunque la constitución lo reconozca como derecho en sus artículos 27 y 30. Este derecho es regulado dependiendo de la materia por cada sector.

No se han emitido en pandemia normas específicas que alteren los regímenes generales de protección de datos o el derecho de acceso a la información.



66 Ver: https://www.corteconstitucional.gov.co/relatoria/2020/C-242-20.htm

Ecuador



Ecuador reconoce los principales estándares en materia de derechos humanos a nivel internacional, como la Declaración Internacional de los Derechos Humanos, el Pacto Internacional de Derechos Civiles y Políticos, el Pacto Internacional de Derechos Económicos, Sociales y Culturales y la CADH. No es parte del Convenio 108 sobre protección de datos y tampoco ha firmado los Principios de la OCDE sobre inteligencia artificial.

Recientemente, en mayo de 2021, Ecuador aprobó su Ley Orgánica de Protección de Datos, normativa presentada a la Asamblea Nacional en septiembre del 2019. Durante el periodo analizado por el OCCA, tal derecho era regido principalmente a partir de garantías constitucionales. En ese sentido, el artículo 66, incisos 11 y 19 establece la reserva de la información personal, incluida aquella relativa a los datos de salud, que solo pueden ser difundidos por mandato legal o autorización personal. El inciso 19 dice explícitamente que "***el derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley***."

Según la Ley del Sistema Nacional de Registro de Datos Públicos, Ley Nº 162, vigente en el periodo de esta investigación, datos de carácter personal presentes en las bases y registros públicos son de carácter confidencial y su acceso solo es posible con autorización expresa de la titular, por mandato de la ley u orden judicial (artículo 6). En relación a los datos de salud, la Ley de Derechos y Amparo del Paciente[67] en sus artículos 2 y 4 establece el derecho a la atención digna y a la confidencialidad de la información en salud[68], lo que se refuerza en el artículo 61 de la Ley Orgánica de Salud que obliga a las instituciones y profesionales de la salud a garantizar la confidencialidad de la información entregada y recibida.

En relación al acceso a la información, Ecuador dispone de la Ley Orgánica de Acceso a la Información[69].

67 Ver: http://instituciones.msp.gob.ec/dps/zamora_chinchipe/images/stories/LEY%20DE%20DERECHOS%20Y%20AMPARO%20AL%20PACIENTE.pdf

68 Ver: https://www.salud.gob.ec/wp-content/uploads/2017/03/LEY-ORG%C3%81NICA-DE-SALUD4.pdf.

69 Ver: https://www.redipd.org/sites/default/files/inline-files/ley_organica_de_acceso_a_la_informacion_en_ecuador.pdf

Durante la pandemia, el artículo 11 del Decreto N° 1.017[70] del Presidente del Ecuador que declaró el Estado de Excepción por calamidad pública el 16 de marzo de 2020, autorizó el uso de plataformas satelitales y de telefonía móvil para monitorear la ubicación de personas en estado de cuarentena sanitaria y aislamiento obligatorio e identificar aquellas que incumplieran con las restricciones impuestas para ponerlas a disposición de las autoridades judiciales y administrativas competentes.

Desde el ámbito judicial, el Dictamen N° 3-20-EE-20[71] de la Corte Constitucional, de 29 de junio de 2020, se refiere al "derecho a la libertad de expresión e información y la obligación del Ejecutivo de presentar datos claros, contrastados y certeros sobre la crisis". La Corte recalca "***la importancia de la obligación del Ejecutivo y subsidiariamente del COEN, en el manejo y producción de información que se entrega a la ciudadanía***". El documento continúa siguiendo lo señalado por la CIDH en su Resolución N° 1/2020 "Pandemia y Derechos Humanos en las Américas", de 10 de abril de 2020, sobre la importancia de la difusión de información en una sociedad democrática y la necesidad de garantizar el acceso a datos sobre la pandemia a la población y "desarrollar medidas positivas para reducir de manera rápida la brecha digital que enfrentan los grupos vulnerables y con menores ingresos". En esa línea la medida determina que no se podrá justificar la imposición de restricción y, por el contrario, se deberá asegurar el derecho de todas las personas de acceder a la información pública en el marco de la emergencia generada por el COVID-19.

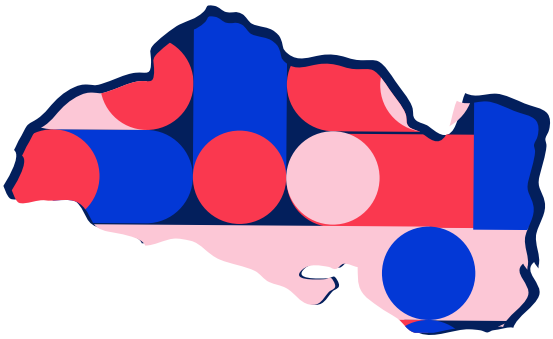
Además indica que debe darse prioridad a "solicitudes de acceso a la información relacionadas con la emergencia de salud pública, así como informar proactivamente, en formatos abiertos y de manera accesible a todos los grupos en situación de vulnerabilidad, de forma desagregada sobre los impactos de la pandemia y los gastos de emergencia, desagregados de acuerdo con las mejores prácticas internacionales".

Sobre la protección de la privacidad, el mismo Dictamen indica que las medidas adoptadas en contexto de pandemia no podrán vulnerar el derecho a la privacidad y los datos personales de las personas, principalmente información sensible. Y que se deberá obtener el consentimiento para recabar y compartir datos personales mientras dure la emergencia.

70 Ver: https://www.defensa.gob.ec/wp-content/uploads/downloads/2020/03/Decreto_presidencial_No_1017_17-Marzo-2020.pdf
71 Ver: https://www.asobanca.org.ec/sites/default/files/Dictamen%20No.%203-20-EE-20.pdf

El Salvador

El Salvador adhiere a la Declaración Universal de Derechos Humanos, el Pacto Internacional de Derechos Civiles y Políticos, el Pacto Internacional de Derechos Económicos, Sociales y Culturales y la CADH. No es parte del Convenio 108 sobre protección de datos y tampoco ha firmado los Principios de la OCDE sobre inteligencia artificial.



A nivel nacional no hay una normativa de protección de datos vigente en el país. La Constitución garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen y establece la indemnización, conforme a la ley, por daños de carácter moral[72].

En materia de acceso a la información, la ley nacional fue promulgada por el Decreto N° 534, de 30 de marzo de 2011 que se refiere a la protección de datos en su artículo 24, que trata de las informaciones confidenciales y determina que éstas incluyen la "*referente al derecho a la intimidad personal y familiar, al honor y a la propia imagen, así como archivos médicos cuya divulgación constituiría una invasión a la privacidad de la persona", "la entregada con tal carácter por los particulares a los entes obligados, siempre que por la naturaleza de la información tengan el derecho a restringir su divulgación", "los datos personales que requieran el consentimiento de los individuos para su difusión*", entre otras[73].

La ley regula además en su artículo 31 una mínima protección de datos personales al garantizar el derecho de acceso a éstos: "*toda persona, directamente o a través de su representante, tendrá derecho a saber si se están procesando sus datos personales; a conseguir una reproducción inteligible de ella sin demora; a obtener las rectificaciones o supresiones que correspondan cuando los registros sean injustificados o inexactos y a conocer los destinatarios cuando esta información sea transmitida, permitiéndole conocerlas razones que motivaron su petición, en los términos de esta ley. El acceso a los datos personales es exclusivo de su titular o su representante*".

Aunque no existe una normativa de protección de datos que se encargue de establecer un régimen general de consentimiento para el tratamiento de datos desde el sector público, el artículo 25 de Ley de Acceso a la

72 Ver: https://www.gobernacion.gob.sv/wp-content/uploads/2015/10/CONSTITUCION-de-la-Rep%C3%BAblica-de-El-Salvador.pdf

73 Ver: https://www.asamblea.gob.sv/sites/default/files/documents/decretos/171117_073009410_archivo_documento_legislativo.pdf

Información Pública se refiere al Consentimiento de la Divulgación señalando "***los entes obligados no proporcionarán información confidencial sin que medie el consentimiento expreso y libre del titular de la misma***".

