HHS Public Access

Author manuscript

Rev Bioet Derecho Perspect Bioet. Author manuscript; available in PMC 2024 August 27.

Published in final edited form as:

Rev Bioet Derecho Perspect Bioet. 2023 March ; 57: 181–191. doi:10.1344/rbd2023.57.39432.

Ethical regulation of digital health applications in the COVID-19 pandemic

Maria de la Paz Lascano,
FLACSO (Argentina)

Timothy Daly, PhD.
Sorbonne Université, Science Norms Democracy UMR 8011, Paris (Francia). Programa de Bioética, Facultad Latinoamericana de Ciencias Sociales (FLACSO), Buenos Aires (Argentina).

Resumen

Desde la pandemia por COVID-19, varios países han desarrollado aplicaciones digitales en salud para ayudar a las políticas de prevención y cuidado de la población. Pero utilizan datos personales y sensibles y pueden depender de una infraestructura inadecuada para el almacenamiento, el resguardo y la protección de los datos. Presentamos diez criterios que deben cumplir las aplicaciones digitales en salud para garantizar la protección del derecho a la intimidad, libertad, privacidad, igualdad y confidencialidad de todo ser humano. Deben establecerse formas adecuadas de gobernanza que impliquen a todas las partes interesadas en su uso para garantizar la transparencia y la responsabilidad en los procesos de generación y transferencia de conocimientos en el sector sanitario.

Resum

Des de la pandèmia per COVID-19, diversos països han desenvolupat aplicacions digitals en salut per a ajudar a les polítiques de prevenció i cura de la població. Però utilitzen dades personals i sensibles i poden dependre d'una infraestructura inadequada per a l'emmagatzematge, el resguard i la protecció de les dades. Presentem deu criteris que han de complir les aplicacions digitals en salut per a garantir la protecció del dret a la intimitat, llibertat, privacitat, igualtat i confidencialitat de tot ésser humà. Han d'establir-se formes adequades de governança que impliquin a totes les parts interessades en el seu ús per a garantir la transparència i la responsabilitat en els processos de generació i transferència de coneixements en el sector sanitari.

Abstract

Since the COVID-19 pandemic, several countries have developed digital health applications to assist prevention and population care policies. But they use personal and sensitive data and may rely on inadequate infrastructure for data storage, safeguarding and protection. We present ten criteria that digital health applications must meet to guarantee the protection of the right to privacy, freedom, equality and confidentiality of every human being. Appropriate forms of

maridelapaz@hotmail.com .

governance must be established that involve all stakeholders in their use to ensure transparency and accountability in the processes of knowledge generation and transfer in the health sector.

Palabras clave:

aplicaciones digitales en salud; pandemia; salud digital; infraestructura digital; datos personales y sensibles; protección

Paraules clau:

aplicacions digitals en salut; pandèmia; salut digital; infraestructura digital; dades personals i sensibles; protección

Keywords

digital health applications; pandemic; digital health; digital infrastructure; personal and sensitive data; protection

1. Introducción

La pandemia por COVID-19 generó, y continúa generando, innumerables desafíos a nivel mundial. El desarrollo y la implementación de aplicaciones digitales en salud fue sin duda una de las principales medidas adoptadas por varios países —China, Colombia, Perú, Singapur, Argentina, Uruguay, Corea del Sur, España, entre otros[1]— como una herramienta para complementar y asistir las políticas de prevención y cuidado de la población en el contexto de la pandemia por COVID-19, de allí la importancia de prestarles especial consideración. Que su uso fuera obligatorio o meramente voluntario, aparecieron tantas aplicaciones digitales en el contexto referido que algunos se atreven a hablar de una "*appdemia*"[2].

Ahora bien, utilizar aplicaciones digitales en el ámbito de la salud no es algo que deba ser ignorado por la población en general, y mucho menos por los Estados que deciden su implementación y son quienes deben enfrentar las consecuencias que sus usos generan.

