https://doi.org/10.11606/issn.2316-9044.rdisan.2023.186259
Artigo Original

Revista de Direito Sanitário

http://www.revistas.usp.br/rdisan

El uso de las aplicaciones tecnológicas para el enfrentamiento del covid-19 en América Latina – *¿Quo vadis?*

The Use of Technological Applications to Face Covid-19 in Latin America – Quo Vadis?

Jorge Luis Ordelin Font[1]
https://orcid.org/0000-0001-8778-882X

Salete Oro Boff[1]
https://orcid.org/0000-0002-7159-1878

[1] Centro de Investigación y Docencia Económicas (CIDE). División do Estudos Jurídicos. México.

RESUMEN

El uso de soluciones tecnológicas durante el período de confinamiento de la pandemia de la covid-19 generó múltiples interrogantes. Incluso con el fin oficial de la pandemia, es necesario un análisis de la efectividad del uso de estos mecanismos. El objetivo del presente trabajo ha sido analizar las experiencias en el uso de soluciones tecnológicas para el enfrentamiento de la pandemia de la covid-19, a partir del régimen de protección de datos personales en el ámbito Latinoamericano. Para su realización se utilizó el método teórico jurídico, en particular desde la perspectiva de protección de datos personales, y su uso en tres países de la región: Argentina, Brasil y México. Se concluyó que el análisis de la eficacia de cualquier solución tecnológica pasa por comprender los retos de la solución tanto desde el punto de vista de la tecnología utilizada como el respeto a las leyes y, condiciones sociales en las que la misma se aplicará.

Palabras clave: Covid-19; Datos Personales; Privacidad.

ABSTRACT

The use of technological solutions during the period of confinement of the Covid-19 pandemic raised many questions. Even with the official end of the pandemic, an analysis of the effectiveness of using these mechanisms is necessary. The objective of this paper was to analyze the experiences in the use of technological solutions to confront the Covid-19 pandemic, based on the personal data protection regime in Latin America. This study followed a legal theoretical method, particularly from the perspective of personal data protection and its use in three countries of the region: Argentina, Brazil and Mexico. It was concluded that the analysis of the effectiveness of any technological solution involves understanding its challenges, both from the point of view of the technology used and the observance of the laws and social conditions in which it will be applied.

Keywords: Covid-19; Personal Data; Privacy.

Correspondencia:
Jorge Luis Ordelin Font
jorge.ordelin@cide.edu

Recibido: 27/05/2021
Revisado: 03/08/2022
Aprobado: 22/09/2022

Conflicto de intereses:
Los autores declaran que no existe ningún conflicto de intereses.

Contribución de los autores:
Todos los autores contribuyeron por igual al desarrollo del artículo.

Introducción

> *Não se subestima a gravidade do cenário de urgência decorrente da crise sanitária nem a necessidade de formulação de políticas públicas que demandam dados específicos para o desenho dos diversos quadros de enfrentamento. O seu combate, todavia, não pode legitimar o atropelo de garantias fundamentais consagradas na Constituição* (BRASIL, 2020).

Los años 2020 y 2021 se caracterizaron por el enfrentamiento mundial a la pandemia provocada por el coronavirus (covid-19). Desde la Segunda Guerra Mundial la humanidad no se había encontrado ante una crisis de sanidad, económica, social, política y cultural de esta magnitud. Ingentes recursos fueron puestos a disposición para enfrentar un enemigo común desconocido e invisible. En un breve período de tiempo quedaron demostradas las fortalezas y debilidades de la Humanidad conformada por seres vivos y sociales. Pese al desarrollo tecnológico alcanzado no éramos tan fuertes como pensábamos.

Una de las principales características del coronavirus es su rápido nivel de contagio. Según la Organización Panamericana de la Salud (OPS) el primer caso en Latinoamérica y el Caribe se reportó el 26 de febrero del 2020 en Brasil, un mes después 48 países y territorios de la región habían reportado casos (BROTE...). Con el objetivo de frenar la transmisión y mitigar el impacto en los sistemas de salud la OPS identificó como una de sus cinco líneas de acción prioritaria, la detección temprana de casos a través de los sistemas de vigilancia existentes, así como prevenir y controlar infecciones por la covid-19 en los servicios de salud (OPS, 2020b). Uniéndose a la velocidad de la transmisión existe un número indeterminado de personas infectadas que son asintomáticas y contribuyen a su propagación por desconocimiento.

El empleo de la tecnología está entre las principales peculiaridades de esta pandemia, y la intención fue usarla en escala masiva. La relación entre la tecnología y la pandemia fue directa, e implicó diversos escenarios, en particular investigación y desarrollo de vacunas, pero también para diagnosticar, contener y predecir los brotes del virus con mayor eficacia y rapidez. En esta relación adquirió particular importancia la privacidad de los datos personales. Múltiples fueron los cuestionamientos que surgieron en este tema. Se abrió un debate en torno a si los datos personales relativos a la salud podían ser tratados en tiempo de crisis, como la que enfrentamos y, en caso de esta respuesta ser positiva, cómo debía ser este tratamiento y bajo cuáles condiciones. En un tiempo relativamente breve se escribió mucho al respecto, en algunos casos, se enfocó desde un enfrentamiento entre el derecho a la salud como derecho colectivo, de interés general y el derecho a la privacidad, siendo claro que esta contradicción no existe. Los interrogantes han estado relacionados específicamente con determinar cómo debió ser este tratamiento, durante la pandemia, particularmente durante el período de confinamiento y como finalmente ha sido. Hoy no está claro cuántos de estos riesgos realmente se materializaron y cuáles aún permanecen.

La incertidumbre generada a raíz de la pandemia no ha permitido analizar si las previsiones normativas fueron superadas por la realidad o fueron realmente efectivas. De hecho, hay que tener en cuenta que el uso de estas soluciones tecnológicas se realizó en una situación de excepcionalidad, por lo cual estas se aplicaron sin realizar los correspondientes estudios de impacto y efectividad, conforme a la urgencia epidemiológica, es decir sin una evaluación previa (HERNÁNDEZ RIVERA, 2021, p. 33). Al propio tiempo, estas mismas circunstancias forzaron a muchos países a crear regulaciones adicionales a las ya existentes para complementarlas y poder realizar una efectiva protección de los datos personales. Tal vez, más que nunca, el régimen jurídico de protección de datos personales estuvo sometido a semejante prueba y se vio en la necesidad de responder de manera inmediata a una situación de urgencia

como la que estamos viviendo (teniendo en cuenta que aun hoy no se ha declarado oficialmente el fin de la pandemia).

Dos años después de la declaración del inicio de la pandemia, existen evidencias sobre la eficacia de la utilización de este tipo de soluciones tecnológicas, así como sus limitaciones, no solo desde el punto de vista técnico, sino también social y jurídico. Por ende, el presente trabajo tiene como pregunta de investigación ¿Cuáles han sido las experiencias adquiridas en el uso de aplicaciones tecnológicas para el control de la pandemia de la covid-19 en materia de protección de datos personales? En correspondencia con ello el objetivo que se persigue es analizar las experiencias en el uso de soluciones tecnológicas para el enfrentamiento de la pandemia de la covid-19, a partir del régimen de protección de datos personales en el ámbito latinoamericano.

El presente artículo tiene un carácter marcadamente descriptivo y de revisión sobre la situación de la temática. Para su realización se utilizó el método teórico jurídico, en particular desde la perspectiva de protección de datos personales, y la experiencia en el uso de estos dispositivos en tres países de la región: Argentina, Brasil y México. Aun cuando el objeto de análisis de este trabajo es el uso de tecnologías para realizar funciones de alerta y seguimiento durante la pandemia de la covid-19 debe tenerse presente que no se abordan todos los riesgos que ello implicó, sino algunos de los más connotados.