Los artículos 19 y 20 de la Ley de deberes y derechos de los pacientes y prestadores de servicios de salud, por otro lado, establecen los derechos de privacidad y confidencialidad de la paciente en el artículo 19 –que afirma que a las pacientes se le garantizará la privacidad e intimidad durante su exploración clínica y estadía hospitalaria– y el artículo 20, referente al derecho de la paciente de que se respete el carácter confidencial de los expediente clínico y toda la información relativa al diagnóstico, tratamiento, estancia, pronósticos y datos de enfermedad o padecimiento[74]. Las excepciones a la confidencialidad son la existencia de una autorización escrita del mismo o de razones legales o médicas imperiosas por la divulgación de la información.

Por su parte la Norma Técnica de Expediente Clínico regula la forma de acceso al expediente clínico, incluyendo el caso de solicitudes por autoridad[75]. Además establece controles de acceso y seguridad en otras disposiciones.

Con relación al acceso a la información pública, aunque no se trate propiamente de un régimen diferenciado, la Ley de Protección Civil, Prevención y Mitigación de Desastres incorpora la obligación para el Director de Protección Civil, de divulgar en los medios de comunicación social boletines de alerta o de avisos importantes a la comunidad (artículo 31) y el derecho de todas las personas a recibir información sobre la inminencia o eventual ocurrencia de un desastre (artículo 35).

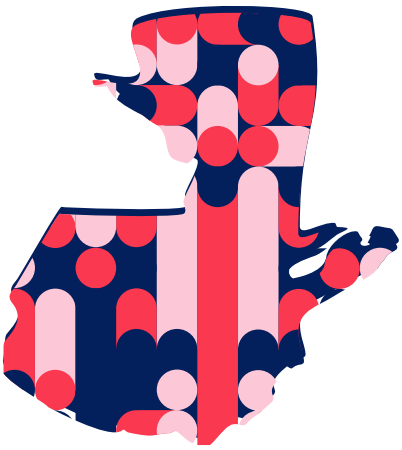
Durante la pandemia, se dictó el Decreto Legislativo Nº 599 que implicó la suspensión de los plazos establecidos en la Ley de Acceso a la Información Pública. Desde una perspectiva positiva, el Instituto de Acceso a la Información Pública emitió "Directrices para el cumplimiento de obligaciones de transparencia y protección de datos personales durante la emergencia sanitaria[76]" y la "Directriz sobre rendición de cuentas emergencia nacional por la pandemia del Covid-19[77]", con las cuáles se pretendía mantener el derecho de acceso a la información pública y la protección del derecho a la autodeterminación informativa en época de emergencia. Aunque estos instrumentos recalcan las obligaciones ya contempladas en la Ley de Acceso a la Información Pública, en ellas se hace un llamado a los entes

74 Ver: https://rrhh.salud.gob.sv/files/webfiles/regulacion/ley_derecho_pacientes.pdf
75 Ver: http://asp.salud.gob.sv/regulacion/pdf/normanormatecnicaconformacioncustodiaconsultaexpedienteclinico.pdf
76 Ver: https://www.mh.gob.sv/downloads/pdf/700-UAIP-DC-2020-11862.pdf
77 Ver: https://www.transparencia.gob.sv/institutions/mag/documents/356161/download

obligados a adoptar medidas para mantener activos en todo momento los canales electrónicos para la atención de solicitudes de información pública, así como el uso de medios tradicionales para la difusión masiva de la información.

La decisión más importante en materia judicial fue pronunciada por la Sala de lo Constitucional, mediante Sentencia de inconstitucionalidad I_21-2020[78], en la cual se declararon inconstitucionales dos Decretos Legislativos, 12 Decretos Ejecutivos y 1 Resolución Ministerial que fueron emitidos para regular el Estado de Excepción como respuesta a la pandemia. Dentro de la resolución, en la página 43, en el numeral 5.A., la Sala, al referirse a la suspensión de los derechos a la libertad de expresión, información y acceso a la información pública, retomó lo señalado en el párrafo 32 de la Resolución 1/2020 de la CIDH, referente al aseguramiento del derecho de acceso a la información pública. Con mayor énfasis, en la página 26, la Sala señaló: ***"La situación de emergencia no supone la inobservancia de las autoridades para cumplir con la eficacia del acceso a la información pública, pues éste, además de ser un derecho fundamental ya reconocido por esta sala, se vuelve más imperioso de ser protegido en situaciones de emergencia, en las cuales la violación de los derechos fundamentales puede agravar su situación de vulnerabilidad ante actos del estado o de particulares. Especial protección supone, además, el uso de los bienes y los fondos públicos."***

Guatemala



Guatemala, como la mayoría de los países de la región, adhiere a la Declaración Universal de Derechos Humanos, el Pacto Internacional de Derechos Civiles y Políticos, el Pacto Internacional de Derechos Económicos, Sociales y Culturales y la CADH. No es parte del Convenio 108 sobre protección de datos y tampoco ha firmado los Principios de la OCDE sobre inteligencia artificial.

A nivel doméstico no hay una ley general de protección de datos y la Constitución hace escueta referencia al derecho a la intimidad en el artículo 25[79]. El artículo establece, también como en otros países latinoamericanos, el derecho de acceso a archivos y registros estatales, que establece los derechos de las personas de conocer lo que de ella conste en archivos, fichas o cualquier otra forma de registros estatales, y la finalidad a que se dedica esta información, así como a

78 Ver: https://www.jurisprudencia.gob.sv/pdf/I_21-2020.pdf
79 Ver: https://www.ine.gob.gt/archivos/informacionpublica ConstitucionPoliticadelaRepublicadeGuatemala.pdf

corrección, rectificación y actualización. La norma explícitamente prohíbe el registro y la creación de archivos sobre filiación política por parte del Estado, excepto los propios de las autoridades electorales y de los partidos políticos.

Por otra parte la Ley de Acceso a la Información Pública regula en su artículo 31 el "Consentimiento expreso" conforme al cual los órganos públicos "no podrán difundir, distribuir o comercializar los datos personales contenidos en los sistemas de información desarrollados en el ejercicio de sus funciones, salvo que hubiere mediado el consentimiento expreso por escrito de los individuos a que hiciere referencia la información". La disposición además prohíbe la comercialización por cualquier medio de datos sensibles o datos personales sensibles.

Las excepciones al consentimiento serían, entre otras, necesidades de interés general previstas en ley, cuando los datos se transmitan entre sujetos obligados o entre dependencias y entidades del Estado, siempre y cuando los datos se utilicen para el ejercicio de facultades propias de los mismos, cuando exista una orden judicial o sea establecido por ley.

En lo relacionado a los datos de salud, el artículo 55 del Código de Salud que se refiere al acceso a servicios señala que "los establecimientos públicos y privados del Sector, deben proporcionar a los enfermos portadores de enfermedades transmisibles y de sus contactos, acceso al diagnóstico etiológico y a la atención de salud, en condiciones en que se respete su integridad personal y la confidencialidad del caso, sin detrimento de lo indicado en el Artículo 54[80]."

En materia de acceso a la información, el artículo 28 de la Constitución establece el derecho a petición y el artículo 30 la publicidad de los actos administrativos. El Decreto Nº 57-2008 aprueba la Ley de Acceso a la Información Pública[81].

En Guatemala no se dictaron normas especiales referentes a la protección de datos personales y acceso a la información pública durante la pandemia. No se suspendieron los plazos relativos a la Ley de Acceso a la Información Pública, de acuerdo al artículo 19 del Decreto Nº 12-2020, que declaró la Emergencia en ese país. Cuestión distinta es que dicho derecho haya sufrido, de facto, algunas restricciones.

80 Ver: http://www.cicad.oas.org/fortalecimiento_institucional/legislations/PDF/GT/decreto_congresional_90-97.pdf

81 Ver: https://www.minfin.gob.gt/images/laip_mfp/docs/decreto_5708b.pdf

México

México reconoce distintos marcos internacionales de protección de derechos humanos, como la Declaración Internacional de los Derechos Humanos, el Pacto Internacional de Derechos Civiles y Políticos, el Pacto Internacional de Derechos Económicos, Sociales y Culturales y la CADH.

El país dispone de una normativa unificada para la protección de datos personales y de una autoridad garante para la supervisión de su aplicación, que es miembro de la RIPD. Por regla general, no podrán tratarse datos personales sensibles, salvo que se cuente con el consentimiento expreso de su titular. Este consentimiento debe de darse de manera libre, específica e informada.

Para que las autoridades del sector público puedan permitir el acceso a información confidencial, requieren obtener el consentimiento de las particulares titulares de la información. Las autoridades no están obligadas a recabar el consentimiento por razones de seguridad nacional y salubridad general, o para proteger los derechos de terceros.

