ISSN 1015-5074

REVISTA IIDH
Enero - Junio 2022
75

REVISTA IIDH

INSTITUTO INTERAMERICANO DE DERECHOS HUMANOS
INSTITUT INTERAMÉRICAIN DES DROITS DE L'HOMME
INSTITUTO INTERAMERICANO DE DIREITOS HUMANOS
INTER-AMERICAN INSTITUTE OF HUMAN RIGHTS

75

Enero - Junio 2022

REVISTA

IIDH

Instituto Interamericano de Derechos Humanos
Institut Interaméricain des Droits de l'Homme
Instituto Interamericano de Direitos Humanos
Inter-American Institute of Human Rights

Revista
341.481
Revista IIDH/Instituto Interamericano de Derechos
Humanos.-Nº1 (Enero/junio 1985)
-San José, C. R.: El Instituto, 1985-
v.; 23 cm.

Semestral

ISSN 1015-5074
1. Derechos humanos-Publicaciones periódicas

Corrección de estilo: Jacinta Escudos

Portada, diagramación y artes finales: Marialyna Villafranca Salom

Impresión litográfica: Litografía Imprenta Versalles

La Revista IIDH acogerá artículos inéditos en el campo de las ciencias jurídicas y sociales, que hagan énfasis en la temática de los derechos humanos. Los artículos deberán dirigirse a: Editores Revista IIDH; Instituto Interamericano de Derechos Humanos; A. P. 10.081-1000 San José, Costa Rica.

Se solicita atender a las normas siguientes:

1. Se entregará un documento en formato digital que debe ser de 45 páginas, tamaño carta, escritos en Times New Roman 12, a espacio y medio.
2. Las citas deberán seguir el siguiente formato: apellidos y nombre del autor o compilador; título de la obra (en letra cursiva); volumen, tomo; editor; lugar y fecha de publicación; número de página citada. Para artículos de revistas: apellidos y nombre del autor, título del artículo (entre comillas); nombre de la revista (en letra cursiva); volumen, tomo; editor; lugar y fecha de publicación; número de página citada.
3. La bibliografía seguirá las normas citadas y estará ordenada alfabéticamente, según los apellidos de los autores.
4. Un resumen de una página tamaño carta, acompañará a todo trabajo sometido.
5. En una hoja aparte, el autor indicará los datos que permitan su fácil localización (Nº fax, teléf., dirección postal y correo electrónico). Además incluirá un breve resumen de sus datos académicos y profesionales.
6. Se aceptarán para su consideración todos los textos, pero no habrá compromiso para su devolución ni a mantener correspondencia sobre los mismos.

La Revista IIDH es publicada semestralmente. El precio anual es de US $40,00. El precio del número suelto es de US$ 25,00. Estos precios incluyen el costo de envío por correo regular.

Todos los pagos deben de ser hechos en cheques de bancos norteamericanos o giros postales, a nombre del Instituto Interamericano de Derechos Humanos. Residentes en Costa Rica pueden utilizar cheques locales en dólares. Se requiere el pago previo para cualquier envío.

Las instituciones académicas, interesadas en adquirir la Revista IIDH, mediante canje de sus propias publicaciones y aquellas personas o instituciones interesadas en suscribirse a la misma, favor dirigirse al Instituto Interamericano de Derechos Humanos, A. P. 10.081-1000 San José, Costa Rica, o al correo electrónico: s.especiales2@iidh.ed.cr.

Publicación coordinada por Producción Editorial-Servicios Especiales del IIDH

Instituto Interamericano de Derechos Humanos
Apartado Postal 10.081-1000 San José, Costa Rica
Tel.: (506) 2234-0404 Fax: (506) 2234-0955
e-mail:s.especiales2@iidh.ed.cr
www.iidh.ed.cr

Índice

Presentación

Para el Instituto Interamericano de Derechos Humanos es motivo de gran satisfacción la salida a la luz pública de su Revista IIDH número 75, la más reciente de una tradición que comenzó en 1985, y que durante 37 años continúa difundiendo doctrina y debates especializados en materia de derechos humanos. En esta edición el IIDH hace un homenaje a uno de sus cursos de formación más emblemáticos, el Curso Interdisciplinario en Derechos Humanos. El Curso Interdisciplinario se lleva a cabo anualmente desde 1983, por lo que en el presente año 2022 sumará 40 ediciones.