El artículo no contiene soluciones *a priori*, ni es su objetivo proponerlas. Para ello sería necesario un trabajo de investigación de mayor envergadura que tome en cuenta los contextos de aplicación de estas tecnologías, las regulaciones normativas y las experiencias adquiridas. La idea central que se sostiene es que el actual régimen jurídico de protección de datos personales, al menos como se encuentra previsto en los países analizados, no es suficiente para alcanzar una protección efectiva ante estos dispositivos tecnológicos y su utilización en futuros contextos, pandémicos o no. Es importante apuntar que, nada impide que las tecnologías utilizadas en el enfrenamiento de la pandemia sean aplicadas en otros contextos de igual o mayor complejidad, por ende, los riesgos que estuvieron presentes pueden continuar y manifestarse en otros posibles escenarios. De ahí la necesidad de hacer una revisión de las experiencias adquiridas en su aplicación, para evitar futuros riesgos.

El trabajo se divide en dos partes. La primera parte explica la necesidad del uso de la tecnología digital para el enfrentamiento de la pandemia, así como la falsa controversia entre protección de la salud y de los datos personales, como bienes jurídicos que merecen ser resguardados en el actual contexto y, cuya protección, no entra en contradicción, como se intentó ver. La segunda parte está enfocada en el análisis de las experiencias que se han adquirido al usar estas soluciones, tanto desde el ámbito de la tecnología, de lo jurídico y lo social. El principal resultado alcanzado es precisamente comprender que el análisis de la eficacia de cualquier solución tecnológica pasa por comprender sus retos tanto desde el punto de vista de la tecnología utilizada como del respeto a las leyes y condiciones sociales en las que la misma se aplicará. Dichos factores se encuentran estrechamente interrelacionados.

I Entre la necesidad y los riesgos: el uso de la tecnología en el enfrentamiento de la pandemia

El diseño de aplicaciones de soporte tecnológico que procesan datos de proximidad e información contextual recogida en dispositivos inteligentes, y que pueden intercambiar información a través de diversas interfaces de red con otros dispositivos conectados, pretendió ser una herramienta válida para la detección temprana de infecciones por la covid-19. Así se reconocía en el inciso a) de la tercera Recomendación (UE) 2020/518

de 8 de abril (EUR-LEX, 2020b). Desde un punto de vista tecnológico los datos recopilados y generados con la utilización de estos medios permitirían conocer cómo se propagaba la enfermedad y, en consecuencia, se podían adoptar medidas eficaces de distanciamiento social. Se esperaba que, de forma inmediata, su uso tuviera un alto impacto en la contención de la pandemia, mientras que, con la misma velocidad, posibilitara el fortalecimiento de los sistemas de salud pública, dado que este tipo de soluciones digitales permitirían aliviar la carga de trabajo de estos, en particular de los servicios de emergencias.

Entre las principales funciones de estas tecnologías se podría mencionar: brindar información precisa sobre la pandemia; la aplicación de cuestionarios de autodiagnóstico y orientación individualizada en función de los síntomas; el envío de alertas cuando se estuviera cerca de una persona infectada para que se adoptaran las medidas correspondientes (hacer prueba y/o aislarse); el asesoramiento en materia de diagnóstico y comunicación entre el personal sanitario y las personas en aislamiento voluntario. Según lo previsto en el considerando 13 de la Recomendación 2020/518 estos dispositivos se consideraron como producto sanitario siempre y cuando fueran utilizados para "el diagnóstico, la prevención, el seguimiento, la predicción, el pronóstico, el tratamiento o el alivio de una enfermedad" (EUR-LEX, 2020b).

Los casos de China, Corea del Sur y Singapur constituyeron los primeros ejemplos de uso intensivo de datos para cumplir con estas funciones. Pero también fueron los primeros ejemplos sobre las posibles consecuencias negativas de estos usos. La vigilancia durante el confinamiento, que implicó la monitorización individual de la cuarentena (Corea del Sur), el uso obligatorio de la aplicación "*Alipay Health Code*" (China) para gestionar la cuarentena, a partir de un nivel de riesgo en tres colores (verde, amarillo y rojo), que funcionaba como una especie de pasaporte para poder acceder a determinados servicios, incluido el transporte público, o el bajo número de descargas de la aplicación (Singapur), estuvieron dentro de las más connotadas experiencias. Algunas se repitieron en otros países.

En América Latina también existieron múltiples ejemplos de utilización de estos dispositivos, especialmente promovidos por los gobiernos tanto en el ámbito nacional como en el local. En Argentina la aplicación oficial del Ministerio de Salud de la Nación "Coronavirus Covid-19" permitía, en principio, una rápida autoevaluación para saber si había síntomas compatibles con el covid-19. Entre los permisos concedidos al descargar la aplicación estaba el acceso a los datos sobre la ubicación física del usuario, la ubicación aproximada, por GPS y por red, conexiones *wifi* y datos recibidos por internet. En relación con la ubicación física del usuario, se especifica que estos son almacenados de forma anónima. A finales de mayo de 2020 comienza a funcionar la aplicación "Cuidar Covid-19" en Argentina, que habilitó a los ciudadanos (a) para que pudieran circular, a partir de la expedición del denominado Certificado Único Habilitante de Circulación. Esta aplicación utilizaba la geolocalización y solicitaba permisos para acceder a la localización a partir de GPS y conexiones de red, así como datos sobre la localización de la aproximación, además solicitaba el Documento Nacional de Identidad (DNI) para su ingreso y registro. En la Ciudad de Buenos Aires el uso de esta aplicación fue obligatorio (NEGRO). Un trabajo realizado por la Asociación de los Derechos Civiles resalta que al menos fueron utilizadas otras 11 aplicaciones en Argentina, una de cobertura nacional, ocho de cobertura provincial y dos de cobertura municipal (EN CASO..., 2020).

En Brasil la aplicación "Coronavírus-SUS" permitía informar los diversos síntomas que

> el usuario presentaba, igualmente informaba sobre cómo prevenirlos y que hacer en casos de sospecha de infección, indicaba las unidades de salud más próximas, permitía realizar un autodiagnóstico, saber si el ciudadano presentaba síntomas compatibles con la enfermedad

> o no, y en caso de ser positivo lo instruía para contactar la unidad de salud más próxima, entre otras funciones. Entre sus principales permisos estaban la localización aproximada por la red y por GPS, el acceso a las llamadas recibidas directamente por números de teléfonos, conexiones a la red y datos recibidos de Internet.

En México la aplicación "Covid-19MX" permitía el acceso directo al teléfono de atención epidemiológica sanitaria, así como brindaba la posibilidad de realizar el autodiagnóstico, recibir ubicaciones de centros de salud, dudas, consejos y noticias. Con su utilización se concedía acceso a la identidad, contactos, información sobre la conexión *wifi*, almacenamiento, teléfono, ubicación (precisa y aproximada), fotos/multimedia/archivos, ID de dispositivo e información de llamada, datos de internet y servicio de configuración de Google. También se puso a disposición una herramienta para brindar respuestas a preguntas, de forma automatizada. En el Plan gradual hacia la nueva normalidad en la Ciudad de México, "Covid19", entre los mecanismos de identificación y seguimiento epidemiológico se reconocía la posibilidad de recabar información voluntaria por medio de aplicaciones.

Fueron varios los actores, instituciones y organizaciones internacionales y de la sociedad civil que en los ámbitos global y regional plantearon su preocupación en relación con la protección de los datos personales y la privacidad en el enfrentamiento de la pandemia. En particular se planteó la necesidad de minimizar el grado de injerencia de estas aplicaciones en la vida privada, la eliminación del riesgo de colección y control indefinido de los datos, la suplantación de las autoridades sanitarias y la posibilidad de que estos datos pudieran ser utilizados de forma discriminatoria.

Diversas organizaciones de la sociedad civil lideradas por *Human Rights Watch* plantearon, a través de una declaración conjunta, su preocupación por la expansión masiva de los sistemas de vigilancia digital invasiva, manifestando a su vez el riesgo de discriminación que existía y apuntaron: "Intentar descifrar cómo se propaga el covid-19 utilizando series de datos incompletas y discriminatorias amenaza nuestros derechos humanos" (DECLARACIÓN..., 2020a).