No pueden desconocerse los innumerables beneficios que las tecnologías de la información traen aparejadas para la población en general. Las aplicaciones digitales en salud permiten predecir conductas y tendencias que a la vez posibilitan una toma de decisiones estatal más informada y fundamentada, por lo que no reconocer la importancia y la necesidad de las mismas, sobre todo en un contexto de pandemia, sería poco prudente e inteligente. Otro argumento a favor del uso de las aplicaciones digitales en salud, es que la tecnología

[1]Davidovsky, S. Privacidad versus salud: uno de los debates sobre los derechos en tiempos de coronavirus. Chequeado. Última consulta: 14 de agosto de 2021. Disponible en: https://chequeado.com/el-explicador/privacidad-versus-salud-uno-de-los-debate-sobre-los-derechos-en-tiempos-de-coronavirus/, https://chequeado.com/el-explicador/sirven-las-apps-de-rastreo-para-acorralar-al-coronavirus-en-america-latina/.

[2]Global Privacy Assembly. GPA COVID-19 Taskforce: Compendium of Best Practices in Response to COVID-19. Última consulta: 4 de octubre de 2022. Disponible en: https://globalprivacyassembly.org/wp-content/uploads/2020/10/Compendium-of-Best-Practices-in-Response-to-COVID-19-final-27-Oct-2020.pdf.

evoluciona y llegó para quedarse, por lo que utilizarla como una herramienta que permita a los estados adoptar medidas de salud pública más inclusivas y que contribuyan así a disminuir la brecha social tan presente en la actualidad, parece convertirse en una tarea fundamental de los gobiernos.

Si bien resulta lógico que en un contexto de emergencia sanitaria los gobiernos arbitren todo lo que tienen a su alcance en pos de implementar políticas de salud pública que protejan a la población, y aminore los efectos catastróficos de la pandemia, esto no implica que cualquier medida adoptada se encuentre justificada. Toda decisión gubernamental debe, o debería, encontrar sustento sobre una base mínima de evidencia científica, y más aún, cuando dicha decisión puede afectar derechos humanos consagrados universalmente. El uso de aplicaciones digitales en salud no es la excepción.

¿Por qué no es la excepción? Dichas aplicaciones se nutren a partir de los datos que los usuarios proporcionan, y al hablar de aplicaciones digitales en salud, nos referimos puntualmente a datos personales y datos en salud, es decir, datos sensibles que merecen protección especial[3]. Cuando el usuario se encuentra utilizando las aplicaciones que se desarrollaron para enfrentar el coronavirus, expone datos sobre su estado de salud y sintomatología compatible con el virus SARS-CoV-2, ubicación, número de identificación personal, personas con las cuales se encontró, nombre completo y apellido, entre otros. Todos datos que pertenecen a su intimidad y los cuales se transforman en un conjunto de datos que permiten identificar a su titular.

Es por ello, que a lo largo del presente trabajo analizaremos algunos de los problemas que trae aparejado el uso de aplicaciones digitales en salud cuando los gobiernos no cuentan con una infraestructura lo suficientemente sustentable para el almacenamiento, resguardo y protección de los datos personales y sensibles que se obtienen a partir del uso de dichas aplicaciones. Expondremos argumentos a favor de las mismas, ya que no podemos desconocer los beneficios que trae aparejado su uso, como así también diversos aspectos que considero deben reunir las aplicaciones digitales en salud para que estas cumplan con estándares mínimos que garanticen la protección del derecho de intimidad, libertad, privacidad, igualdad y confidencialidad de todo ser humano.