El Curso es un espacio intersectorial y multidisciplinario permanente para la capacitación en derechos humanos y el Sistema Interamericano de protección, así como para el intercambio de visiones y experiencias de personas provenientes de las entidades de la sociedad civil, las instituciones públicas y los organismos internacionales, que trabajan en favor de la vigencia efectiva de los derechos humanos y la creación y fortalecimiento de la institucionalidad y convivencia democráticas. A la fecha es reconocido como el punto de convergencia académico más importante para el movimiento de derechos humanos en las Américas, entre sus miles de exalumnos/as se cuenta buena parte de los líderes y activistas de derechos humanos en el continente.

Por lo tanto, para este número de la Revista se han elegido contribuciones académicas de personas que han formado parte del Curso, ya sea como exalumnos y exalumnas, como parte de su cuerpo docente, o que son cercanas colaboradoras de

este Instituto en sus acciones de promoción y protección. Los artículos abordan situaciones contemporáneas en materia de derechos humanos, con las que se busca contribuir a ahondar en el debate en este campo y a propiciar el desarrollo de nuevos conocimientos.

Brevemente, a continuación se reseñan los artículos que contiene esta edición, comenzando con la contribución de Camila Denise Beguiristain. Su artículo *Gestación por sustitución: las minorías o mayorías frente a la última palabra de jueces y juezas* busca demostrar cómo el poder judicial, a través de una actitud dialógica, podría activar la labor legislativa para garantizar los derechos (no) reproductivos -en particular, la gestación por sustitución- del colectivo LGBTI. Para ello, desarrolla el criterio de (no) discriminación por sexo y orientación sexual en torno al colectivo LGBTI; explica la gestación por sustitución como técnica de reproducción humana asistida y su vinculación con los DESCA; evidencia los inconvenientes del control robusto de constitucionalidad-convencionalidad; manifiesta las particularidades que adquiere dicho mecanismo en la justiciabilidad de los DESCA; y expone alternativas de discusión para sortear la -inevitable- ¨última palabra¨ de los jueces y juezas frente a conflictos de discriminación estructural y omisión política.

Por su parte, Eduardo Bertoni en *El Impacto por las Medidas de Salud Pública en torno a la Pandemia de Covid-19,* explora la discusión sobre los beneficios de Internet y otras tecnologías para la sociedad, pero también sus efectos al permitir o coadyuvar con posibles violaciones de derechos humanos durante la pandemia. El artículo resume las conclusiones de estudio más amplio (disponible en la página web del IIDH) sobre el impacto en ciertos derechos humanos por parte de normas específicas promulgadas durante o para combatir la enfermedad. El estudio

busca completar un vacío en los esfuerzos para avanzar de mejor manera en la protección de los derechos humanos en un momento en que, por un lado, el uso de la tecnología se vuelve cada vez más crítico, y, por el otro, ante una emergencia sanitaria de proporciones no afrontadas anteriormente.

En *Nuevas posibilidades de comunicación, nuevos peligros, nuevos desafíos: La libertad de expresión y el discurso de odio en internet,* Martina Brun Pereira, Brahian Furtado Duarte, Belén Hernández Rimoldi y Federico Pereyra Burghi observan que el devenir de la modernidad y la globalización han generado un cambio significativo en la estructura de la sociedad donde expresiones vinculadas al discurso del odio, hacen necesaria su regulación. Sin embargo, desde su perspectiva, la ausencia de normativa favorece su proliferación ante la dificultad de determinar cuándo estas manifestaciones se convierten en un ejercicio abusivo de la libertad. Por lo tanto, su artículo analiza si tal discurso goza de protección jurídica en cuanto ejercicio de la libertad de expresión, o si suponen un ejercicio abusivo, quedando fuera de toda protección del ordenamiento jurídico. Asimismo, se consideran posibles herramientas para abordar esta problemática de manera eficiente.