La Comisión Interamericana de Derechos Humanos (CIDH) adoptó, el 10 de abril del 2020, la Resolución N.° 1/2020 sobre Pandemia y Derechos Humanos en las Américas. Entre otros aspectos esta resolución manifestó la preocupación por el uso de tecnología de vigilancia para rastrear la propagación del coronavirus, y el almacenamiento de datos de forma masiva (CIDH, 2020). A estos efectos se enunciaron un conjunto de principios y obligaciones de los Estados durante esta situación para que se adoptaran políticas y medidas sanitarias que fueran respetuosas para con los derechos humanos. En este sentido se consideró que cualquier medida adoptada en materia de derechos humanos debía ajustarse al principio *pro persona*, de proporcionalidad, temporalidad y siendo su única finalidad el cumplimiento de objetivos de salud pública y protección integral (apartado 3.f) (CIDH, 2020).

La Unión Europea no solo mostró preocupación por esta temática, sino que trató de promover el diseño de herramientas tecnológicas no invasivas (por ejemplo el protocolo DP3T). En correspondencia con ello adoptó un grupo de instrumentos jurídicos para poder establecer un campo de actuación claro durante la pandemia. Dentro de estos se pueden mencionar, la Recomendación 2020/518 (EUR-LEX, 2020b), anteriormente mencionada, y la Comunicación 2020/C 124 I/01 de la Comisión Interamericana de Derechos Humanos con orientaciones sobre las aplicaciones móviles de apoyo a la lucha contra la pandemia de covid-19 en lo referente a la protección de datos (EUR-LEX, 2020a).

El uso de este tipo de herramientas tecnológicas en el contexto de la pandemia solo podría hacerse a partir de la adopción de una perspectiva ética, legal y transparente de la gestión de los datos. Sin embargo, la búsqueda de un equilibrio entre la prevención,

control y mitigación de la pandemia y la protección de datos personales no estuvo exenta de escollos, puesto que no se trata solo de cuestiones de regulación, sino también de los recursos tecnológicos que cada país disponía para hacerle frente y, en particular. de las brechas tecnológicas que existen en cada uno de estos.

II Estados de excepción, salud pública y tratamiento de datos personales

Desde el mismo momento en que se analizó la posibilidad de utilizar herramientas tecnológicas en el enfrentamiento de la pandemia surgió el cuestionamiento en relación con la restricción o no del derecho de protección de datos personales y en qué medida esta podía ser realizada. Desde esta perspectiva se intentó generar un debate, un poco preciso, en relación con la supuesta rivalidad entre el derecho a la protección de los datos personales y el derecho a la salud. Finalmente quedó demostrado que dicha colisión o existió. Al igual que cualquier otro derecho humano, el primero de los derechos anteriormente referido, no es un derecho absoluto.

En principio, se aceptó que siendo la pandemia provocada por la covid-19 una situación de emergencia, las restricciones de libertades solo podrían estar permitidas siempre y cuando fuesen proporcionadas y limitadas al período de emergencia. Ninguna medida adoptada para combatirla podría ser considerada irreversible, y debería además ser necesaria, apropiada y sometida a control judicial. En principio, pues es claro que no era necesario el consentimiento de los titulares en situaciones excepcionales como las que enfrentamos, y en particular, aquellas relacionadas con cuestiones de salud pública. Lo que realmente se apreció, entre la situación pandémica y los regímenes de protección de datos personales, fueron imprecisiones sobre los límites técnicos y legales previstos en los preceptos normativos.

Se reconoció que cualquier relación entre el derecho a la salud, como derecho colectivo, y el derecho a la privacidad debía comenzar teniendo en cuenta que : (i) los datos relativos a la salud se encuentran dentro de las categorías especiales de datos personales o datos sensibles, como los denominan en algunos ordenamientos jurídicos y, (ii) la excepción en la solicitud del consentimiento para tratar estos datos no exime del cumplimiento de las obligaciones y garantías para el respeto de esta categoría especial de datos. Esto último fue reafirmado por Andrea Jelinek, presidente del Comité Europeo de Protección de Datos (EDPB):

> Las reglas de protección de datos (como GDPR [General Data Protection Regulation]) no obstaculizan las medidas tomadas en la lucha contra la pandemia de coronavirus. Sin embargo, me gustaría subrayar que, incluso en estos momentos excepcionales, el controlador de datos debe garantizar la protección de los datos personales de los interesados. Por lo tanto, se deben tener en cuenta una serie de consideraciones para garantizar el procesamiento legal de los datos personales (EDPB., 2020a).

Los datos relativos a la salud entendidos como los datos relacionados con la salud física o mental de una persona que incluya la prestación de servicios de atención sanitaria y cualquier otro dato que revele información sobre su estado de salud (art. 4.15 [(EUR-LEX, 2016]), y el hecho de que estos datos sean considerados una categoría especial de datos personales (art. 9.1 [(EUR-LEX, 2016]), reafirma la excepcionalidad en su tratamiento, así como la importancia de adoptar las medidas técnicas y legales necesarias para ello. La pandemia y la necesidad de la protección de la salud pública como razón de interés público si bien justificó el tratamiento, al propio tiempo reforzó la idea de que este debía ser realizado en base al derecho, e ir de la mano con el establecimiento de medidas adecuadas y

específicas para proteger los derechos y libertades del interesado, incluyendo el secreto profesional (art. 9.1(i) [(EUR-LEX, 2016]).

La autorización del tratamiento de datos personales sensibles justificados por motivos de salud pública se encontraba prevista en varias legislaciones de protección de datos personales, aunque su aplicación nunca había sido necesaria en un contexto como el provocado a raíz de la pandemia de la covid-19. Por ejemplo, así se refleja en el artículo 11, inciso g, de la Ley de Protección de Datos de Brasil, modificada por la Ley N.º 13.853/2019[1], en el artículo 22, apartado VI y VII de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados[2] (LGPDPPSO [(MEXICO, 2017]) y el artículo 10 apartado VI de la Ley Federal de Protección de Datos Personales en Posesión de Particulares (LFPDPPP [(MEXICO, 2010]), ambas del ordenamiento jurídico mexicano. En este último, la regla general es que los datos personales sensibles no se pueden tratar, salvo que exista un consentimiento expreso de su titular o se trate de una situación de emergencia, que sean necesarios para la prevención, diagnóstico y prestación de asistencia humanitaria o sometidos a un procedimiento previo de disociación, conforme lo establecido en el artículo 7 en relación con el artículo 22 apartados VI, VII y IX de la LGPDPPSO (MEXICO, 2017), así como el artículo 10, apartados III, V, y VI de la LFPDPPP (MEXICO, 2010).

Pese a que existe un fundamento jurídico para el tratamiento de los datos relativos a la salud sin consentimiento de sus titulares, la CIDH en la Resolución N.º 1/2020 (CIDH, 2020) anteriormente referida, reafirmó la necesidad de recabar el consentimiento para poder utilizarlos y compartirlos, así como la necesidad de conservar el derecho de cancelación de estos (apartado 36) (CIDH, 2020). De manera similar, la OPS, al momento de establecer sus directrices éticas para el enfrentamiento de la pandemia señaló que el análisis de datos personales o su recolección no constituye investigación en seres humanos, por ende, no podían quedar supeditados a las normas y regulaciones que regían las investigaciones sobre estos, como la aprobación previa de protocolos (OPS, 2020a), por ende, era necesario que el titular de los datos tuviera conocimiento de que estos se estaban recopilando como parte de los esfuerzos de vigilancia para mejorar la salud pública, así como de las normas sobre su uso responsable (OPS, 2020a).

Como ya se afirmó el principal problema nunca estuvo en el fundamento del tratamiento, que estaba totalmente justificado, sino cómo este debía ser realizado y, particularmente, cómo sería realizada su eliminación una vez que se extinguiera la causa que lo fundamenta. Asimismo, tampoco deberían existir dudas sobre los fines específicos del tratamiento, su extensión, plazo de conservación y accesibilidad. Dos años después de la implementación de estas herramientas tecnológicas la eficacia de las mismas ha sido puesta en entredicho, por razones no necesariamente tecnológicas, sin embargo, las preguntas relacionadas con los requerimientos legales que deberían cumplir se han mantenido.