Por último, plantearemos los motivos por los cuales considero que como sociedad nos encontramos frente a una oportunidad única de exigirles a los gobiernos que arbitren medidas con el suficiente respaldo legal en pos de proteger verdaderamente nuestros derechos. La tecnología avanza a pasos agigantados y la transformación digital es de carácter irreversible, lo que conlleva a la necesidad de contar con una normativa tanto

[3]Ley N° 25.326. Protección de Datos Personales, Argentina, Artículo 2°: “A los fines de la presente ley se entiende por:— Datos personales: Información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables.— Datos sensibles: Datos personales que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual.(…)”. También el Reglamento 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 (Reglamento general de protección de datos) de la UE establece: “Son categorías especiales de datos aquellos que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas o la afiliación sindical, los datos genéticos y biométricos, datos relativos a la salud y la vida sexual o las orientaciones sexuales de una persona física”.
Véase también el Convenio n.º 108 de 1981 del Consejo de Europa. Última consulta: el 4 de octubre de 2022. Disponible en: https://www.europarl.europa.eu/factsheets/es/sheet/157/la-proteccion-de-los-datos-personales

internacional como local que sea lo suficientemente flexible para adaptarse a los constantes cambios pero que al mismo tiempo sea lo suficientemente sólida para evitar la vulneración de derechos humanos básicos.

No debemos permitir que el uso de la tecnología a través de aplicaciones digitales en salud genere aún más inequidades que las ya existentes. Debemos velar por ello.

2. Desarrollo

El sector de la salud no es ajeno al auge del uso de tecnologías de la información y de las comunicaciones (TICs). La historia clínica electrónica, la telemedicina, la inteligencia artificial, la receta electrónica, son algunas de las tantas herramientas del sector de la salud que se valen de la tecnología para su desarrollo, crecimiento e implementación.

Sin embargo, la pandemia por COVID-19, declarada como tal por la Organización Mundial de la Salud el 11 de marzo de 2020[4], generó que diferentes países implementaran, como una innovación en salud pública sin precedentes, el uso de tecnología mediante aplicaciones digitales en salud. A través de dichas aplicaciones, los estados se propusieron detectar tempranamente los casos, rastrear los contactos, garantizar la atención y seguimiento de las personas, como también evitar y disminuir la transmisión del virus. Decimos sin precedentes, porque la cantidad de aplicaciones digitales en salud que comenzaron a implementarse a nivel mundial fue explosiva. Algunos ejemplos son los siguientes: Cuidar (Argentina), Trace Together (Singapur), Self-quarantine safety protection (Corea del Sur), Health Kit (Pekín), Coronapp (Colombia), Radar Covid (España), Perú en tus manos (Perú), Coronavirus UY (Uruguay).

Ahora bien, ¿tienen a su disposición los gobiernos una infraestructura que les posibilite el almacenamiento, resguardo y protección real de los datos personales y sensibles que se obtienen a partir del uso de dichas aplicaciones? Probablemente algunos si la tengan y otros no. La respuesta a dicho interrogante no es un tema que deba pasar desapercibido, ya que el carácter de los datos que los usuarios proporcionan al usar esas aplicaciones es lo que los convierte en especiales, y por ende, merecedores de una protección específica. Esto genera que las aplicaciones digitales en salud no deben –o no deberían-ser impuestas sin una infraestructura que permita y garantice la protección de esos datos. Si no, los gobiernos terminan siempre dependiendo de las grandes empresas tecnológicas, como Apple, Google, Microsoft, o empresas tecnológicas nacionales, por ejemplo, Indra Sistemas en España, que ofrece servicios privados de consultoría así como servicios al sector público.