México también cuenta con una normativa de acceso a la información, que posee un régimen específico para situaciones de emergencia. Por regla general, el Ejecutivo Federal, los poderes ejecutivos de las Entidades Federativas, el Órgano Ejecutivo del Distrito Federal y los municipios tienen la obligación de poner a disposición del público y actualizar diversos tipos de información, incluyendo las disposiciones administrativas que realicen directamente o a través de la autoridad competente. Estas autoridades solo tendrán como excepción reservar la información respecto a diversas disposiciones administrativas si su difusión pueda comprometer los efectos que se pretenden lograr con la disposición o se trate de situaciones de emergencia.

Durante la pandemia a nivel federal se declaró la suspensión de plazos establecidos en las leyes federales en materia de transparencia, acceso a la información y protección de datos personales, excepto en los casos de autoridades que realizan actividades "esenciales" [82]_[83]. Dicha suspensión de plazos duró alrededor de 6 meses para las autoridades federales. A nivel

82 Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.
ACUERDO ACT-EXT-PUB/20/03/2020.02, disponible en: <https://www.dof.gob.mx/nota_detalle.php?codigo=5590620&fecha=27/03/2020>

83 Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.
ACUERDO ACT-PUB/30/04/2020.02, disponible en: <https://www.dof.gob.mx/nota_detalle.php?codigo=5593419&fecha=15/05/2020>

local, el lapso de la suspensión de plazos establecidos fue diferenciado de acuerdo a la evolución de la pandemia en cada localidad. El acceso a la información fue afectado por la suspensión de plazos en varios casos incluso después de que estos fuesen reanudados debido al retraso de algunos procesos.

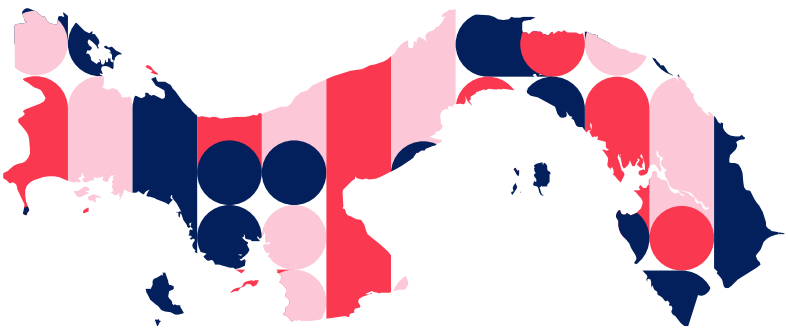
Panamá

Panamá adhiere a la Declaración Internacional de los Derechos Humanos, el Pacto Internacional de Derechos Civiles y Políticos, el Pacto Internacional de Derechos Económicos, Sociales y Culturales y la CADH. No es parte del Convenio 108 sobre protección de datos y tampoco ha firmado los Principios de la OCDE sobre inteligencia artificial.

Desde el punto de vista de la protección de datos personales, su autoridad garante es miembro de la RIPD – aunque la Ley N° 81 de 2019 sobre la protección de datos, haya entrado en vigencia solamente en marzo de 2021, o sea, durante la pandemia.

Con relación a las condiciones de consentimiento para el tratamiento de datos desde el sector público, la Ley de Protección de Datos Personales establece que el consentimiento debe ser expreso, claro e inequívoco, pero que no será exigido cuando los datos sean necesarios para la Administración Pública o para fines estadísticos o históricos, entre otras excepciones previstas en su artículo 8. La legislación panameña no menciona explícitamente cómo debe ser el consentimiento en los datos personales relativos a la salud, pero la ley de protección de datos personales puede ser aplicada supletoriamente a falta de norma regulatoria en el sector salud.

En materia de acceso a la información, la Ley N° 06 de 2002 es la que dicta las reglas correspondientes, la cual no sufrió suspensiones ni modificaciones durante la pandemia.



Paraguay

Paraguay reconoce los principales estándares en materia de derechos humanos a nivel internacional, como la Declaración Universal de Derechos Humanos, el Pacto Internacional de Derechos Civiles y Políticos, el Pacto Internacional de Derechos Económicos, Sociales y Culturales y la CADH. El país firma además el Convenio 108 y los Principios de la OCDE sobre inteligencia artificial.

A pesar de eso, el país no cuenta todavía con una ley general unificada para la protección de datos personales. Entre las normas sectoriales que protegen este derecho están la Ley N° 6534/2020 de Protección de Datos Personales Crediticios, que derogó la Ley N° 1682/2001 que reglamentaba la información de carácter privado y sus leyes modificatorias. Ella define en su artículo 3 el concepto de consentimiento como toda manifestación de voluntad libre, específica, informada e inequívoca que autoriza el tratamiento de datos personales por parte de la titular. El artículo 6, por su vez, reconoce el derecho de las personas de ser informadas sobre ***"la finalidad que se dará a los datos personales requeridos sobre ella, a fin de manifestar expresamente su consentimiento para la obtención y utilización de sus datos personales, el cual deberá ser expreso e inequívoco, en condiciones que no admitan dudas de su otorgamiento y deberá constar de manera escrita, electrónica, digital u otro mecanismo fehaciente"***. La ley también reconoce que el "consentimiento podrá ser revocado de forma expresa en las mismas condiciones y a título gratuito" y que el acto tendrá efecto retroactivo.

Con relación a los datos de salud, la Resolución S.G. N° 146/2012 del Ministerio de Salud es relevante, una vez que en su artículo N° 4 determina que ***"el personal de salud tiene la obligación de respetar y de proteger los derechos a la intimidad y a la privacidad de las personas, por lo que en los servicios de salud queda terminantemente prohibido filmar o fotografiar a usuarios sin su consentimiento"***. El artículo 6, por su vez, establece que ***"todo personal de salud está obligado a respetar el carácter confidencial de la información y datos de todas las personas que reciben una atención en salud o acuden para recibir información y orientación en un servicio de salud, y por tanto, garantizar el secreto profesional".***

En materia de acceso a la información, es la Ley N° 5282 de Libre Acceso Ciudadano a la Información Pública y Transparencia Gubernamental la que establece las reglas aplicables. Si bien la ley no establece un régimen especial para contextos de emergencia, se ha utilizado la clasificación de

"información pública reservada" para restringir el acceso a ciertos tipos de información.

En el contexto de la pandemia de COVID-19, el Poder Judicial ha determinado que declaraciones juradas vinculadas a la Ley de Emergencia serán públicas[84]. En una línea parecida, la Dirección Nacional de Contrataciones Públicas de Paraguay ha creado un sistema de alertas tempranas a través del seguimiento en tiempo real de cada una de las compras de emergencia por medio de la publicación de datos abiertos sobre contrataciones[85].

Perú

Perú adhiere a la Declaración Internacional de los Derechos Humanos, el Pacto Internacional de Derechos Civiles y Políticos, el Pacto Internacional de Derechos Económicos, Sociales y Culturales y la CADH. A nivel nacional cuenta con una normativa general para la protección de datos, la Ley Nº 29733, Ley de Protección de Datos Personales, reglamentada por el Decreto Supremo 003-2013-JUS. El país tiene además una autoridad nacional de protección de datos, que es miembro de la RIPD.

Las disposiciones previstas en la Ley Nº 29733 no son aplicables para competencias asignadas exclusivamente por ley para entidades públicas referidas a la defensa nacional, seguridad pública, y para el desarrollo de actividades en materia penal para la investigación y represión del delito. En otras áreas de la gestión pública, el consentimiento no es requerido cuando el tratamiento de datos personales tiene como finalidad el ejercicio de las funciones de las entidades públicas en el ámbito de sus competencias. El consentimiento tampoco es necesario cuando haya razones de interés público previstas por ley.