Del análisis de las aplicaciones referidas, se desprende que su uso fue voluntario, con excepción de la aplicación "Cuidar Covid-19" y solo en el caso de la Ciudad Autónoma de Buenos Aires. Si bien estas herramientas tenían una finalidad esencialmente de autodiagnóstico con el avance de la pandemia se incorporaron otras funciones relacionadas con el seguimiento epidemiológico. Un aspecto crítico del uso de estos dispositivos fue la ausencia de políticas de privacidad claras y específicas. En el caso de la aplicación argentina cuando se revisaron sus términos y condiciones nos percatamos que se utilizaban los mismos que los utilizados para los denominados "Servicios Digitales", los cuales son aplicados para todos los servicios que brinda el Gobierno Federal argentino, sin que existieran disposiciones específicas para este tipo de aplicaciones. Posteriormente serían adoptados los términos y condiciones específicos de esta aplicación.

En el caso de Brasil no constan las políticas de privacidad, ni tampoco términos y condiciones de uso, mientras que, en la aplicación APP COVID-19 CDMX, el aviso simplificado de privacidad no especifica inicialmente su fin, y solo se refiere a que la información únicamente será tratada para realizar "las acciones necesarias y pertinentes para la atención de la emergencia sanitaria" (MEXICO). Tampoco se establecen normas claras sobre la cancelación de la aplicación, la temporalidad del almacenamiento, medidas de anonimización, medidas tecnológicas relacionadas con la seguridad digital en especial con el secreto y confidencialidad de los datos.

Posteriormente el aviso de privacidad sufriría modificaciones y esto quedaría resuelto, en particular todo lo concerniente a la especificación de las finalidades, así como el mecanismo para ejercer sus derechos de acceso, rectificación, cancelación u oposición de sus datos personales (en adelante derechos ARCO). Las finalidades de la aplicación tecnológica quedaron delimitadas a (i) brindar orientación médica a quienes proporcionaban sus datos para ser contactadas y atender la situación de emergencia y (ii) estadísticos. Conforme lo regulado en el párrafo VII del artículo 22 de la LGPDPPSO (MEXICO) no era necesario recabar el consentimiento de los titulares de los datos para su tratamiento, ni para su transferencia.

De manera general, en el uso de estas aplicaciones no quedaron evidenciadas las medidas de seguridad adoptadas para garantizar la disponibilidad, autenticidad, integridad y confidencialidad de los datos. De hecho, algunas de estas aplicaciones experimentaron brechas de seguridad que implicaron la exposición de datos de carácter personal de los usuarios.

Teniendo en cuenta la excepcionalidad de la situación y la aplicación del tratamiento de los datos era necesario someter a un mayor escrutinio y garantías la protección de los datos durante este período, el uso de estos debía ser transparente y sometido a acciones de control de las autoridades competentes. En este punto la protección debía implicar un plus a lo reconocido en los textos normativos. Nada de esto aconteció durante la pandemia. De hecho, las declaraciones de las organizaciones de la sociedad civil, sobre la necesidad de mecanismos de rendición de cuentas y salvaguardias contra el uso indebido, que hicieran posible una participación libre, activa y significativa no solo de los titulares de los datos, sino también de la sociedad civil, fueron desoídas, al igual que la necesidad de una estricta supervisión y la posibilidad de interponer recursos ágiles y efectivos contra el tratamiento irregular o inadecuado de estos datos (DECLARACIÓN…, 2020a). De hecho, lo que se observó durante todo este período fue la inexistencia de procedimientos y garantías para una verdadera protección de los datos personales, sumado todo ello a la práctica paralización de los sistemas de administración de justicia en casi todos los países.

Aun cuando estas aplicaciones tenían esencialmente funciones informativas y de comprobación de síntomas, ello no impidió que incorporaran otras funciones, inclusive aquellas relacionadas con el seguimiento. Garantizar el ejercicio de estas funciones bajo estándares jurídicos y éticos de respeto a la privacidad de las personas deviene crucial no solo para la protección de su intimidad, sino también para impedir el riesgo que supone la configuración de Estados de vigilancia permanente, similares a los descritos en la obra "1984", de George Orwell (2021).

III Retos tecnológicos, sociales y jurídicos

En principio, la propuesta debía ser de soluciones eficaces no solo desde un punto de vista técnico, sino también médico, respetando en todo momento el ordenamiento jurídico de protección de los derechos humanos, lo que incluye, además de la protección de los datos personales, el cumplimiento de requisitos de accesibilidad para personas con discapacidad, la interoperabilidad y el intercambio de datos e información entre

los diversos actores que intervinieron en el enfrentamiento de la pandemia y, en particular, los encargados de poner en práctica las políticas públicas de sanidad. Al analizar la eficacia del uso de estos tipos de soluciones quedó evidenciada la necesidad de tener en cuenta no solo factores de índole tecnológica, sino también legal y social.

1 Tecnología y privacidad: buscando un equilibrio

Con el uso de las aplicaciones tecnológicas para el enfrentamiento de la pandemia la información relacionada con la ubicación de una persona y/o sus desplazamientos adquirió particular importancia. Una de las funciones reconocidas a este tipo de aplicaciones fue la de advertir a las personas cuando estuvieran cerca de alguien positivo para el virus, todo ello con el fin de interrumpir las cadenas de contagio, garantizar el distanciamiento físico y realizar el seguimiento y control del cumplimiento de la cuarentena. Los datos de ubicación podían ser recopilados por una red o servicio donde estuviera ubicado el teléfono u otro dispositivo del titular, y podían inferirse por las torres de los operadores de telefonía móvil, redes *wifi*, sistema de posicionamiento global, *bluetooth* o una combinación de señales. Estos datos podían estar en posesión de proveedores de servicios de telecomunicaciones, proveedores de servicios de internet o titulares de aplicaciones (datos de ubicación o procesamiento de datos de tráfico).

La cuestión se centró en cuál de estos tipos de tecnologías era la menos invasiva para cumplir con dicha función sin que ello supusiera una vulneración de la privacidad de las personas, y en general que fuera acorde con un modelo de respeto de los derechos humanos. En un primer momento se pensó en la realización de los estudios de movilidad para entender el comportamiento de la pandemia y su propagación, a partir del cruce de datos de los operadores móviles de manera agregada y anonimizada, utilizando fundamentalmente los datos de geolocalización (GNSS/GPS o datos de localización de dispositivos móviles). Este fue el caso de España y Brasil, por ejemplo, en los que se emitieron órdenes al respecto[3].

Aun cuando se afirmó que los datos de geolocalización serían sometidos a procesos de disociación, ya sea de forma anónima o seudónima, en los que es imposible asociarlos a un titular por su estructura, contenido o grado de desagregación, no quedó claro como estas aplicaciones tendrían en cuenta los factores objetivos, costos, tiempos para la identificación así como brindar las garantías necesarias de que estos procesos no fueran revertidos (ser nuevamente identificables), o utilizada dicha información para otros fines, como aconteció posteriormente al menos en materia de seguridad pública.

Aun cuando ninguna de las aplicaciones anteriormente mencionadas realizó el rastreo de contactos y alerta, ello no significó que desde el ámbito tecnológico no existiera esa posibilidad. La pandemia demostró que existe una disonancia entre la realidad tecnológica, las posibilidades que brinda, y el deber ético y jurídico. Necesariamente no tiene que existir coincidencia entre estos elementos, de hecho, las diferencias existentes son parte de la realidad que la tecnología supone, porque esté prohibida, no significa que tecnológicamente no exista. Por ello, fue importante encontrar otros tipos de tecnologías que fueran menos invasivas, o al menos que no utilizaran esta.

La Comisión Europea consideró que los datos de localización no eran necesarios a efectos del rastreo del contacto y recomendó que no fueran utilizados porque implicaba la invasión a la seguridad e intimidad de los usuarios (EDPB., 2020b). En este sentido se comprobó que era posible detectar los encuentros de proximidad y emitir los correspondientes avisos, utilizando otras tecnologías menos intrusivas, como

la tecnología *bluetooth*. Dicha tecnología además permitía tener en cuenta criterios epidemiológicos más objetivos establecidos a partir del riesgo real de infección, como era la intensidad de los contactos y los riesgos de contaminación a partir de la duración del contacto.