Los datos a los cuales hacemos referencia son datos, en primer lugar, personales, es decir, datos que pertenecen a la esfera más íntima de la persona, y en segundo lugar, son datos en salud, los cuales en la gran mayoría de las legislaciones gozan de una protección especial. Son datos que refieren a los aspectos más sensibles o delicados sobre el individuo y que pertenecen a la esfera más intangible de la persona. Asimismo, lo que caracteriza un dato

[4]Organización Mundial de la Salud. Alocución de apertura del Director General de la OMS en la rueda de prensa sobre la COVID-19 celebrada el 11 de marzo de 2020. Última consulta el 14 de agosto de 2021. Disponible en: https://www.who.int/es/director-general/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing-on-covid-19-−-11-march-2020.

como dato sensible, es su potencialidad para generar actitudes discriminatorias respecto de sus titulares. Por lo cual, no se puede justificar la entrega de estos datos a cualquier entidad pública o privada sin el debido resguardo y protección. Independientemente de la era digital que transitemos, los titulares de esos datos son quienes debieran tener el control sobre los mismos, ya que esto puede acarrear implicancias en la libertad no solo de sus titulares sino también de generaciones futuras.

Como se refirió *ut-supra*, el uso de las aplicaciones, en algunos supuestos fue obligatorio, generándose de esta manera un gran dilema ético y legal, porque el límite entre la emergencia sanitaria e imponerle a la población que utilice una aplicación a través de la cual está proporcionando datos personales y sensibles que merecen protección especial sin garantizarles esa protección, es muy fino. Conforme se expone en el Convenio para la protección de los derechos humanos y la dignidad del ser humano con respecto a las aplicaciones de la Biología y la Medicina, los intereses de la ciencia y de la tecnología no deben prevalecer por sobre el interés individual: *Art. 2.: "Primacía del ser humano. El interés y el bienestar del ser humano deberán prevalecer sobre el interés exclusivo de la sociedad o de la ciencia."*

La pandemia no es razón suficiente para la implementación de aplicaciones digitales en salud sin un respaldo legal, ético y social que garantice una mínima protección a los siguientes ciertos derechos fundamentales decretados en el Pacto Internacional de Derechos Civiles y Políticos[5]. Incluyen el derecho a la privacidad, confidencialidad, igualdad, intimidad, libertad, autodeterminación[6]. A los fines de velar por los mismos, es que toda aplicación digital en salud que se implemente debería cumplir con determinados requisitos (Tabla 1, por orden alfabético)[7]. Nos encontramos transitando una era de salud digital que no puede ser ignorada. Frente a ello, los estados deben aunar esfuerzos para adecuar sus sistemas a los tiempos actuales, pero sin que esto implique que se acentúe aún más la brecha social por las desigualdades digitales también presentes. No toda la población tiene acceso a teléfonos inteligentes, a sistemas de internet, a conocimiento digital, por lo que al incorporar la tecnología a los sistemas de salud se debe poner especial atención en que esa incorporación no esté siendo utilizada para crear nuevas inequidades. A medida que se reduce la brecha de género en el acceso a Internet, la segunda brecha digital —la habilidad— adquiere cada vez más importancia. Sin lugar a duda es un desafío que deben enfrentar los gobiernos a la hora de decidir implementar la tecnología en el sistema de salud, y refuerza nuestro argumento de que el responsable del tratamiento debe cumplir con el

[5]Naciones Unidas. Pacto Internacional de Derechos Civiles y Políticos. Última consulta el 4 de octubre de 2022. Disponible en https://www.ohchr.org/es/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights

[6]La privacidad se entiende aquí como lo que tiene "cualidad de privado o no público" y "No es sinónimo de intimidad ('ámbito íntimo, espiritual o físico, de una persona')" (RAE). Ultima consulta el 4 de octubre de 2022. Disponible en https://www.rae.es/dpd/privacidad. En España, el derecho a la intimidad viene consagrado en la Constitución Española, Título I (De los derechos y deberes fundamentales), Capítulo Segundo (Derechos y libertades), Sección 1ª (De los derechos fundamentales y de las libertades públicas), artículo 18.