En el artículo *Acceso a la Información Pública: aplicación de la primera ley en Argentina y desafíos para la región,* Marcelo Krikorian hace un análisis de las experiencias de aplicación de la primera ley de Acceso a la Información en Argentina que se encuentra vigente desde el año 2017. El artículo reseña los principales aspectos de la ley y algunas resoluciones emblemáticas de su órgano garante, evidenciando que el trabajo de la Agencia de Acceso a la Información Pública ha significado el desarrollo de notables aportes para la protección de derechos relacionados con el acceso a la información. En particular, se abordan algunos casos que tuvieron lugar en el contexto de

la pandemia COVID-19, tales como información relacionada con los contratos para la adquisición de las vacunas, la política "Ingreso Familiar de Emergencia" e, incluso, la negociaciones con farmacéuticas realizadas vía correo electrónico. A partir de una serie de reflexiones finales, el artículo concluye reconociendo la Ley Modelo Interamericana sobre Acceso a la Información Pública y generando algunas recomendaciones para fortalecer esta agenda común en la región.

El artículo *Defender Derechos Humanos un derecho sin reconocer, una crisis latente,* Adriana Carolina Lozano Olarte e Yleana Montserrat Balboa Rivera analizan el derecho a defender los derechos humanos considerando que tiene un corto desarrollo tanto en el derecho internacional de los derechos humanos, como en los marcos nacionales y en la academia, por lo que su reconocimiento legal y teórico que desemboca en la protección jurídica de los derechos en los cuerpos normativos de cada país apenas está en proceso. Desde su perspectiva, esto abre una ventana de oportunidad para fundamentarlo desde los derechos humanos en medio de la coyuntura actual, en la que se hace necesaria su exigibilidad en medio de las realidades sociales y jurídicas que han desembocado específicamente en América Latina en una crisis, las cuales han permitido que se avive la vulneración de los derechos de aquellas personas que se dedican a la defensa de los derechos humanos.

En su artículo *La reunificación familiar de personas refugiadas y migrantes de Venezuela en la Región: Proceso de Quito,* Juan Sebastián Medina Canales observa el movimiento masivo de personas que atraviesan la carretera Panamericana a partir de la crisis política, social, económica e institucional que tiene lugar en Venezuela, con la esperanza de que otros Estados puedan acogerlos y permitirles empezar nuevamente. Su contribución busca describir los avances sobre la institución de

la familia versus la protección de esta frente a los escenarios de personas refugiadas y migrantes provenientes de Venezuela, sus cambios, normativas y procedimientos para su implementación como parte de las iniciativas presentadas dentro del Proceso de Quito.

Diego Mendy en su artículo denominado *Tratamiento actual de datos personales de salud e intimidad humana* repasa de manera breve las principales problemáticas que surgen en torno al tratamiento que se da de los datos personales de salud sobre el derecho a la privacidad. Al mismo tiempo, realiza una exposición concisa sobre las soluciones jurídicas actuales en ese rubro. El artículo observa que la aplicación de nuevas tecnologías a la atención médica significa una transformación de los servicios de salud pero a su vez conlleva importantes riesgos para la humanidad, especie que se enfrenta a un cúmulo de información sobre sí misma nunca antes alcanzado que tal vez permita su determinación algorítmica.

En el artículo *El control de Convencionalidad: Es posible la Aplicación y la interpretación por parte de la autoridad pública,* Carlos Ordaya López analiza de qué manera se aplicaría y se realizaría la labor interpretativa del control de convencionalidad por parte de la autoridad pública fuera del Poder Judicial, y como sería el procedimiento a seguir para una correcta aplicación e interpretación de la Convención, ante una norma interna que restringe o limita derechos humanos establecidos en la Convención Americana. Además, pretende establecer el mecanismo correcto para la aplicación e interpretación de este control, sin conllevar a inaplicar una norma interna o interpretar indebidamente la norma con el tratado internacional, ya que de acuerdo con la legislación nacional y jurisprudencial de determinados Estados, la autoridad pública no tiene las facultades para realizar el control difuso de carácter "administrativo".