El artículo 14 numeral 6 dispone que no se requiere consentimiento para el caso de tratamiento de datos personales referidos a la salud cuando el tratamiento sea necesario, en circunstancia de riesgo, para la prevención, diagnóstico y tratamiento médico o quirúrgico de la titular, siempre que dicho tratamiento sea realizado en establecimientos de salud o por profesionales en ciencias de la salud. También se exceptúa el consentimiento cuando deban tratarse por razones de salud pública, tales situaciones deben ser calificadas por el Ministerio de Salud. Finalmente, se

84 Ver: https://www.idea.org.py/2020/05/14/buena-noticia-para-la-transparencia/

85 Ver: https://www.open-contracting.org/es/2021/05/03/un-llamado-a-la-rendicion-de-cuentas-como-las-contrataciones-abiertas-pueden-contribuir-a-restablecer-la-confianza-publica-en-paraguay/

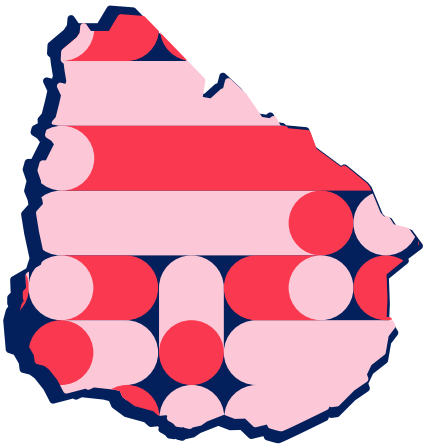
exceptúa para la realización de estudios epidemiológicos o análogos, en tanto se apliquen procedimientos de disociación adecuados.

En materia de acceso a la información, Perú cuenta con la Ley de Transparencia y Acceso a la Información Pública. La Ley no prevé un régimen diferenciado para situaciones de emergencia. Al contrario, el derecho de acceso a la información pública no se suspende cuando se decretan estados de excepción.

Durante la pandemia no se emitieron normativas específicas relacionadas a la protección de datos o el acceso a la información. Sin embargo, la Autoridad Nacional de Transparencia y Acceso a la Información Pública y de Protección de Datos Personales emitió opiniones consultivas sobre la materia. En ese sentido podemos mencionar la Opinión Consultiva 20-2020 sobre el acceso a la información pública en pandemia, que refuerza que el derecho de acceso a la información pública aún se puede ejercer en la situación de Estado de Emergencia no obstante que esta declaratoria genera una barrera fáctica al ejercicio regular del derecho de acceso a la información pública (al restringir la circulación en vías de uso público). Así, considera que será una afectación al derecho de acceso a la información pública si la entidad no entrega la información que se requiere no obstante haber implementado el trabajo remoto, contar con canales virtuales para la recepción de solicitudes de acceso a la información pública y se haya optado por el formato de entrega por correo electrónico.

La Opinión Consultiva 32-2020 indica que las empleadoras podrán tratar datos personales de las empleadas sin consentimiento cuando sean necesarios para garantizar la seguridad y salud en el trabajo con la finalidad de evitar la propagación de COVID-19. Asimismo, las trabajadoras se encuentran obligadas a cooperar y a brindar la información a la empleadora respecto al posible o real contagio que padezcan de COVID-19. La medida indicó que el tratamiento de datos personales de las trabajadoras que realice la empleadora con la finalidad de evitar la propagación de COVID-19 debe atender a lo establecido en la Ley de Protección de Datos Personales y su reglamento, en especial a los principios de finalidad, calidad, proporcionalidad y seguridad.

Uruguay



Uruguay reconoce los principales estándares de derechos humanos internacionales, como la Declaración Internacional de los Derechos Humanos, el Pacto Internacional de Derechos Civiles y Políticos, el Pacto Internacional de Derechos Económicos, Sociales y Culturales y la CADH. Además, forma parte del Convenio 108 y ha adoptado los Principios de la OCDE sobre Inteligencia Artificial.

A nivel nacional, Uruguay adoptó una ley general de protección de datos en 2008, la Ley Nº 18.331 de Protección de Datos Personales y Acción de Habeas Data, que fue actualizada en 2018 teniendo en cuenta los nuevos desarrollos tecnológicos y la evolución en las formas de tratamiento de los datos personales por medio de la Ley Nº 19.670. Su órgano garante, la Unidad Reguladora y de Control de Datos Personales (URCDP) forma parte de la RIPD.

Con relación al tratamiento de datos por parte de entes públicos, el artículo 9 determina como excepciones a la obligatoriedad de consentimiento, entre otras situaciones, que los datos se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal.

Cuando se trata de la comunicación de datos, el artículo 17 determina que los datos personales ***"sólo podrán ser comunicados para el cumplimiento de los fines directamente relacionados con el interés legítimo del emisor y del destinatario y con el previo consentimiento del titular de los datos, al que se le debe informar sobre la finalidad de la comunicación e identificar al destinatario o los elementos que permitan hacerlo".*** Sin embargo, las excepciones incluyen que "se trate de datos personales relativos a la salud y sea necesario por razones de salud e higiene públicas, de emergencia o para la realización de estudios epidemiológicos, en tanto se preserve la identidad de los titulares de los datos mediante mecanismos de disociación adecuados".

Cabe observar que, bajo la normativa uruguaya, los datos sensibles –que incluyen datos de salud– son considerados "especialmente protegidos". Además, el Decreto Nº 274/010, de septiembre de 2010, determina en el artículo 30 que la historia clínica será reservada y sólo podrán acceder a la misma las responsables de la atención a la salud de la paciente y el personal administrativo vinculado a dicha institución, la paciente o las personas que sean autorizadas por él o ella o el representante legal de la paciente declarada judicialmente incapaz. También se establece que ***"los***

servicios de salud y los trabajadores de la salud deberán guardar reserva sobre el contenido de la historia clínica y no podrán revelarlo a menos que fuere necesario para el tratamiento del paciente o mediare orden judicial". Sin embargo, la normativa establece la posibilidad de que el Ministerio de Salud Pública, incluyendo la Junta Nacional de Salud, pueden tener acceso a la historia clínica "cuando lo consideren pertinente".

En el marco de la pandemia, el Dictamen Nº 2/020 de la URCDP determina que el tratamiento de datos de salud puede realizarse sin previo consentimiento de las titulares. Tal norma fue publicada el mismo día del lanzamiento público de la aplicación analizada en Uruguay: el 20 de marzo de 2020[86].

Con relación al acceso a la información pública, la Ley Nº 18.381 de 2008[87], reglamentada por el Decreto Nº 232/010[88], establecen las reglas aplicables.

Entre las normativas con posible afectación al derecho de protección de datos personales y el acceso a la información aprobadas durante la pandemia se pueden destacar, además del Dictamen Nº 2/020 de la URCPD, el Decreto Nº 131/020, referente a un seguro por enfermedad profesional para trabajadoras de salud expuesta al riesgo de contagio por Covid-19 y que crea un registro de las profesionales en el Ministerio de Salud Pública. Según su artículo 2, sin embargo, "toda la información contenida en el Registro cumplirá con las disposiciones relativas a la protección de datos personales dispuestos en la Ley Nº 18.331 de 11 de agosto 2008 y normas complementarias". También cabe mencionar la Ley Nº 19.869, que establece los lineamientos generales para la implementación y desarrollo de telemedicina como prestación de los servicios de salud y que también determina que los datos personales transmitido y almacenados en el ámbito de los servicios de telemedicina deben ser tratados conforme lo establecido en la ley de protección de datos. Finalmente, la Ley Nº 19.932[89], restringió el derecho a la libre reunión.

86 Ver: https://www.presidencia.gub.uy/transparencia/ley-18_381
87 Ver: https://www.impo.com.uy/bases/decretos/232-2010
88 Ver http://impo.com.uy/bases/leyes-originales/19932-2020
89 Ver http://impo.com.uy/bases/leyes-originales/19932-2020

Análisis de las tendencias regionales desde los estándares del sistema interamericano

A. Legalidad

Las Resoluciones Nro. 1/20 y 4/20 de la CIDH establecen criterios de legalidad para el desarrollo de aplicaciones relacionadas con Covid-19. En nuestro análisis se destacan algunos puntos relacionados con el cumplimiento de estos estándares.

La Resolución Nº 1/20 de la CIDH indica que aún en los casos más extremos y excepcionales donde pueda ser necesaria la suspensión de determinados derechos, el derecho internacional impone una serie de requisitos, entre ellos el de legalidad, dirigidos a evitar que medidas como el estado de excepción o emergencia sean utilizadas de manera ilegal, abusiva y desproporcionada, ocasionando violaciones a derechos humanos o afectaciones del sistema democrático de gobierno[90]. En lo que respecta a limitaciones en el ejercicio de los derechos a la protección de datos personales o el acceso a la información, los decretos legislativos o administrativos en los cuales se fundan las declaraciones de estados de excepción constitucional decretados en la región, en general, no avanzaron en forma específica en satisfacer el requisito de legalidad de manera material y formal. Por ejemplo, en el caso de Ecuador, el artículo 11 del Decreto Nº 1.017[91] de la presidencia -citado más arriba- autorizó el uso de plataformas satelitales y de telefonía móvil para monitorear la ubicación de personas en estado de cuarentena sanitaria y aislamiento obligatorio e identificar aquellas que incumplieran con las restricciones impuestas para ponerlas a disposición de las autoridades judiciales y administrativas competentes. La orden administrativa impuso severas restricciones al ejercicio de la protección de datos personales y a la privacidad, sin encontrarse acompañada de un debate democrático al respecto a través de una norma de rango legal que pudiera determinar mecanismos de control sobre una restricción tan severa al ejercicio de derechos.