[7]OCDE. Última consulta el 4 de octubre de 2022. Las directrices de la OCDE sobre protección de la privacidad y flujos transfronterizos de datos personales de 1980, revisadas en 2013. Disponible en https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm. Véase también Amnistía Internacional Argentina. Última consulta el 14 de agosto de 2021. Disponible en https://amnistia.org.ar/los-estados-deben-respetar-los-derechos-humanos-al-emplear-apps-para-combatir-la-pandemia-del-covid-19/.

derecho de información para garantizar la transparencia de los datos, el acceso a los datos siendo automático en lugar de requerir la habilidad del usuario para su obtención.

Los principios de las directrices de la OCDE han sido ampliamente aceptados. La principal diferencia es su aplicación entre Europa y Estados Unidos. Mientras en Europa existe una amplia legislación de protección de datos aplicada por las autoridades públicas, en EE.UU., la regulación de la privacidad se desarrolla para cada sector de la economía y se basa en la aplicación privada y la autorregulación. En EE.UU., los individuos están poco protegidos y rara vez son conscientes de las opciones que ofrecen las políticas de privacidad y pueden aceptarlas sin saberlo. Además, en este país la anonimización de los conjuntos de datos mediante la desidentificación ha sido la principal herramienta utilizada para abordar los problemas de privacidad. Sin embargo, un estudio reciente realizado en EE.UU. reveló que el 99,98% de los estadounidenses serían reidentificados correctamente en cualquier conjunto de datos utilizando 15 atributos demográficos como la edad, el sexo y el estado civil (Rocher et al., 2020).

La sociedad debe exigirles a quienes eligieron para que los representen, que las medidas que implementen se encuentren enmarcadas en un marco normativo y regulatorio que garantice transparencia y vele por la igualdad y el resguardo de los derechos de todos los habitantes. Las aplicaciones digitales en salud traen aparejado el surgimiento de nuevos derechos, tales como el derecho a la portabilidad del dato, derecho al olvido, derecho a no ser objeto de toma de decisiones automatizadas, entre otros y frente a ello surge el siguiente interrogante: ¿resulta suficiente el marco normativo existente a nivel internacional y/o nacional para asegurar la protección de los derechos que dicho marco pregona?¿están estos nuevos derechos alcanzados por los marcos normativos vigentes?

Es allí donde deben poner especial atención los gobiernos que decidan implementar su uso, en un marco normativo que proteja íntegramente los derechos de los usuarios y que sea lo suficientemente flexible para adaptarse a los avances de la tecnología. Sin un marco normativo como tal, los usuarios de las aplicaciones y sus datos, se encuentran expuestos y librados a la mera voluntad y decisión de los gobernantes, posicionándolos en una situación irreversible de vulnerabilidad innecesaria. Se corre el riesgo de que la garantía de la no reidentificación desaparezca y los datos personales y sensibles sean utilizados para fines totalmente desconocidos.

Dicho marco normativo debe velar para que no se continúen reproduciendo y replicando inequidades que se suscitan en la actualidad.

3. Conclusión

Las aplicaciones digitales en salud implementadas como consecuencia del contexto de pandemia por COVID-19 han llegado para quedarse. Sin lugar a dudas, que los estados comenzarán a valerse de diversas aplicaciones digitales en salud para la toma de decisiones en materia sanitaria. Esto no debe ser considerado como algo negativo sino todo lo contrario.

El uso de la tecnología en salud es necesario para adecuar el sistema a los tiempos presentes, y a la transformación digital que nos encontramos atravesando a nivel mundial.

Sin embargo, es fundamental que se arbitren nuevas formas de gobernanza en el uso de dichas aplicaciones y que todos los implicados en su uso –titulares de datos y organismos gubernamentales— participen en la implementación y desarrollo de las mismas. Debemos exigir transparencia y rendición de cuentas en los procesos de generación y transferencia de conocimiento en el sector de la salud. El uso de los datos personales y sensibles no puede, o no debe, resultar indiferente ni quedar librado al azar y a las decisiones de unos pocos.