Oscar Zumbi Rorra Rodríguez, en *Afrodescendientes en las Américas y el Derecho a la Educación: El caso de Uruguay,* analiza los avances en términos de equidad étnica–racial que hoy existen en Uruguay, particularmente sobre la conquista del derecho a la educación de la población afrouruguaya. Su análisis parte de un desafío, debido al escaso desarrollo de investigaciones sobre la educación desde una perspectiva étnico-racial en dicho país. Por lo tanto, su artículo hace una aproximación teórico-conceptual sobre raza, educación, desigualdad y derecho a la educación a partir de la consulta a material disponible a nivel nacional e internacional, incluyendo estudios sociodemográficos nacionales sobre los indicadores de educación y exclusión afrodescendiente. El estudio evidencia los avances pero también los desafíos para contrarrestar la brecha de desigualdad en el ámbito educativo que evidencia el racismo que aún permanece estructuralmente en la realidad del Estado uruguayo.

Concluyo esta presentación con el agradecimiento de siempre a la cooperación noruega, sin cuyo apoyo no sería posible la producción y difusión de nuestra Revista IIDH, al Consejo Consultivo Editorial por sus valiosos aportes, y a las autoras y autores por sus relevantes contribuciones.

José Thompson J.
Director Ejecutivo, IIDH
Instituto Interamericano de Derechos Humanos

El impacto en la privacidad por las medidas de salud pública en torno a la pandemia de COVID-19*

*Eduardo Bertoni***

1. El impacto de las medidas de salud pública implementadas durante la pandemia

La pandemia de COVID-19 tuvo y tiene un gran impacto en la salud, pero también en áreas como la educación, el trabajo, el entretenimiento y el comercio internacional. Por primera vez ocurre una emergencia sanitaria mundial al mismo tiempo que presenciamos un extraordinario avance de la tecnología. Sin

---

* En este artículo se exponen algunos hallazgos que surgieron de una investigación más extensa y que puede ser consultada en el sitio web del IIDH en www.iidh.ed.cr. La investigación fue realizada desde la Oficina Regional para América del Sur del IIDH y dirigida por su representante, Dr. Eduardo Bertoni. Por razones de espacio aquí se han incluido especialmente las conclusiones y las recomendaciones que se propusieron. El IIDH agradece el apoyo de la Fundación Ford sin la cual esta investigación no hubiera sido posible.

** Representante y Coordinador de la Oficina Regional para América del Sur del Instituto Interamericano de Derechos Humanos -IIDH-,. Ex Director de la Agencia de Acceso a la Información Pública y de la Dirección Nacional de Protección de Datos Personales, Jefatura de Gabinete de Ministros, Argentina (2016-2020). Fundador del Centro de Estudios en Libertad de Expresión y Acceso a la Información (CELE) de la Facultad de Derecho e la Universidad de Palermo (2009-2016). Ex-Director Ejecutivo de Due Process of Law Foundation (DPLF) con sede en Washington D.C. hasta mayo de 2009. Entre 2002 y 2005, Relator Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos (CIDH) en la Organización de Estados Americanos (OEA).

embargo, hay relativo consenso en que las leyes y regulaciones que gobiernan internet y otras tecnologías, carecen de las protecciones sólidas necesarias para garantizar un adecuado ejercicio de los derechos fundamentales.

Es importante destacar y no soslayar la discusión sobre los beneficios de internet y otras tecnologías para la sociedad, pero también sus efectos al permitir o coadyuvar con posibles violaciones de derechos humanos durante la pandemia.

Para ello, el IIDH estudió el impacto en Argentina, Chile y Uruguay sobre ciertos derechos humanos de normas específicas promulgadas durante o para combatir la enfermedad. Cabe destacar que ese estudio incluye no solo a normas relacionadas con internet y otras tecnologías sino también a otras normas no vinculadas directamente con el entorno digital.

Este artículo pretende complementar un vacío en los esfuerzos para avanzar de mejor manera en la protección de los derechos humanos en un momento en que, por un lado, el uso de la tecnología se vuelve cada vez más crítico, y, por el otro, ante una emergencia sanitaria de proporciones no afrontadas por la humanidad en tiempos recientes, se adoptaron medidas extremas para intentar paliar los efectos en la salud de las personas.