Por su parte los considerandos de la Resolución Nº 4/20 de la CIDH, ponen el acento en la obligación de los Estados de utilizar ***"el máximo de los recursos disponibles, así como que pueden enfrentar contextos de escasez de recursos y que, incluso en este supuesto, se encuentran obligados por las normas que derivan del derecho internacional de los derechos humanos y cualquier restricción debe ser debidamente justificada en términos de legalidad y proporcionalidad".*** Lo anterior invita a la reflexión

90 Resolución 1/20 CIDH, Par.3 letra g.
91 Ver: https://www.defensa.gob.ec/wp-content/uploads/downloads/2020/03/Decreto_presidencial_No_1017_17-Marzo-2020.pdf

acerca de cómo la situación de urgencia no puede ser una carta blanca a la inversión de recursos estatales, de suyo escasos, sin un debate legislativo democrático que permita aportar contrapeso a la evaluación de toma de decisiones administrativas sobre asignación de recursos en contexto de pandemia.

Además, las resoluciones también recomiendan que las aplicaciones, especialmente las que se refieren a la geolocalización, deben "informar debidamente la finalidad para la cual estos datos serán utilizados, el tipo de localización de la que serán objeto, y con cuáles autoridades sanitarias, empresas u otros usuarios se compartirá la información[92]". Este requisito tampoco fue seguido por algunos estados, con información poco clara sobre los derechos de las titulares o posible intercambio de datos con terceros. Conforme surge del análisis de transparencia, en la mayoría de las aplicaciones, tampoco se llevó a cabo una evaluación de impacto previa y pública. Solo Ecuador contó con la participación de la sociedad civil en el desarrollo y evaluación de la iniciativa. Además, solo Colombia, Ecuador y Uruguay prevén auditorías externas de aplicaciones.

La mayoría de los países analizados cuentan con leyes de protección de datos con un régimen especial de consentimiento para los datos de salud, considerándolos como "datos sensibles" o "datos especialmente protegidos", cuyo uso depende del consentimiento expreso de las interesadas. Algunos de estos países, como Argentina, Brasil, Chile, Uruguay y Colombia, no requieren el consentimiento de la titular ante una emergencia médica o un riesgo para la salud pública debidamente justificado. Lo mismo se defiende en la Resolución Nº 4/20 de la CIDH, por la cual cualquier tipo de tratamiento médico de las personas con Covid-19 debe asegurar el consentimiento previo, libre e informado de las personas afectadas. A pesar de ello, los requisitos para la obtención del consentimiento no se han cumplido en la mayoría de las aplicaciones estudiadas: menos de la mitad de las aplicaciones estudiadas cumplen con todos los requisitos.

Las relaciones entre el Estado y el sector privado son muchas veces oscuras y carecen de transparencia en cuanto a los términos de posibles acuerdos para el uso de tecnologías privadas. En la mayoría de los casos, no se sabe qué beneficios pueden tener estas empresas, ni se sabe si pueden acceder a los datos de población. Esto, nuevamente, pone en tela de juicio el cumplimiento de los estándares de la CIDH, que establece que los Estados deben, al contratar sistemas privados, "***asegurar que la tecnología contratada, incluidos los algoritmos, cumpla con los principios de no***

92 Resolución 4/20 CIDH, Par.34.

discriminación y auditar externa e independientemente el impacto que puede tener en los derechos humanos[93]*".*

Por último, resulta relevante el rol del principio de legalidad en su sentido formal, ya que a través de procesos legislativos accesibles a la ciudadanía los Estados entregan información valiosa sobre sus procesos de toma de decisiones. En situación de pandemia tales procesos no tuvieron lugar y las iniciativas aquí examinadas se desarrollaron por vía administrativa, lo que ha motivado algunos casos salientes en que los órganos jurisdiccionales han intervenido para poner de manifiesto la insuficiencia constitucional de las normas que fueron implementadas.

En Brasil, el Tribunal Constitucional (Supremo Tribunal Federal) suspendió la disposición de la Medida Provisional (MP) Nº 954/2020, que determinaba el compartimento de datos de las clientes de las empresas de telecomunicaciones con el IBGE (Instituto Brasileño de Geografía y Estatística). Según la Corte, los derechos fundamentales consagrados en la Constitución no fueron salvaguardados. También afirmó que el Decreto Nº 10.212/2020, que incorporó al ordenamiento jurídico brasileño la normativa sanitaria internacional de la Organización Mundial de la Salud (OMS), impide el tratamiento de datos prescriptivos incompatibles con la finalidad de evaluación y gestión de riesgos sanitarios.

En Ecuador, el Dictamen Nº 3-20-EE-20 de la Corte Constitucional, de 29 de junio de 2020, se refiere al "derecho a la libertad de expresión e información y la obligación del Ejecutivo de presentar datos claros, contrastados y certeros sobre la crisis" (6.5.2). La Corte recalca ***"la importancia de la obligación del Ejecutivo y subsidiariamente del COE N, en el manejo y producción de información que se entrega a la ciudadanía. Tan solo a partir de cifras y datos reales y públicos, la ciudadanía podrá comprender la magnitud de la situación, concienciar sobre los efectos de esta pandemia y cooperar en la mitigación del COVID-19***[94]***".***

El debate democrático requerido por el principio de legalidad en sentido material y formal ha sido un elemento ausente en el despliegue de políticas públicas que consideran el uso de tecnologías en la región, y la consecuencia directa son impactos perceptibles a la privacidad, protección de datos personales y acceso a la información por parte de la ciudadanía.

93 Resolución 4/20 CIDH, Par.37.
94 Ver: https://www.asobanca.org.ec/sites/default/files/Dictamen%20No.%203-20-EE-20.pdf

B. Necesidad

La Resolución Nº 1/20 de la CIDH previó en concreto que, en los casos más extremos y excepcionales en que fuera necesaria la suspensión de determinados derechos en la contención de la pandemia, los Estados debían atender el principio de legalidad, proporcionalidad, temporalidad y necesidad[95].

El principio de necesidad refiere, en concreto, a la adecuación de la limitación de un derecho que debe poder satisfacer los fines imperiosos que dice perseguir. Debe tratarse de una limitación adecuada, proporcionada e idónea[96]. Este juicio de necesidad requiere que la limitación propuesta haya sido evaluada de cara a otras que sean menos restrictivas e invasivas del derecho afectado, al tiempo que permita la realización del fin propuesto[97].

Su aplicación es extensible frente a las limitaciones del derecho de acceso a la información[98] así como a las limitaciones pretendidas al derecho de protección de datos[99], y que se desprenden de los artículos 13 y 11 de la Convención Americana de Derechos Humanos de la cual son parte los Estados examinados en este informe. Su aplicación debe además estar materializada en auténticas leyes, en un sentido material y formal[100]. Es el Estado quien debe sustentar que la limitación satisface con el principio de necesidad y aquellos otros que tornan legítima las limitaciones a los derechos comprendidos en la CADH.