Debemos velar para que el conjunto de datos que se manipulan a partir del uso de dichas aplicaciones se encuentren verdaderamente protegidos y considero que una herramienta fundamental para que esto pueda lograrse es promoviendo el desarrollo de infraestructuras públicas propias para la gestión de dichos datos junto con un marco normativo que contemple acabadamente todos los aspectos que el uso de dichas aplicaciones suscita. En particular, nos parece razonable que se puedan establecer leyes de seguridad nacional en estados soberanos, con la participación imprescindible de los organismos internacionales de salud para establecer marcos normativos.

Cualquiera que sea el sistema de implementación elegido, los principios de privacidad, confidencialidad, calidad de los datos, proporcionalidad, minimización del dato, igualdad, licitud, equidad, entre otros, deben encontrarse garantizados y protegidos no sólo a la hora de usar las aplicaciones sino también a la hora de trabajar en un marco normativo que respalde dicho uso y que empodere a la ciudadanía.

La privacidad y la innovación provocadas por la tecnología no deben ser posicionados como valores en conflicto, pueden y deben convivir al mismo tiempo, armonizándose para que la sociedad pueda avanzar hacia un uso de la tecnología más consciente, responsable y eficaz. Aunque este artículo se ha centrado en la protección contra el uso indebido de datos sensibles, consideramos que la transformación digital de la salud es positiva para las Américas si el respeto de los derechos está en su centro. Así que compartimos los objetivos de un reciente documento elaborado por la Organización Panamericana de la Salud (OPS) en 2021 para ayudar a los Estados a tomar decisiones inclusivas y sostenibles. Este documento ofrece “ocho principios rectores de la transformación digital del sector de la salud.” Los ocho principios son: conectividad universal, bienes públicos digitales, salud digital inclusiva, interoperabilidad, derechos humanos, inteligencia artificial, seguridad de la información y arquitectura de salud pública. Ahora que esa reflexión está en marcha, corresponde a los actores de la transformación digital garantizar que una ética protectora, inclusiva y sostenible esté en el centro de la innovación.

Supplementary Material

Refer to Web version on PubMed Central for supplementary material.

Agradecimientos

La investigación presentada en esta publicación fue apoyada por el Centro Internacional Fogarty de los National Institutes of Health bajo el número de subsidio R25TW001605. El contenido es responsabilidad exclusiva de las/los autoras/es y no representa necesariamente las opiniones oficiales de los National Institutes of Health.

Referencias

Creus J, Guanyabens J,Balestrini M,Righi V,Barbiero A,Masfarré G,Campins G, Arguedas D SALUS.COOP. Towards citizen governance and management of health data. Ideas for change + Mobile World Capital, Barcelona Foundation, December, 2016. Disponible en: https://www.ideasforchange.com/en/tools/saluscoop-report. Fecha de consulta: 14 de agosto de 2021.

de Lecuona I (Coord.), "Pautas para evaluar proyectos de investigación e innovación en salud que utilicen tecnologías emergentes y datos personales", Observatorio de Bioética y Derecho - Cátedra UNESCO de Bioética, Universidad de Barcelona, 2020. ONLINE: http://www.bioeticayderecho.ub.edu/sites/default/files/documents/doc_eval-proyectos.pdf.

_____, "Aspectos éticos, legales y sociales del uso de la inteligencia artificial y el Big Data en salud en un contexto de pandemia", Revista internacional de pensamiento político, Nº. 15, 2020, págs. 139–166.

Ley N° 25.326. Protección de Datos Personales. Boletín Oficial de la República Argentina 02 de noviembre del 2000. Disponible en: https://www.boletinoficial.gob.ar/detalleAviso/primera/7209468/20001102?busqueda=1.

Organización Mundial de la Salud. Alocución de apertura del Director General de la OMS en la rueda de prensa sobre la COVID-19 celebrada el 11 de marzo de 2020. Disponible en: https://www.who.int/es/director-general/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing-on-covid-19---11-march-2020. Fecha de consulta: 14 de agosto de 2021.