2. Las regulaciones en Argentina, Chile y Uruguay que tuvieron impacto en la privacidad

2.1 Pandemia y utilización de tecnologías de vigilancia

Durante la pandemia, la tecnología jugó un rol fundamental, tanto positivo como negativo. En lo primero, y como ejemplo más

claro, la utilización de distintas tecnologías fue lo que permitió la obtención de vacunas en tiempos que hubieran sido impensables en otros momentos de los estudios científicos en la lucha contra enfermedades.

Sin embargo, también se utilizaron tecnologías que pueden afectar los derechos que estamos abordando en esta investigación, especialmente el derecho a la privacidad y a la protección de datos personales. La habilitación para el uso de esas tecnologías se llevó a cabo a partir de regulaciones aprobadas por los Estados de los que se ocupa este estudio.

Es preciso destacar que asumimos la buena fe por parte de los gobiernos cuando se habilitó el uso de las tecnologías, toda vez que el fin que se buscó y que expresamente se dijo en las regulaciones estaba vinculado con la emergencia sanitaria y el objetivo de hacer frente a la pandemia que generó el COVID-19.

Sin embargo, por las razones que veremos, la habilitación del uso de esas tecnologías no tuvo las suficientes garantías para que no se produjeran injerencias “abusivas o arbitrarias” al derecho a la privacidad, cuestión que es central para la protección del derecho de acuerdo a los estándares internacionales. En otros casos, la habilitación de las tecnologías pudo no haber cumplido con el “test tripartito” exigido por los estándares internacionales (limitaciones a un derecho previstas en la ley, necesarias y proporcionadas), toda vez que, por ejemplo, las injerencias a la privacidad no estuvieran ordenadas por leyes, sino por decretos o autoridades administrativas.

Dos temas que resultan claves a tener en cuenta a la hora del análisis de estas cuestiones están vinculados con el consentimiento del titular para la utilización de sus datos personales y la proporcionalidad de las medidas.

Analizado cómo evolucionó la cuestión en el derecho comparado, se señala que:

> Durante los meses de marzo y abril de 2020, las diferentes agencias de protección de datos personales europeas y de otras jurisdicciones abordaron inmediatamente el tema de la pandemia del coronavirus y sus diversos aspectos de distintas maneras y con enfoques diferentes. En general todas lo hicieron espontáneamente publicando en sus canales informativos comunicados donde explicaban si era posible usar o ceder los datos sobre la enfermedad.
>
> […]
>
> En las opiniones de las distintas agencias, podemos diferenciar tres tipos de posturas:
>
> Enfoque restrictivo: se basa en aplicar en forma directa las leyes de protección de datos personales a las diversas situaciones relacionadas con la pandemia, como ser tratamiento en el ámbito laboral o por parte del Estado, exigiendo siempre el consentimiento del titular del dato personal.
>
> Enfoque neutral: se trata de una postura intermedia que tiene en cuenta los principios de datos personales, pero que permite recopilar datos con la finalidad de evitar contagio o amparar el lugar de trabajo del empleado, incluyendo límites como destrucción de los datos personales una vez finalizada la pandemia.
>
> Enfoque permisivo: este enfoque da prioridad al derecho a la salud y a la emergencia sanitaria por sobre las normas de protección de datos. Entre otras cosas permite compartir datos e incluso publicarlos cuando ello ayude a frenar el contagio[1].

1 Véase "Pandemia (COVID-19) y protección de datos personales. Primeras aproximaciones", Palazzi, Pablo A.; Elaskar, Mercedes, en revista *La ley*, del 13/05/2020, Argentina.

De acuerdo con ese estudio de derecho comparado surge que no hubo un consenso claro sobre la necesidad del otorgamiento del consentimiento para el tratamiento de los datos personales vinculados con la prevención de la expansión de la pandemia.

Sin embargo, no puede perderse de vista que, de los tres países analizados, dos (Argentina y Uruguay) son considerados países de legislación con protección adecuada para las regulaciones de la Unión Europea[2].

Ello reviste importancia porque a partir de la entrada en vigencia del "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 (Reglamento general de protección de datos, RGPD)"[3], las directrices emanadas del Comité Europeo de Protección de Datos" (CEPD constituyen una fuente interpretativa importante a tener en cuenta. Ello así, porque ambos países se encuentran sometidos a un proceso de revisión de su legislación y sus prácticas en vistas a la nueva normativa.