Entre los beneficios de esta tecnología se puede mencionar el rastreo de las personas sin necesidad de la activación de los servicios de geolocalización, y su interoperabilidad, lo que adquiere especial importancia en las relaciones transfronterizas. También, es posible, en base al principio de minimización, solo tratar datos necesarios como el día del contacto, pero no el momento ni lugar exacto donde este tuvo lugar. El objetivo no era seguir los movimientos de las personas, pues se consideró que no era necesario para enfrentar la pandemia.

El almacenamiento fue un requerimiento que aportó mucha ventaja a esta tecnología, puesto que este tiene lugar en el dispositivo del usuario (tratamiento descentralizado) y no en los servidores de las autoridades sanitarias (EDPB., 2020b). Los datos almacenados en el dispositivo del usuario de forma cifrada solo se compartían a las autoridades sanitarias de forma cifrada y con autorización del titular, una vez que se confirmara la existencia de riesgo de contagio. Tampoco era posible que la persona infectada pudiera obtener información sobre la identidad de las personas que habían sido alertadas por tener contacto en los últimos dieciséis días.

Por las bondades de esta tecnología la Unión Europea decidió recomendar su uso o el de una equivalente (FALIERO, 2020). A raíz de dicha recomendación se desarrollaron dos grandes proyectos a partir de este tipo de tecnología, aunque con visiones un poco diferentes. Si bien estos modelos utilizaban la tecnología *bluetooth* adoptaron perspectivas diferentes, uno privado, fruto de la unión de dos de las empresas más poderosas del ámbito de la tecnología digital, Google y Apple, y otro creado a partir de un régimen colaborativo entre desarrolladores, especialistas en privacidad e instituciones de la sociedad civil.

El Rastreo Paneuropeo de Proximidad para Preservar la Privacidad (PEPP-PT), tenía como objetivo crear un sistema para aplicaciones que contribuyera a frenar las cadenas de contagio del covid-19, respetando los principios de privacidad europeos establecidos en el RGPD (EUR-LEX, 2016], teniendo en cuenta el desarrollo de protocolos de anonimización y seguridad.

La finalidad del proyecto era ayudar a las iniciativas nacionales, a partir del suministro de los estándares técnicos, mecanismos y servicios de interoperabilidad necesarios para realizar el rastreo de la infección más allá de las fronteras nacionales, respetando la privacidad y las normativas y costumbres nacionales. En sentido general, la tecnología que se sustentaba en los estándares aprobados por la Unión Europea para medir la proximidad de los dispositivos. Es válido resaltar que dicho proyecto como resultado de un trabajo colaborativo proponía también el uso de licencias abiertas para la creación de aplicaciones locales y la certificación de estas, en cuanto a requerimientos tecnológicos, de seguridad y de protección de la privacidad.

Del otro lado, se encontraba la propuesta de las empresas Google y Apple para la ejecución de un protocolo de rastreo de la covid-19. Denominado sistema de notificación de exposición permitía a los teléfonos con sistemas operativos Apple y Android intercambiar datos entre sí. Desde el mismo momento de su anuncio, y sin aun contar con una versión definitiva del protocolo, existían muchas dudas en relación con su funcionamiento. Entre los anuncios realizados se encontraba la inclusión del *software* por defecto en los sistemas operativos de los teléfonos, así como brindar información sobre la estimación del día que tuvo lugar el contagio y la posibilidad de que las autoridades sanitarias pudieran acceder a los datos, aun cuando se mantuviera en privado lo relacionado con la identidad e información del contagiado.

Entre los aspectos positivos de esta tecnología se podían mencionar la emisión de un aviso cuando existiera el riesgo de contagio, la puesta a disposición del protocolo para que los gobiernos nacionales desarrollasen sus propias aplicaciones, su carácter interoperable, la masividad de su uso, al estar disponible en casi todos los dispositivos móviles, la posibilidad que los usuarios pudieran conectarse y desconectarse cuando quisiesen, así mismo el hecho de que la actualización solo tuviera lugar con permiso del usuario (HOWELL O`NEILL, 2020).

En una versión inicial este funcionaba a partir de la programación de claves criptográficas, también denominadas diagnóstico, que no eran más que el conjunto de claves de seguimiento diario con sus números de día asociados a cada cliente, posteriormente se informó que en lugar de esta clave sería utilizado un código (PÉREZ COLOMÉ, 2020). Igualmente, se manifestó que las listas de notificaciones, cuando los códigos coincidieran, serían gestionadas por ambas empresas con todas las implicaciones que ello podría ocasionar.

Aun cuando la tecnología *bluetooth* fuera menos invasiva debía cumplir con los requisitos de protección y seguridad necesarios para garantizar su uso acorde con el respeto a los derechos humanos y, en particular con su privacidad. Nada asegura que, pese a su utilización, se desarrollen aplicaciones nacionales que utilicen metadatos relacionados con la conexión del dispositivo móvil, ni como herramienta de investigación masiva. También surgen interesantes preguntas sobre la tecnología considerada en sí misma, es decir, que sea utilizada con otras finalidades una vez finalizada la pandemia. Aun cuando no tuvo los efectos previstos desde el ámbito de su eficacia, eso no significa que la tecnología no pueda ser probada y/o utilizada en otros contextos sino todo lo contrario.

A la par quedó evidenciado que en conjunto con la tecnología es necesario analizar las condiciones sociales en las cuales esta será aplicada, y en particular aspectos como la brecha digital, lo que no es una cuestión baladí.

2 Las condiciones sociales de aplicación

Desde el mismo momento de su adopción este tipo de tecnología plantó múltiples preocupaciones relacionadas también con su efectividad. Más allá de las implicaciones que se plantearon en relación con la protección de la privacidad, no existía claridad sobre el uso de los metadatos, relacionados con la ubicación, asociados al dispositivo, su efectividad cuando exista cercanía entre inmuebles o entre las personas que no utilizan dispositivos, como niños o adultos mayores. La realidad demostró que el cumplimiento de requerimientos técnicos no era suficiente para garantizar la eficacia de su utilización. La tecnología brindó una posibilidad, que requería que se utilizara conforme determinados requisitos técnicos y legales, pero también sociales.

Desde el mismo momento de su concepción existieron dudas sobre el impacto que podía tener este tipo de tecnologías en la mitigación de los efectos de la pandemia. De hecho, la pandemia no solo reflejó las profundas desigualdades que existen en los ámbitos mundial y regional en lo económico y social, sino también, en el acceso y uso de las tecnologías digitales, especialmente de grupos vulnerables.

Como quedó demostrado en el Índice de la Corporación Andina de Fomento (CAF) "la universalización del acceso y las inversiones en infraestructura digital de calidad se tornan urgentes" (LAS OPORTUNIDADES..., 2020, p. 3). El acceso demostró, en conjunto con el tema de la confianza de la ciudadanía en el uso de este tipo de tecnologías, ser uno de los principales elementos para garantizar la efectividad del uso de estos dispositivos, para lograr un enfrentamiento eficaz y para generar los datos suficientes

y precisos que permitieran cumplir las funciones que se preveían. Si los ciudadanos no podían acceder a las aplicaciones, o retiraban su consentimiento para el uso su eficacia quedaba limitada.

A diferencia de las experiencias de países como Singapur y Corea del Sur en América Latina el nivel de digitalización es menor. Esta última región se enfrentó a la pandemia con un nivel intermedio de desarrollo del ecosistema digital, particularmente si se compara con el resto de las regiones en el ámbito planetario. El Índice de la CAF sobre el Desarrollo del Ecosistema Digital de la región era de 49,92 (en una escala de 0 a 100), superior al de otras regiones como África (35,05) y Asia Pacífico (49,16), pero inferior a América del Norte y Europa (LAS OPORTUNIDADES..., 2020, p. 5). A esta situación se deben agregar las diferencias que existen entre regiones y países, tanto en infraestructura de conectividad, acceso limitado a dispositivos y la baja capacidad económica de algunas regiones dentro de los países (SAAVEDRA RIONDA; OSPINA CELIS; UPEGUI MEJÍA, 2020, p. 5).