En general, todos los Estados que impusieron limitaciones al derecho a la protección de datos y el acceso a la información como medidas comprendidas en el fin más abstracto de contención a la pandemia, lo hicieron a través de decisiones expedidas por el poder ejecutivo, o bien a

95 Resolución 1/20 CIDH, Par.3 letra g.

96 Comisión Interamericana de Derechos Humanos, Relatoría Especial para la Libertad de Expresión, Informe "Libertad de expresión e internet", OEA/Ser.L.V/II, CIDH/RELE/INF. 11/13, del 31 de diciembre de 2013, prr. 61. Disponible en:http://www.oas.org/es/cidh/expresion/docs/informes/2014_04_08_Internet_WEB.pdf

97 Comisión Interamericana de Derechos Humanos, Relatoría Especial para la Libertad de Expresión, Informe "Libertad de expresión e internet", OEA/Ser.L.V/II, CIDH/RELE/INF. 11/13, del 31 de diciembre de 2013, prr. 64. Disponible en:http://www.oas.org/es/cidh/expresion/docs/informes/2014_04_08_Internet_WEB.pdf

98 Comisión Interamericana de Derechos Humanos, Relatoría Especial para la Libertad de Expresión, Informe "El derecho de acceso a la información en el marco jurídico interamericano", OEA/sER.I/V/II, CIDH/RELE/INF.1/09, del 30 de diciembre de 2009, prr. 53. Disponible en: http://www.oas.org/es/cidh/expresion/docs/publicaciones/ACCESO%20A%20LA%20INFORMACION%20FINAL%20CON%20PORTADA.pdf

99 Informe del Comité Jurídico Interamericano CIJ, "Principios actualizados del Comité Interamericano sobre la privacidad y la protección de datos personales", principio tres titulado "pertinencia y necesidad". Disponible en: https://www.redipd.org/sites/default/files/2021-05/CJI-doc_638-21.pdf

100 Corte Interamericana de Derechos Humanos, Opinión Consultiva OC P-6/86, del 9 de mayo de 1986, prr 21 y ss. Disponible en: https://www.corteidh.or.cr/docs/opiniones/seriea_06_esp.pdf

través de decretos, disposiciones administrativas, resoluciones, dictámenes o disposiciones adicionales a decretos vigentes en materia de protección de datos o acceso a la información. Es decir, sin satisfacer el principio de legalidad en sentido material.

La exposición de motivos de las medidas que fueron dictadas en Ecuador, Uruguay, Chile, Brasil, Colombia y Argentina para la limitación de la protección de datos durante la emergencia sanitaria, así como las medidas que apuntaron a la limitación del derecho de acceso a la información expedidas por Colombia y Argentina se caracterizan, en general, por (i) la ausencia de las razones específicas por las que la limitación propuesta era adecuada, proporcionada e idónea, (ii) la ausencia de valoraciones sobre la existencia o no de alternativas menos invasivas para el ejercicio de dichos derechos, y (iii) la ausencia de alguna justificación suficiente sobre cómo la limitación propuesta permitía, en concreto, el logro de un fin concreto.

Bolivia, Panamá y Paraguay por su parte, fueron los únicos países que no expidieron regulación infralegal que apuntara a la limitación de ambos derechos, lo que no significa, en todo caso, que en la práctica no hayan limitado su alcance o ejercicio.

La tendencia entre los países que impusieron limitaciones al derecho a la protección de datos a través de normativa administrativa se caracteriza, a su vez, por (i) facilitar la compartición de datos del sector privado a entidades del sector público, o facilitar la compartición de datos entre entidades del sector público entre sí, así como por (ii) introducir excepciones al consentimiento informado.

La tendencia entre los países que limitaron el alcance o vigencia del derecho de acceso a la información se caracteriza, a su turno, por (i) la ampliación de los plazos de respuesta a las solicitudes de acceso a la información, (ii) o la suspensión total de los términos para proveer respuesta.

La ausencia de razones en cada caso que permitieran comprender por qué frente al derecho a la protección de datos la compartición abierta de datos o las excepciones al consentimiento eran medidas idóneas, adecuadas y proporcionales y cuál era el fin concreto que perseguían, distinto a la declaración abierta de "cuidado de la salud pública", dificulta el escrutinio sobre la valoración de las medidas impuestas y el proceso argumental que condujo a su imposición como única medida posible. Lo mismo sucede en el caso de las limitaciones impuestas frente al derecho de acceso a la información.

No se cuenta con información sobre cómo, en el transcurso de la pandemia, las medidas empleadas en cada caso fueron moduladas, justificadas con

posterioridad o convertidas en verdaderos cuerpos legales en sentido material y formal que permitieran, en el marco del debate democrático, entender la necesidad detrás de la vigencia de cada una.

Tampoco se cuentan con decisiones sancionatorias en firme en los países en los que existe una autoridad de protección de datos independiente que se refieran a la ausencia de valoración de la necesidad de cada limitación impuesta. Lo mismo sucede tratándose del derecho de acceso a la información: en los países en los que existe una agencia especializada en la materia no existen pronunciamientos que se refieran al respecto.

C. Proporcionalidad

I. Proporcionalidad en el balance de derechos

La definición de la medida de afectación de distintos derechos humanos que deben ser balanceados es siempre una cuestión de difícil determinación, por ello resulta interesante atender a la orientación provista por los principios del Comité Jurídico Interamericano sobre la privacidad y la protección de datos personales. Allí se plantea que **"*[e]n el contexto del Tratamiento de Datos del sector público, la idea de necesidad a veces se mide sobre la base de la proporcionalidad; por ejemplo, al exigir un equilibrio entre 1) el interés del público en el Tratamiento de los Datos Personales y 2) la protección de los intereses de las personas en materia de privacidad*[101]**"**.** Tal balance en el despliegue tecnológico en el contexto de la pandemia de COVID-19 en nuestra región parece lejos de estar anclado en evidencia concreta de cómo las tecnologías seleccionadas avanzan efectivamente en la satisfacción del interés público que las motiva, y dejan abiertas muchas interrogantes respecto a "intereses públicos" concurrentes no del todo develados.

El estudio realizado para el OCCA muestra escasa atención de parte de los gobiernos a la perspectiva de proporcionalidad. Aún cuando la Resolución 1/20 de la CIDH hizo un llamado directo a los Estados a guiar su actuación teniendo en consideración que: ***"[e]l objetivo de todas las políticas y medidas que se adopten deben basarse en un enfoque de derechos humanos que contemple la universalidad e inalienabilidad; indivisibilidad; interdependencia e interrelación de todos los derechos humanos; la igualdad y la no discriminación; la perspectiva de género, diversidad e interseccionalidad; la inclusión; la rendición de cuentas; el respeto al Estado de Derecho y el fortalecimiento de la cooperación entre los Estados*[102]***".**

La misma resolución avanza en definir los contornos de qué se entiende como proporcionado en el contexto de pandemia, llamando la atención a

101 Principios del Comité Jurídico Interamericano sobre la privacidad y la protección de datos personales, Anotados, página 13.
102 Resolución 1/20 CIDH, Par.3 letra e.

que "*[l]as medidas que los Estados adopten, en particular aquéllas que resulten en restricciones de derechos o garantías, deben ajustarse a los principios «pro persona», de proporcionalidad, temporalidad, y deben tener como finalidad legítima el estricto cumplimiento de objetivos de salud pública y protección integral, como el debido y oportuno cuidado a la población, por sobre cualquier otra consideración o interés de naturaleza pública o privada*[103]".

La información obtenida respecto de las tecnologías utilizadas en la región revela una total ausencia de estudios integrales en materia de impactos en el ejercicio de derechos fundamentales más allá de la consideración -por supuesto atendible, pero aislada- de utilizarlas como parte de la estrategia para garantizar el derecho a la salud de la población. Aunque algunos casos se destacan con relación a las garantías de protección de datos, como Argentina, Ecuador y Uruguay, los cuidados no se expanden de modo de abarcar el riesgo de afectación de otros derechos como la movilidad, libertad de expresión, derecho a reunión, o no discriminación en el ejercicio de derechos económicos y sociales (como empleo, educación, acceso a la salud, acceso a la seguridad social, entre otros).

Por su parte la Resolución Nº 4/20 de la CIDH prescribe en particular a los Estados la realización de "*una evaluación previa y pública del impacto que tienen en la privacidad de las personas afectadas por el virus las aplicaciones tecnológicas y herramientas de georreferenciación que se proyecten desarrollar para preservar la salud, a los efectos de justificar de forma fundada el beneficio de esas herramientas frente a otras alternativas que afecten en menor medida la privacidad. Asimismo, deberán prevenir la identificación selectiva de las personas y cuidar de que se recaben y utilicen los datos personales estrictamente necesarios para combatir la propagación de la COVID-19*". En su mayoría los Estados de la región han fallado en satisfacer este requisito cuando se trata de las iniciativas analizadas por este estudio, una vez que no se han encontrado evidencias de que se hayan realizado estudios de impacto en derechos humanos antes de su implementación. Del mismo modo, tal como se ha mencionado en los apartados anteriores, se observa una carencia de mecanismos de evaluación y auditorías técnicas externas.