Expresado más precisamente, las características y contenido que surgen del RGPD al "consentimiento" como base legal para el tratamiento de datos personales adquiere relevancia para esos países a la hora del diseño de las aplicaciones como las que hemos visto.

2 Véase en: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_es. Último chequeo: 30 de agosto de 2021.

3 Véase en: https://www.boe.es/doue/2016/119/L00001-00088.pdf. Último chequeo: 30 de agosto de 2021.

Así las cosas, en mayo de 2020, el CEPD emitió las "Directrices 5/2020 sobre el consentimiento en el sentido del Reglamento (UE) 2016/679"[4].

En ese documento, luego de establecer claramente que el consentimiento es toda manifestación del titular de los datos personales que sea libre, informada, específica e inequívoca, se dan algunas pautas que son relevantes para esta investigación.

Por ejemplo, el documento destaca el desequilibrio de poder que existe cuando es el Estado el que reclama consentimiento, como es el caso de las aplicaciones que surgieron durante la pandemia. El CEPD determina que:

> No es probable que las autoridades públicas puedan basarse en el consentimiento para realizar el tratamiento de datos ya que cuando el responsable del tratamiento es una autoridad pública, siempre hay un claro desequilibrio de poder en la relación entre el responsable del tratamiento y el interesado. Queda también claro en la mayoría de los casos que el interesado no dispondrá de alternativas realistas para aceptar el tratamiento (las condiciones de tratamiento) de dicho responsable. El CEPD considera que hay otras bases jurídicas que son, en principio, más adecuadas para el tratamiento de datos por las autoridades públicas.

Un ejemplo que propone el documento como un caso de consentimiento válido es el siguiente:

> Un municipio está planificando obras de mantenimiento de carreteras. Dado que dichas obras pueden perturbar el tráfico durante un periodo largo de tiempo, el municipio ofrece a sus ciudadanos la oportunidad de suscribirse a una lista de correo electrónico con el fin de recibir información actualizada sobre el avance de las obras y sobre los retrasos previstos. El municipio deja claro que no existe la obligación de participar y pide el consentimiento para utilizar las direcciones de correo electrónico para este (único) fin. Los ciudadanos que no dan su consentimiento no se ven privados de ningún servicio básico del municipio o del ejercicio de ningún derecho, por ello tienen la capacidad de dar o negar libremente el consentimiento a este uso de los datos. La información sobre las obras estará también disponible en el sitio web del municipio.

4 Véase en: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_es.pdf. Último chequeo: 30 de agosto de 2021.

Y un ejemplo, aunque no vinculado con una aplicación estatal que no validaría el consentimiento es el siguiente:

> Una aplicación móvil para edición de fotografías pide a sus usuarios que tengan activada su localización GPS para el uso de sus servicios. La aplicación indica también a sus usuarios que utilizará los datos recogidos para fines de publicidad comportamental. Ni la geolocalización ni la publicidad comportamental son necesarias para la prestación del servicio de edición de fotografías y van más allá de lo necesario para prestar el servicio básico ofrecido. Dado que los usuarios no pueden utilizar la aplicación sin dar su consentimiento a estos fines, no puede considerarse que el consentimiento se haya dado libremente.

Por otro lado, el CEPD más adelante aclara que

> Un responsable del tratamiento debe tener también en cuenta que el consentimiento no puede obtenerse mediante la misma acción por la que el usuario acuerda un contrato o acepta los términos y condiciones generales de un servicio. La aceptación global de los términos y condiciones generales no puede considerarse una clara acción afirmativa destinada a dar el consentimiento al uso de datos personales. El RGPD no

> permite que los responsables del tratamiento ofrezcan casillas marcadas previamente o mecanismos de exclusión voluntaria que requieran la intervención del interesado para evitar el acuerdo (por ejemplo, «casillas de exclusión voluntaria»).

Además de la relevancia del RGPD, también debe observarse que dos de los países objeto de esta investigación (Argentina y Uruguay) han ratificado el Convenio 108[5] y uno (Uruguay) el conocido como Convenio 108+ y otro, a lo menos, es país signatario (Argentina)[6].