Además de las limitaciones que son propias de este tipo de tecnologías, incluyendo su uso y acceso, es necesario tener en cuenta otros elementos que incidieron en su eficacia. El contexto en el que estas se aplicarían y en particular la precariedad de los sistemas de salud de la región. Pese a los esfuerzos de algunos países, por lo general América Latina y el Caribe cuentan con sistemas de salud débiles y fragmentados, que no garantizaban el acceso universal a la salud, sino que eran servicios segregados y de calidad diferenciada según el poder económico de los sectores poblacionales, concentrados además en los centros urbanos (CEPAL, 2020). Desde el mismo inicio de la pandemia la OPS consideró que para suplir las carencias de estos sistemas en el enfrentamiento, era necesario un apoyo financiero de, al menos, 94,8 millones de dólares hasta septiembre de 2020 (DIRECTORA..., 2020). Posteriormente quedó demostrado que este apoyo financiero debería ser mayor, incluyendo la realización de gastos fiscales de naturaleza extraordinaria. La ausencia de políticas públicas claras donde se insertaría el uso de estas soluciones tecnológicas también incidió en su efectividad.

La pandemia demostró que no basta con el hecho de garantizar aquellas tecnologías que fueran más favorables y menos invasivas, sino que también se debía conceder importancia a las condiciones de acceso y uso. La confianza de las personas y de los usuarios en el proceso de adopción es también un elemento importante que debe ser tenido en cuenta al momento de incorporar su utilización dentro del contexto de cualquier política pública, obedezca esta o no a razones excepcionales como la pandemia. Generalmente, se cree que en el ámbito tecnológico todas las personas parten de un piso igual, cuando es todo lo contrario. Estas desigualdades también influyen en la recepción de la tecnología y en su efectividad.

3 Entre la gestión ética y el cumplimiento de requerimientos legales

Desde el mismo momento en que se adoptaron soluciones tecnológicas para coadyuvar en la contención de los efectos de la pandemia, la protección de los derechos humanos y los datos personales, en particular, constituyó una preocupación. La Resolución N.° 1/2020 (CIDH, 2020) de la CIDH estableció los requisitos indispensables para garantizar el respeto a los derechos humanos cuando se utilizaran herramientas de vigilancia digital para determinar, acompañar o contener la expansión de la epidemia. Entre estos se mencionaba: (i) su uso limitado en términos de propósitos y tiempo; (ii) la protección de los derechos individuales, el principio de no discriminación y las libertades fundamentales; (iii) la obligación de los estados de transparentar las herramientas de vigilancia según su finalidad; (iv) la puesta en marcha de mecanismos de supervisión independientes del uso de estas tecnologías de vigilancia, y los canales y mecanismos seguros para recepción de denuncias y reclamaciones (CIDH, 2020).

La Recomendación (UE) 2020/518 propone un enfoque paneuropeo para las aplicaciones móviles (EUR-LEX, 2020b). Sin embargo, el uso de estos requisitos no era por si suficiente, también se debía considerar que la adopción de cualquier aplicación que persiguiera funcionalidades similares en los países de la región debía tener en cuenta las prescripciones establecidas en el modelo paneuropeo, en particular, el papel de las autoridades sanitarias en la rendición de cuentas sobre el uso y tratamiento de los datos personales, su responsabilidad, el pleno control del usuario sobre sus datos personales, los límites estrictos al almacenamiento de datos, seguridad de los datos, garantía de exactitud de los datos tratados y la intervención de las autoridades de protección de datos.

Dada las características de propagación del virus SARS-CoV-2 adquirió un particular interés el procesamiento de datos de ubicación no anónimos, el cual solo puede realizarse excepcionalmente, sustentado en motivos de seguridad pública. La geolocalización revela con quién hemos contactado, con quien nos hemos encontrado, los lugares donde hemos estado y durante cuánto tiempo. Su relación con nuestro estado de salud se entendió como un dato relativo a la salud, aun cuando en principio no lo era. Sin embargo, así podría ser entendido cuando una persona obtenía un resultado positivo para la enfermedad. Estando dicha información asociada no solo a su estado de salud de forma individual, sino también en relación con otras personas, dado que la misma coadyuvaba a identificar el riesgo del estado de salud de otras personas.

De manera general, en materia de geolocalización las experiencias regulatorias y de aplicación fueron disímiles. Desde el ámbito regulatorio y legal se pueden mencionar, las experiencias de la Unión Europea, Argentina, Brasil y México.

La Unión Europea adoptó un conjunto de medidas que tomaban como punto de partida el Reglamento General de Protección de Datos (RGPD [(EUR-LEX, 2016]). El enfoque paneuropeo concibió las estrategias de salida de la crisis mediante el uso de datos de localización agregados y anonimizados. Las ya citadas Recomendación 2020/518 (EUR-LEX, 2020b) y la Comunicación 2020/C 124 I/01 (EUR-LEX, 2020a), partían de un conjunto de principios que esencialmente trataban de respetar los estándares europeos de protección de datos, y en particular establecían: (i) el procesamiento de datos solo con el objetivo de preservar la salud pública y minimizar las interferencias en la vida privada; (ii) el respeto a la privacidad desde el diseño, incluyendo código fuente público; y (iii) la adopción voluntaria de las aplicaciones (EDPB., 2020a). A los datos de proximidad solo se podría acceder ya fuera por el consentimiento del titular o porque se considerase necesario según las funcionalidades de cada aplicación. Sin embargo, como se reconoce en el apartado 3.4 de la Comunicación 2020/C 124 I/01 (EUR-LEX, 2020a) la carga de datos de proximidad no era necesaria para el funcionamiento de las aplicaciones que fueron utilizadas para realizar el seguimiento para enfrentar la pandemia, por ende, solo se podría acceder a los datos con el consentimiento de los titulares.

En Argentina, la Agencia de Protección de Datos Personales estableció cómo debían tratarse los datos para el uso de herramientas de geolocalización ante la emergencia sanitaria del covid-19 (PROTECCIÓN..., 2020). Dado que la Ley N.º 25.326 (ARGENTINA, 2000) de protección de datos personales no prohíbe, al menos de forma expresa, el monitoreo de la ubicación de las personas, se establecieron un conjunto de principios para el tratamiento de estos, tomando como referencia tanto el marco normativo vigente como el convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, suscrito en Estrasburgo el 28 de enero de 1981 y del cual este país es parte (REPUBLICA ORIENTAL DEL URUGUAY, 2012).

En Brasil el Supremo Tribunal Federal declaró inconstitucional la Medida Provisoria N.º 954/2020 de 17 de abril, en virtud de la medida cautelar en acción directa de inconstitucionalidad N.º 6.387 (AMORIM, 2020). La Medida Provisoria N.º 954/2020, adoptada en el marco de la Ley N.º 13.979/2020 de 6 de febrero, sobre las medidas de enfrentamiento de emergencia de salud pública de importancia internacional, que facultaba, en su artículo 2 a las empresas prestadoras de servicios telefónicos fijo y móvil, a compartir por medio electrónico, la lista de nombres, números de teléfonos y dirección de sus consumidores, ya fueran personas físicas o jurídicas, con la Fundación Instituto Brasileño de Geografía y Estadística (IBGE).

La medida cautelar adoptada tuvo en cuenta vicios de inconstitucionalidad formal y material. En el primer supuesto por inobservancia de los requisitos constitucionales para la promulgación de medidas previsorias, mientras que la inconstitucionalidad material se sustentó en la violación de la dignidad humana, la inviolabilidad de la intimidad, la vida privada, la honra, la imagen de las personas, el secreto de los datos y la autodeterminación informativa, que están regulados en los artículos 1º, inciso III, y 5º, incisos X y XII, de la Constitución brasileña (BRASIL, 1988).