Resulta interesante en este aspecto que la Resolución Nº 1/20 de la CIDH se refiere específicamente a que cuando resulten necesarias las limitaciones a DESCA, "*los Estados deben velar porque tales medidas estén plena y estrictamente justificadas, sean necesarias y proporcionales, teniendo en cuenta todos los derechos en juego y la correcta utilización de los máximos recursos disponibles*[105]". Ello porque contrario a esta directriz, las iniciativas

104 Resolución 4/20 CIDH, Par.35.

desarrolladas no fueron acompañadas en ningún caso de estudios técnicos o económicos que apoyaran la inversión de recursos públicos que ellas significaron, con datos concretos sobre la contribución al combate a la pandemia que ellas podían realizar, o las circunstancias de contexto de despliegue de conectividad, accesibilidad a dispositivos o habilidades de vinculación con la tecnología que debían acompañar su implementación para asegurar su efectividad.

Precisamente porque aquello que no se mide queda invisibilizado y excluido de la implementación de una política pública, todas las tecnologías desplegadas estudiadas fallan en satisfacer la directriz de la Resolución N° 1/20 de la CIDH en cuanto a ***"[i]ntegrar medidas de mitigación y atención enfocadas específicamente en la protección y garantía de los DESCA dado los graves impactos directos e indirectos que contextos de pandemia y crisis sanitarias infecciosas les pueden generar. Las medidas económicas, políticas o de cualquier índole que sean adoptadas no deben acentuar las desigualdades existentes en la sociedad[106]".***

Las tecnologías desplegadas destinan recursos importantes a su desarrollo, pero benefician mayoritariamente a los segmentos más afluentes de sus poblaciones que gozan de mejor acceso económico a la conectividad y cuentan con habilidades tecnológicas necesarias para el mejor uso de las aplicaciones o chatbots. Las poblaciones deficientemente conectadas, como grupos indígenas, adultos mayores, poblaciones rurales y migrantes, no se encuentran al centro de las soluciones desplegadas y el foco en estas tecnologías contribuye a acentuar las desigualdades preexistentes respecto de ellas, en una situación sanitaria que las pone en riesgo adicional.

II. Proporcionalidad en el tratamiento de datos personales

Dos materias fundamentalmente vinculadas a la proporcionalidad en la recogida y uso de datos son el rol del consentimiento y la forma, tiempo de almacenamiento y acceso a terceros de los datos personales recogidos. Respecto de ambos aspectos las Resoluciones Nro. 1/20 y 4/20 de la CIDH ofrecieron orientaciones a los Estados que no vimos del todo satisfechas en las implementaciones estudiadas.

En materia de consentimiento, la Resolución N° 4/20 aborda específicamente que para el desarrollo de aplicaciones de geolocalización y de alerta a la exposición al COVID-19, ***"los Estados deben controlar que los actores públicos o privados que presten este servicio recaben el consentimiento informado de las personas con COVID-19 cuyos datos personales sean incorporados a los mismos. Esto incluye informar debidamente la finalidad para la cual estos datos serán utilizados, el tipo de localización de la***

105 Resolución 1/20 CIDH, Par.14.
106 Resolución 1/20 CIDH, Par.15.

que serán objeto, y con cuáles autoridades sanitarias, empresas u otros usuarios se compartirá la información[107]*"*. Como vimos en el análisis comparativo de funcionalidades y en el análisis de transparencia, gran parte de las aplicaciones desplegadas en la región fallan en este aspecto: ya sea porque no hay suficiente claridad en la información que se provee o porque los mecanismos para recabar el consentimiento no son aptos para una toma de decisiones verdaderamente libre.

En cuanto a la forma, tiempo de almacenamiento y el acceso por terceros de los datos personales recogidos, la Resolución Nº 1/20 es clara al indicar que *"[s]olo deben almacenar los datos personales recabados durante la emergencia con el fin limitado de combatir la pandemia, sin compartirlos con fines comerciales o de otra naturaleza*[108]*"*. Coincidente con ello, la Resolución Nº 4/20 indica que *"[e]l almacenamiento de datos de las personas con COVID-19 debe estar limitado al fin legítimo y limitado de contener y revertir la pandemia, por el tiempo estrictamente necesario y estarán desvinculados de la identidad y otros aspectos personalísimos. Los datos recabados con tal fin serán suprimidos cuando hayan dejado de ser necesarios o pertinentes para los fines de la emergencia*[109] *(…)"*. Sin embargo, vemos que en la mayor parte de las tecnologías desplegadas estudiadas no hay previsiones explícitas relacionadas con la limitación del uso de los datos para el contexto de pandemia. En algunos casos, por el contrario, se observan habilitaciones amplias o ambiguas que pueden permitir a los Estados continuar su utilización una vez concluida la emergencia.

Cerramos este apartado con las orientaciones provenientes de los principios del Comité Jurídico Interamericano sobre la privacidad y la protección de datos personales sobre las excepciones basadas en el interés legítimo del Estado que resultan admisibles para la afectación de la privacidad. Lo primero es el refuerzo de la exigencia de cumplimiento del principio de legalidad para que la restricción pueda entenderse como proporcionada, y luego, la indicación del contenido mínimo que una legislación de ese tipo debiera satisfacer, incluyendo *"disposiciones relativas a la finalidad del Tratamiento, las categorías de datos personales de que se trate, el alcance de las limitaciones establecidas, las garantías adecuadas para evitar accesos o transferencias ilícitas o desproporcionadas, la determinación del Responsable, los plazos de conservación de los datos personales, los posibles riesgos para los derechos y libertades de los Titulares, y el derecho de los Titulares a ser informados sobre la limitación, salvo que resulte perjudicial o incompatible a los fines de ésta. Las autoridades nacionales deberían poner tales leyes o normas en conocimiento del público a la*

107 Resolución 4/20 CIDH, Par.34.
108 Resolución 1/20 CIDH, Par.35.
109 Resolución 1/20 CIDH, Par.35.

brevedad posible*[110]*". Como evidencia el análisis de la situación de los despliegues por país, ninguna de las tecnologías ha sido acompañada de estatutos generales o excepcionales que satisfagan tales requisitos. Las iniciativas analizadas son producto de políticas públicas desarrolladas en el marco de potestades administrativas que no han sido sometidas a un escrutinio democrático consistente con la guía aquí provista.

Conclusiones

El análisis pormenorizado de las características principales de las aplicaciones implementadas en 14 países de la región permite observar algunas tendencias comunes que fueron detalladas a lo largo de este informe. Resulta extremadamente preocupante que al buscar soluciones tecnológicas para auxiliar el combate a la pandemia de COVID-19, los Estados fallen en dar cuenta de una perspectiva integral de atención a los derechos humanos conforme lo orientan los estándares emanados de órganos internacionales en la materia, y no cumplan con sus obligaciones frente a la protección de tales derechos, y por el contrario, en muchos casos los vulneren.

Con escasas excepciones, factores como las brechas de acceso, el potencial de impacto en derechos humanos o la evidencia de efectividad no fueron tomados en cuenta en la planificación de las iniciativas analizadas. La tendencia da cuenta de una actitud en general pasiva del Estado frente a la adopción de tecnologías que pueden afectar de manera directa el ejercicio de derechos fundamentales de la población y una ausencia sistemática de consulta a las múltiples partes interesadas.

Sea en el contexto de pandemia o más allá, el despliegue tecnológico desde el sector público debe ir acompañado de medidas estrictas de transparencia, participación y rendición de cuentas. Es inaceptable en cualquier situación que este tipo de iniciativas no cuente con respaldos públicos que justifiquen su implementación ni informe los gastos públicos involucrados de manera directa o indirecta, más aún en un contexto en que los países de la región se ven enfrentados a atender demandas sociales cada vez más urgentes.

Este análisis sirve como un punto de partida para explorar oportunidades de mejora en el diseño e implementación de tecnologías en el contexto de pandemia y para reflexionar sobre el futuro del rol de la tecnología en el control social y el desarrollo de relaciones entre los Estados y la ciudadanía en nuestra región. En ese sentido, buscamos, a modo de conclusión, explorar puntos críticos que deberían ser tomados en consideración.

110 Principios del Comité Jurídico Interamericano sobre la privacidad y la protección de datos personales, Anotados, página 28.

Necesidad de atención reforzada a los niveles de conectividad
Las tecnologías propuestas, para ser eficaces en su despliegue, deben seleccionarse en consideración al acceso a internet o a las comunicaciones móviles, que se pretenden usar como base del despliegue. Con vastos segmentos de población que sufren restricciones de acceso, por razones de habilidad digital, accesibilidad de la tecnología, infraestructura, disponibilidad de servicios por actores comerciales, precios altos o baja calidad de servicio que interrumpe la calidad de la conectividad, la posibilidad de las tecnologías de alcanzar en forma masiva a la población en el combate a la pandemia se estrecha.