En consecuencia, también resultan relevantes las obligaciones que surgen de estos instrumentos en relación con el consentimiento de los titulares de los datos y la proporcionalidad de los datos recolectados teniendo en cuenta su finalidad.

5 Véase en: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108?module=signatures-by-treaty&treatynum=181. Último chequeo: 30 de agosto de 2021. El Convenio 108 es el único instrumento multilateral de carácter vinculante en materia de protección de datos personales, que tiene por objeto proteger la privacidad de los individuos contra posibles abusos en el tratamiento de sus datos. Dado que se encuentra abierta la adhesión a cualquier Estado –no miembro del Consejo de Europa–, es el único estándar vinculante que tiene el potencial de ser aplicado en todo el mundo, proporcionando seguridad jurídica y previsibilidad en las relaciones internacionales. Suscripto en 1981, el Convenio 108 se ha convertido en la columna vertebral de la legislación de protección de datos personales en Europa y en el resto del mundo. En virtud de este Convenio, los Estados Parte deben tomar las medidas necesarias en su legislación nacional para aplicar en su territorio los principios que el Convenio dispone, con el fin de garantizar un tratamiento adecuado de los datos personales y que los titulares de los datos puedan ejercer sus derechos.

6 Véase en: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108?module=signatures-by-treaty&treatynum=223. Último chequeo: 30 de agosto de 2021. El 10 de octubre de 2018, el Consejo de Europa, como consecuencia del avance de la tecnología, adoptó un Protocolo Adicional que modificó el Convenio 108, a los efectos de incrementar la protección de los datos personales, considerando la globalización de las actividades de procesamiento de datos y la circulación de la información.

Ello así, resulta importante tener en cuenta lo establecido en el documento *"Digital Solutions to Fight COVID-19"* publicado por el Consejo de Europa en octubre del 2020[7].

Allí puede leerse que:

> El artículo 5 del Convenio 108+ establece que el procesamiento de datos puede llevarse a cabo sobre la base del "consentimiento libre, específico, informado e inequívoco del interesado o de alguna otra base legítima establecida por la ley", que, según el informe explicativo de la Convención, incluye el tratamiento necesario para la protección de los intereses vitales del interesado o de otra persona, (...) para el cumplimiento de una obligación legal a la que está sujeto el responsable del tratamiento, y el tratamiento de datos realizado por motivos de interés público o por intereses legítimos superiores del responsable del tratamiento o de un tercero.

Más adelante se reconoce que: "Si bien el consentimiento es una de las posibles bases legales para procesar datos personales, los requisitos para que el consentimiento sea válido son difíciles de cumplir, especialmente en vista de la sensibilidad de los datos de salud y ubicación y, en las circunstancias de COVID-19, la presión para aceptar el procesamiento, debido al contexto excepcional de la pandemia".

Y en relación con la proporcionalidad se explica que:

> El carácter intrusivo de las medidas adoptadas durante la pandemia está en el centro de las reacciones de muchos actores, incluidas las autoridades de protección de datos, los parlamentos, los tribunales y la sociedad civil. El "justo equilibrio entre todos los intereses involucrados, ya sean

7 Véase en: https://rm.coe.int/prems-120820-gbr-2051-digital-solutions-to-fight-covid-19-text-a4-web-/16809fe49c. Último chequeo: 30 de agosto de 2021.

públicos o privados, y los derechos y libertades en juego" previsto en el artículo 5 del Convenio 108+ se ha evaluado en diferentes contextos.

Las medidas que no pueden lograr su propósito previsto nunca pueden considerarse proporcionadas. Sin embargo, la efectividad real de muchas medidas aún no ha sido probada y examinada, y los debates sobre la proporcionalidad de la injerencia en el derecho a la protección de datos, a la luz de la eficacia comprobada y real de la medida adoptada, continúan en curso.