Sin embargo, no se puede suponer que estos fueron los procedimientos adoptados por todos los países, o al menos en la mayoría de ellos. En otros, como México, no se dictaron disposiciones particulares al respecto. Durante la contingencia sanitaria en este país, solo se emitieron un conjunto de recomendaciones, destinadas particularmente a la verificación de la autoridad, entidad u organismo público autorizado a recolectar datos, la necesidad de consultar el aviso de privacidad, y evitar proporcionar datos relativos a la salud por medios electrónicos engañosos o no oficiales. Asimismo, se advertía que los sujetos obligados podrían realizar transferencias de datos personales sin necesidad de requerir el consentimiento de los titulares. **Sin embargo, lo cierto es que estos instrumentos no fueron más allá de su función: ser recomendaciones cuya aplicación quedaba al amparo de los sujetos obligados al tratamiento de datos personales.**

En principio, el establecimiento de normas claras debía impedir la proliferación de aplicaciones incompatibles con los estándares de protección de los datos. Sin embargo, lo cierto es que esto no se ha podido corroborar en toda su extensión. Uno de los aspectos que más importancia adquirieron en el tratamiento de estos datos, bajo las condiciones de la pandemia, fue el de su temporalidad. El modelo de tratamiento de datos ofrecido por la Unión Europea proponía su eliminación una vez levantadas las medidas de confinamiento. Casi tres años después del inicio de la pandemia el confinamiento prácticamente no existe en ningún país, oficialmente la pandemia ha terminado y no existen pruebas sobre la eliminación de estos datos por parte de quienes los recabaron. Tampoco han sido evidenciados los resultados de las revisiones periódicas de las causas que justifican dicha necesidad, así como tampoco su conservación, tal como se proponía, ni los supuestos en los que estos datos se han conservado por su valor científico.

No basta que exista proporcionalidad entre los datos y las funcionalidades de la aplicación, es preciso que exista una distinción entre cada una de estas, de tal forma que el consentimiento se otorgue por separado dependiendo de las funciones que el usuario quiera utilizar. Por ejemplo, si solo se persigue una función de información no es necesario el tratamiento de los datos almacenados en el equipo de salud, distinto es cuando se busca comprobar síntomas o realizar actividades propias de la telemedicina. En ningún caso las autoridades sanitarias podrán tener acceso a ningún dato sin previo consentimiento.

Es necesario que queden establecidos con claridad cuáles son las acciones, actividades, controles o mecanismos técnicos y físicos que se han utilizado y que evitan su acceso, modificación, difusión o destrucción de forma no autorizada, así como el plan de

contingencia para responder de forma directa, inmediata y efectiva cuando alguna de estas situaciones tenga lugar.

Estas condiciones y garantías no siempre fueron tenidas en cuenta al momento de establecer el uso de estas aplicaciones. Un ejemplo de la necesidad de que estos requisitos técnicos y legales fueran cumplidos se evidenció en la declaración de inconstitucionalidad de la Medida Provisoria N.º 954/2020 del Gobierno de Brasil, anteriormente explicada. De particular interés puede considerarse el fundamento esgrimido en relación con el hecho de que la medida provisoria no contenía el mecanismo técnico u administrativo apto para proteger los datos personales de los accesos no autorizados, fugas accidentales y utilización indebida en su tratamiento o transmisión (apartado 18). Puesto que no previa estos mecanismos o procedimientos, inclusive aquellos relacionados con la anonimización de los datos. De esta forma se consideró que el texto normativo no satisfacía las exigencias de la Constitución brasileña (BRASIL, 1988) en relación con la efectiva protección de los derechos fundamentales de los ciudadanos de este país.

Conclusiones

El uso de aplicaciones móviles con fines de alerta, prevención y seguimiento de contactos para enfrentar la pandemia fue importante para llevar a cabo la desescalada o vuelta a la normalidad. Su utilización también fue necesaria en la *postcuarentena*. La recopilación, transmisión, tratamiento y almacenamiento de datos por parte de estas aplicaciones deben estar garantizados por una gestión ética y transparente que responda tanto a medidas legales como tecnológicas, como las condiciones de acceso y contexto en el cual se aplicarán.

Su uso durante la pandemia permitió una mayor comprensión de la relación que se establece entre las personas y la tecnología. No solo confirmó la importancia de que existieran prescripciones legales que protegieran los derechos de las personas, sino también que se buscaran y utilizaran tecnologías éticamente responsables. Aunque las autoridades sanitarias realizaran el tratamiento de datos personales bajo determinados criterios éticos y legales, ello es necesario, pero no suficiente, dado que deben tenerse en cuenta otras condiciones. Es importante que el uso de la tecnología responda a las necesidades concretas de la situación y a la capacidad de la ciudadanía de asimilarlas, puesto que esto último es vital para garantizar la efectividad de la medida adoptada. En América Latina el uso de estas aplicaciones no puede ser realizado si no se tiene en cuenta la realidad existente en materia de brecha digital.

Desde el ámbito tecnológico es necesario tener en cuenta los riesgos que un tipo determinado de tecnología representa para la sociedad. Por ello, deben tomarse medidas claras y precisas para garantizar la protección de los datos personales, quedando claro en los términos y condiciones cuales son las finalidades que se persiguen, ante quien se deben ejercer los derechos de acceso, rectificación, cancelación y oposición, la limitación del plazo de conservación de estos datos y, en consecuencia, el período de eliminación definitiva. Hoy existe una deuda por parte del sector gubernamental que rinda cuenta del cumplimiento de estas medidas en las tecnologías aplicadas durante la pandemia para realizar funciones de rastreo de contactos.

Aun cuando el tratamiento realice las aplicaciones de forma anónima o seudónima es importante que se garanticen las medidas técnicas, físicas y jurídicas para evitar la reversión de estos datos una vez que hayan sido eliminados, o la asociación a una persona determinada. La transparencia debe garantizar el cumplimiento de dichas medidas cuando sean sometidas a control por parte de las autoridades de protección de datos o por terceros, incluyendo los propios titulares.

Referencias

AMORIM, Felipe. STF barra medida do governo para repasse de dados telefônicos ao IBGE. *UOL*, São Paulo, 7 maio 2020. Disponible en: https://www.uol.com.br/tilt/noticias/redacao/2020/05/07/stf-tem-maioria-de-votos-contra-o-envio-de-dados-telefonicos-ao-ibge.htm.

ARGENTINA. Congreso de la Nación Argentina. *Ley 25.326*. Protección de Datos Personales y Normas Reglamentarias y Complementarias. Promulgada con observaciones: Octubre 30 de 2000. Texto actualizado con las modificaciones de la ley 26.343 (BO 9-1-2008) Boletín Oficial: Noviembre 2 de 2000. Disponible en: https://www.diputados.gov.ar/export/hcdn/secparl/dgral_info_parlamentaria/dip/archivos/Ley_25326.pdf. Acceso en: 27 jul. 2023.

BRASIL. *Constituição da República Federativa do Brasil de 1988*. Disponible en: https://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm. Acceso en: 17 jul. 2023.

BRASIL. Supremo Tribunal Federal. *Ação Direta de Inconstitucionalidade – ADI*. Medida Cautelar Urgência. Relatora: Min. Rosa Weber, julgado em: 17/04/2020. Disponible en: https://jurisprudencia.stf.jus.br/pages/search/despacho1095308/false. Acesso en: 28 jul. 2023.

BROTE de enfermedad por el Coronavirus (COVID-19). *Organización Panamericana de la Salud (OPS)*. Disponible en: https://www.paho.org/es/temas/coronavirus/enfermedad-por-coronavirus-covid-19. Acceso em: 3 abr. 2020.

COMISIÓN ECONÓMICA PARA AMÉRICA LATINA Y EL CARIBE (CEPAL). *América Latina y el Caribe ante la pandemia del COVID-19*: efectos económicos y sociales. 2020. (Informe Especial COVID-19 n. 1). Disponible en: https://repositorio.cepal.org/server/api/core/bitstreams/82414c93-33bf-4a64-af1e-b26e28e1437e/contente.

COMISIÓN INTERAMERICANA DE LOS DERECHOS HUMANOS -- CIDH. *Resolución No. 1/2020 Pandemia y Derechos Humanos en las Américas*. Costa Rica: OEA, 10 de abril de 2020. Disponible en: http://oas.org/es/cidh/decisiones/pdf/Resolucion-1-20-es.pdf. Acceso en: 17 jul. 2023.

DECLARACIÓN conjunta de la sociedad civil: Los Estados deben respetar los derechos humanos al emplear tecnologías de vigilancia digital para combatir la pandemia. *Human Rights Watch*, 02 abr. 2020. Disponible en: https://www.hrw.org/es/news/2020/04/02/declaracion-conjunta-de-la-sociedad-civil-los-estados-deben-respetar-los-derechos. Acceso em: 13 abr. 2020.