Como se ha destacado en la sección anterior, hay una baja representatividad de las tecnologías estudiadas en el uso y adopción por parte de la población, con excepción de los casos de Argentina y Colombia donde se establecieron obligaciones para que ciertos grupos adhirieran a su uso. La situación corrobora brechas y barreras estructurales existentes con relación a procesos de digitalización del sector público, y evidencia la necesidad de mejor planeamiento de este tipo de iniciativas de modo a tornarlas más efectivas.

También resulta necesario tener en consideración la disponibilidad de dispositivos por persona que permitan asociar la información disponible en éste con su titular. En nuestra región aún existe un número no reducido de personas que, por edad, condición económica, origen étnico o incluso por factores de género carecen de la posibilidad de acceder y controlar un dispositivo de carácter personal. Debe prestarse atención a que la información recolectada a través de los despliegues tecnológicos no provoque una marginalización adicional a estos grupos afectados muchas veces más fuertemente por la pandemia. En ese sentido, la funcionalidad de uso por múltiples usuarias en un mismo dispositivo ofrecida por la aplicación uruguaya ha sido destacada como una buena práctica en términos de accesibilidad y debería ser considerada en el diseño de iniciativas similares, siempre que sea acompañada de las medidas adecuadas de seguridad y protección de datos.

Evaluaciones de impacto en derechos humanos para garantizar toma de decisiones responsables por gobiernos y empresas

La información recabada de los distintos despliegues tecnológicos identificados no da cuenta de evidencia de que las iniciativas hayan sido evaluadas bajo una perspectiva de legalidad, necesidad y proporcionalidad en el impacto de derechos humanos en una perspectiva integral. La totalidad de las iniciativas corresponden a iniciativas desarrolladas en forma administrativa sin que se encuentren revestidas de discusiones legislativas específicas, ni satisfagan claramente mandatos legales previamente existentes que velen por su implementación con impacto proporcionado en el ejercicio de derechos distintos del derecho a la salud.

Desde la perspectiva de la necesidad, no se ha constatado en la información levantada la existencia de antecedentes técnicos que hayan sido usados por los tomadores de decisiones para determinar por qué la solución tecnológica en el contexto en que se buscó implementar resultaba más apropiada que otras alternativas (tecnológicas o no).

Finalmente, tanto desde la perspectiva de las autoridades públicas y de las empresas involucradas en el despliegue de la tecnología, resulta necesario que el compromiso -al menos declarado- con la protección de datos personales, se complemente con la visión más amplia del impacto de estas tecnologías en otros derechos tales como: la privacidad, acceso a la información, no discrimiandción, derecho a reunión, movilidad, derecho al trabajo, por mencionar algunos.

Los estándares internacionales de derechos humanos, y entre ellos las guías específicas provistas por la CIDH para el contexto de pandemia, destacadas más arriba, deben ser tenidas en consideración en el diseño y despliegue de estas tecnologías, las cuales pueden tener impactos de larga duración en el ejercicio de derechos aún luego de terminada la emergencia sanitaria. La iniciativa de las empresas privadas y la respuesta a los requerimientos provenientes de los Estados debe además ser evaluada en el marco de los Principios Guía de Derechos Humanos y Empresas de las Naciones Unidas (UNGP)[111].

Necesidad de una gobernanza de datos bien definida

Estudios internacionales muestran que la gobernanza de datos bien definida y la capacidad de supervisión en el despliegue de los sistemas son esenciales para poder ganar la confianza de la ciudadanía, y por consecuencia, para mejorar la efectividad de la contribución de la tecnología en la contención de la pandemia[112].

111 Principios Guía de Derechos Humanos y Empresas de las Naciones Unidas, disponibles en: <https://www.ohchr.org/documents/publications/guidingprinciplesbusinesshr_en.pdf>

112 Ver Blasimme, Alessandro et lt. "What's next for COVID-19 apps? Governance and oversight", Science 13 Nov 2020: Vol. 370, Issue 6518, pp. 760-762 DOI: 10.1126/science.abd9006, disponible en: <https://science.sciencemag.org/content/370/6518/760>

La evidencia levantada por el OCCA muestra que cuando se trata del uso de datos personales por parte de las autoridades encargadas de la gestión de las aplicaciones, hay poca definición en la información ofrecida a las usuarias sobre quiénes son las responsables por el tratamiento, una solicitud de consentimiento activa y la garantía de los derechos de acceso, rectificación, cancelación y oposición, en la mayoría de los casos. Sin embargo, permanecen dudas sobre cómo se efectivizan tales derechos, especialmente en los países donde no hay una normativa de protección de datos personales o instituciones capacitadas para garantizar su cumplimiento; en particular con relación a la oposición al tratamiento de datos o la retirada del consentimiento para ello.

Por otro lado, la identificación, en algunos de los países, de tráfico de datos con entidades como Amazon o Google sin que haya suficiente información en los términos y condiciones de uso de las aplicaciones se muestra preocupante desde el punto de vista de la autodeterminación informativa de las ciudadanas que deciden utilizarlas. Igualmente preocupante es el hecho de que menos de la mitad de las aplicaciones cumplen con el requisito de consentimiento expreso, libre e informado para el tratamiento de datos personales.

Medidas de seguridad tales como el cifrado (en almacenamiento y tránsito de la información), arquitecturas de datos descentralizadas y límites temporales al almacenamiento de datos, son aún elementos limitadamente incorporados o ausentes en la mayor parte de las iniciativas identificadas, todos elementos relevantes para una gobernanza que por diseño privilegie la adecuada protección de los datos personales recogidos.

Finalmente, es inadmisible que permanezcan dudas con relación al uso compartido o la transferencia de datos entre agencias del gobierno, especialmente en un contexto de polarización política e incluso periodos electorales en muchos de los países de la región. Aunque la contención al avance de la pandemia podría llegar a justificar que cierto nivel de intrusión a la privacidad sea necesario para compartir informaciones en situaciones puntuales y pre-definidas, los criterios de legalidad, necesidad y proporcionalidad deben ser observados en todos los casos en estas excepciones. Además, la titular de datos debe tener informaciones precisas sobre las situaciones en que eso puede ocurrir. Las autorizaciones genéricas de acceso deben ser evitadas y debe adoptarse medidas para impedir el uso de datos legítimamente compartidos entre entidades públicas para fines distintos de aquellos para los cuales fueron recolectados.

Transparencia hacia la ciudadanía en selección y despliegue de la tecnología

Las habilidades digitales para entender, controlar y generar vínculos de confianza con la tecnología son un obstáculo considerable para ubicarla como una pieza central en la estrategia contra la pandemia. Para ello las autoridades a cargo de su despliegue tienen un deber con la ciudadanía de información y transparencia, desde su diseño y durante todo su despliegue.

En ese sentido, es importante resaltar la necesidad de avanzar hacia medidas de participación, así como de mecanismos de supervisión por la ciudadanía. Si bien es loable la disposición del sector privado de colaborar con la respuesta a una emergencia de salud pública de dimensiones extremas, la donación de soluciones tecnológicas al Estado no resta a su obligación de satisfacer estándares de protección en el ejercicio de derechos, especialmente considerando los potenciales impactos que el acceso y tratamiento de los datos recolectados pueden tener para el ejercicio de derechos fundamentales. Además, aunque no involucren intercambios financieros, las condiciones de los acuerdos público-privados establecidos para el despliegue de esas y otras tecnologías deben ser fácilmente accesibles para la ciudadanía.

Las iniciativas analizadas muestran escasos esfuerzos por incorporar las perspectivas de la sociedad civil e, incluso, de la academia, lo que compromete su potencial. Del mismo modo, por lo general carecen de mecanismos de auditorías externas o vías para recibir e incorporar contribuciones de la sociedad civil. Donde esos mecanismos fueron incorporados se observa cómo ellos contribuyeron a avances en relación a las primeras versiones de las aplicaciones, como en el caso de Argentina, por ejemplo.

La pandemia ha reforzado la ubicuidad de la tecnología en nuestras vidas, no solo para su contención si no en todo aspecto, y es por ello una excelente oportunidad para sentar principios y procedimientos robustos de parte de los Estados, en consistencia con estándares internacionales de derechos humanos, acerca cómo la tecnología debe ser presentada y comunicada a la ciudadanía como parte de las políticas públicas, en forma que le permitan reclamar y mantener el control individual y colectivo del uso de sus datos en función de objetivos de política pública enunciados en su nombre.

AlSur