Pan American Health Organization (2021). "8 Principles for Digital Transformation of Public Health Disponible en: https://www3.paho.org/ish/index.php/en/8-principles. Fecha de consulta: 14 de agosto de 2021.

Rocher L, Hendrickx JM & de Montjoye YA. Estimating the success of re-identifications in incomplete datasets using generative models. Nat Commun 10, 3069 (2019). 10.1038/s41467-019-10933-3. [PubMed: 31337762]

World Health Organization (2020). "Ethical considerations to guide the use of digital proximity tracking technologies for COVID-19 contact tracing. Interim guidance 28 May 2020." Disponible en: https://apps.who.int/iris/bitstream/handle/10665/332200/WHO-2019-nCoV-Ethics_Contact_tracing_apps-2020.1-eng.pdf. Fecha de consulta: 14 de agosto de 2021.

____ (2020). Proyecto de estrategia mundial sobre salud digital 2020–2025 Disponible en: https://www.who.int/docs/default-source/documents/200067-lb-full-draft-digital-health-strategy-with-annex-cf-6jan20-cf-rev-10-1-clean-sp.pdf?sfvrsn=4b848c08_2.

Tabla 1:

Requisitos legales, éticos y sociales que garantizan una mínima protección de derechos fundamentales.

Requisito	Explicación
Control	La recolección y el uso de los datos debe estar sujeta a una supervisión independiente, capaz de examinar la amplia gama de impacto en los derechos humanos más allá de la privacidad y la protección de datos personales.
Eficacia	La aplicación debe haber sido sometida a pruebas de eficacia y estar basada en evidencia científica que demuestre que contribuye al control del virus COVID-19.
Fin	La aplicación y los datos que esta recolecte puede ser utilizada solamente para controlar la propagación del virus COVID-19. Su uso debe estar dirigido a informar y proteger a las personas. Se debe evitar y prohibir cualquier otro uso.
Igualdad	La aplicación debe ser accesible para todas las personas. Los estados deben garantizar que los datos no se utilicen de manera que impacten desproporcionadamente en algunas personas como consecuencia de su situación particular, como la posición socioeconómica, el estatus migratorio o la edad.
Legalidad	Toda información que se obtenga a partir del uso de las aplicaciones debe estar autorizada por ley.
Límite	La aplicación debe ser utilizada durante un período de tiempo definido. La recolección de datos debe ser lo más limitada posible y los datos se deben almacenar en sitios seguros, confidenciales, y estar sujetos a eliminación dentro de un plazo determinado.
Minimización	La aplicación debe utilizar la mínima cantidad de datos posible.
Seudonimización	Deben establecerse medidas técnicas y organizativas para que el uso de las tecnologías con determinados fines en salud no permita la reidentificación de las personas, es decir, la no atribución de personalidad. La seudonimización debería exigirse por defecto[1].
Seguridad	Los datos recolectados deben ser eliminados tan pronto como sea posible luego de cumplido el fin específico declarado. La recolección y el uso de los datos debe finalizar cuando concluya la situación de emergencia.
Transparencia	Los Estados deben ser transparentes sobre la naturaleza y el alcance de la medida implementada, incluyendo con quiénes comparten los datos que recolectan. El código de uso de datos personales debe ser puesto en el dominio público, y el responsable del tratamiento debe cumplir con el derecho de información[2].
Voluntariedad	No se puede imponer el uso obligatorio de la aplicación. Su utilización debe ser voluntaria y debe poder ser desactivada y eliminada. No deben existir elementos de coerción o negociación de partes con poderes desiguales.

[1]Seudonimización: “tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyen a una persona física identificada o identificable”. Real Academia Española: Diccionario de la lengua española.

[2]Agencia Española de Protección de Datos. Derecho de información. Última consulta: el 4 de octubre de 2022. Disponible en https://www.aepd.es/es/derechos-y-deberes/conoce-tus-derechos/derecho-de-informacion.