DIRECTORA de la OPS llama al sectro privado a cooperar en la respuesta a la COVID-19 en las Américas. *Organización Panamericana de la Salud (OPS)*, 03 abr. 2020. Disponible en: https://www.paho.org/hq/index.php?option=com_content&view=article&id=15770:directora-de-la-ops-llama-al-sector-privado-a-cooperar-en-la-respuesta-a-la-covid-19-en-las-americas&catid=740:press-releases&lang=es&Itemid=1926. Acceso em24 de abril de 2020.

EN CASO de emergencia: descargue una app. *Asociación por los Derechos Civiles (ADC)*, 21 may 2020. Disponible en: https://adc.org.ar/2020/05/21/en-caso-de-emergencia-descargue-una-app/. Acceso em: 24 jun. 2022.

EUR-LEX. *Comunicación de la Comisión orientaciones sobre las aplicaciones móviles de apoyo a la lucha contra la pandemia de covid-19 en lo referente a la protección de datos 2020/C 124 I/01*. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52020XC0417(08). Acceso en: 17 jul. 2023.

EUR-LEX. *Recomendação (UE) 2020/518 da Comissão de 8 de abril de 2020 relativa a um conjunto de instrumentos comuns a nível da União com vista à utilização de tecnologias e dados para combater a crise da COVID-19 e sair da crise, nomeadamente no respeitante às aplicações móveis e à utilização de dados de mobilidade anonimizados*. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex:32020H0518. Acesso em: 01 ago. 2023.

EUR-LEX. *Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE*. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32016R0679. Acceso en: 17 jul. 2023.

EUROPEAN DATA PROTECTION BOARD – EDPB. *Twenty-first plenary session of the European Data Protection Board-Letter concerning the European Comission`s draft Guidance on apps supporting the fight against the COVID.19 pandemic*. 2020. Disponible en: https://edpb.europa.eu/news/news/2020/twenty-first-plenary-session-european-data-protection-board-letter-concerning_en. Acceso em: 24 abr. 2020.

EUROPEAN DATA PROTECTION BOARD – EDPB. *Twenty-fourth Plenary session: EDPB doubles down on COVID-19 guidance in newly adopted letters*. 24 abr. 2020. Disponible en: https://edpb.europa.eu/news/news/2020/twenty-fourth-plenary-session-edpb-doubles-down-covid-19-guidance-newly-adopted_en. Acceso em: 2 mayo 2020.

FALIERO, Johana. Coronavirus, privacidad y protección de datos personales. Los peligros del determinismo algoritmico, la inteligencia artífical y el perfilamiento en tiempos de pandemia. *La Ley*, Buenos Aires, p. 5-10, mayo de 2020.

HERNÁNDEZ RIVERA, Laura Nathalie. El uso de tecnologías para el combate en la pandemia: datos personales en Latinoamérica. *Derechos Digitales y Global Network Initiative*, oct. 2021. Disponible en: https://globalnetworkinitiative.org/wp-content/uploads/2021/11/COVID19-LAC-SPA.pdf.

HOWELL O`NEILL, Patrick. Así funcionará la app de Google y Apple para rastrear a la COVID 19. Traducido por Ana Milutinovic. *MIT Technology Review*, 16 abr. 2020. Disponible en: https://www.technologyreview.es/s/12087/asi-funcionara-la-app-de-google-y-apple-para-rastrear-la-covid-19.

LAS OPORTUNIDADES de la digitalización en América Latina frente al Covid 19. Corporación Andina de Fomento. Naciones Unidas, 2020. Disponible en: https://repositorio.cepal.org/server/api/core/bitstreams/657e3543-74b1-4163-89e5-8e422d23edd8/contente.

MEXICO. Câmara de Diputados. *Ley Federal de Protección de Datos Personales en Posesión de los Particulares*, 05/07/2010. Disponible en: https://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf. Acceso en: 17 jul. 2023.

MEXICO. Câmara de Diputados. *Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados*, 26/01/2017. Disponible en: https://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf. Acceso en: 17 jul. 2023.

MÉXICO. Gobierno de la Ciudad de México. *Términos y condiciones de uso de la "APP Covid-19 CDMX"*. Disponible en: https://adip.cdmx.gob.mx/storage/app/media/Alameda%20Central_Terminos%20y%20Condiciones/alameda-central-terminos-y-condiciones.pdf.

NEGRO Adrián. *La credencial en un celular*. Disponible en: https://www.todociencia.com.ar/la-credencial-en-un-celular/. Acceso em: 24 jun. 2022.

ORGANIZACIÓN PANAMERICANA DE LA SALUD – OPS. *Orientación ética sobre cuestiones planteadas por la pandemia del nuevo coronavirus (COVID-19)* de 16 de marzo del 2020. Washington-DC: OPS, 16 mar. 2020. Disponible en: https://iris.paho.org/handle/10665.2/52142.

ORGANIZACIÓN PANAMERICANA DE LA SALUD – OPS. *Respuesta de la Organización Panamericana de la Salud a la Covid-19 en la región de Las Américas*. 17 ene. al 31 mayo 2020. Disponível em: https://docs.bvsalud.org/biblioref/2020/06/1100377/respuesta-ops-covid-19-americas-31-mayo-2020.pdf. Acceso em: 5 jul. 2020.

ORWELL, George. *1984*. México: Gandhi editors, 2021.

PÉREZ COLOMÉ, Jordi. Apple y google permitirán que su sistema de rastreo funcione sin que los usuarios descarguen una aplicación. *El País*, 24 de abril de 2020.

PROTECCIÓN de datos personales y geolocalización. *Argentina.gob.ar, noticias*, 29 abr. 2020. Disponible en: https://www.argentina.gob.ar/noticias/proteccion-de-datos-personales-y-geolocalizacion. Acceso en: 24 abr. 2020.

REPUBLICA ORIENTAL DEL URUGUAY. Camara de Senadores. Carpeta N° 833 de 2012. Repartido N° 681, noviembre de 2012. Convenio N° 108 del Consejo de Europa para la Protección de las Personas con Respecto al Tratamiento Automatizado de Datos de Carácer Personal y Protocolo Adicional al Convenio Para La Protección de las Personas con Respecto al Tratamiento Automatizado de Datos de Carácter Peronal, a las Autoridades de Control y a los Flujos Trasfronterizos de Datos. Disponible en: https://www.oas.org/es/sla/ddi/docs/U12%20convenio%20n%20108.pdf. Acceso: 20 abr. 2020.

SAAVEDRA RIONDA, Víctor Práxedes; OSPINA CELIS, Daniel; UPEGUI MEJÍA, Juan Carlos. *Tecnología para combatir la pandemia*: consciente de sus límites, mejor en sus potencialidades. Bogotá: Editorial DeJusticia, 2020. (Del miedo a la acción, n. 7).

Notas

1 La Ley N.° 13.709, de 14 de agosto de 2018 sin entrar en vigor fue modificada por la Ley N.° 13.853, de 2019 y debía entrar en vigor en agosto de 2020, sin embargo, la Medida Provisoria N.° 959, de 29 de abril de 2020, modificó el artículo 65 y amplió la *vactio legis* hasta el 3 de mayo de 2021.

2 Son considerados sujetos obligados en virtud del artículo 1 de la Ley en el ámbito federal, estatal y municipal, cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos.

3 En España se declaró el estado de alarma para la gestión de la crisis sanitaria ocasionada por el COVID-19, en virtud del Real Decreto 463/2020, de 14 de marzo. La Orden SND/297/2020 de 27 de marzo, encomendó a la Secretaría de Estado de Digitalización e Inteligencia Artificial, el desarrollo de diversas actuaciones para la gestión de la crisis sanitaria ocasionada por el COVID-19. Esta orden previó la necesidad de permitir la geolocalización para verificar que cada persona se encuentra en la comunidad autónoma que dice declarar y realizar un estudio de movilidad a partir del cruce de datos de los operadores móviles (artículo 2). En Brasil, la referida Medida Provisoria N.° 954/2020 permitía el compartimento de datos por parte de las empresas prestadoras de servicios telefónicos fijo y móvil con la finalidad de producir estadística oficial, así como realizar entrevistas con carácter no presencial en el ámbito de investigaciones domiciliares (apartado 1 del artículo 2).