Los Estándares de Protección de Datos Personales para los Estados Iberoamericanos[8], desarrollados y aprobados por la Red

8 Véase en: https://www.redipd.org/es/documentos/estandares-iberoamericanos. Último chequeo: 31 de agosto de 2021. De acuerdo a lo que se explica en la introducción del documento, "En el marco del XV Encuentro Iberoamericano de Protección de Datos, la Red Iberoamericana de Protección de Datos (RIPD o Red) ha aprobado y presentado oficialmente los llamados 'Estándares de Protección de Datos de los Estados Iberoamericanos', dando cumplimiento así a un objetivo largamente anhelado por todas las entidades integrantes de la misma, así como a uno de los acuerdos adoptados en la XXV Cumbre Iberoamericana de Jefes de Estado y de Gobierno, celebrada el 28 y 29 de octubre de 2016 en Colombia, relacionado con solicitar a la Red la elaboración de una propuesta para la cooperación efectiva relacionada con la protección de datos personales y privacidad. El texto ahora aprobado trata de dar respuesta a uno de los ejes de la estrategia acordada por la RIPD en noviembre de 2016 en Montevideo, plasmada en el documento 'RIPD 2020', consistente en 'impulsar y contribuir al fortalecimiento y adecuación de los procesos regulatorios en la región, mediante la elaboración de directrices que sirvan de parámetro para futuras regulaciones o para la revisión de las existentes'. En este sentido, los Estándares Iberoamericanos se constituyen en un conjunto de directrices orientadoras que contribuyan a la emisión de iniciativas regulatorias de protección de datos personales en la región iberoamericana de aquellos países que aún no cuentan con estos ordenamientos, o en su caso, sirvan como referente para la modernización y actualización de las legislaciones existentes".

Iberoamericana de Protección de Datos[9] resultan también otra fuente a tener en cuenta para el desarrollo de políticas públicas que involucren el tratamiento de datos personales aún durante una emergencia sanitaria.

En referencia a los temas que se han abordado, la necesidad de consentimiento como base legal del tratamiento y la proporcionalidad de los datos recolectados en función de la finalidad perseguida, los Estándares siguen criterios muy similares a los del RGPD que se expusieron más arriba.

Por ejemplo, el documento para Iberoamérica establece que el consentimiento se define como la "manifestación de la voluntad, libre, específica, inequívoca e informada, del titular a través de la cual acepta y autoriza el tratamiento de los datos personales que le conciernen".

Vinculado con la proporcionalidad, se establece que podrán tratarse "únicamente los datos personales que resulten adecuados, pertinentes y limitados al mínimo necesario con relación a las finalidades que justifican su tratamiento".

En lo que sigue se citarán los ejemplos que se relacionan con regulaciones que son las más cuestionables en lo que se refiere a la protección de la privacidad y los datos personales.

2.2 Pandemia y ciber vigilancia

En la República Argentina, el Ministerio de Seguridad aprobó un "Protocolo General para la Prevención Policial del Delito con Uso de Fuentes Digitales Abiertas" mediante la Resolución 144 del 31 de mayo de 2020.

9 Véase en: https://www.redipd.org/es/la-red/historia-de-la-red-iberoamericana-de-proteccion-de-datos-ripd. Último chequeo: 31 de agosto de 2021.

El dictado de esta resolución Ministerial estuvo relacionado de manera explícita con la emergencia sanitaria que se había decretado en Argentina mediante el DNU 260/20. Asimismo, la resolución se hace cargo, también explícitamente, de la necesidad de proteger los derechos humanos, incluso al implementar las medidas que propone el protocolo que se aprueba.

Por ejemplo, en la resolución Ministerial se reconoce que la Resolución No. 1 de la CIDH del 10 de abril del 2020, se recomendó a los Estados:

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

De acuerdo con lo que establece la Resolución Ministerial que venimos tratando, el protocolo que aprueba tiene por finalidad establecer principios, criterios y directrices generales para las tareas de prevención del delito que desarrollan en el espacio cibernético los cuerpos policiales y fuerzas de seguridad. Aclara que las tareas de prevención policial del delito en el espacio cibernético se llevarán a cabo únicamente mediante el uso de fuentes digitales abiertas, entendiendo por "fuentes digitales abiertas" a los medios y plataformas de información y comunicación digital de carácter público, no sensible y sin clasificación de seguridad, cuyo acceso no implique una

vulneración al derecho a la intimidad de las personas, conforme lo normado en la Ley de Protección de Datos Personales No. 25.326 y sus normas reglamentarias.

Por su lado, a la hora de determinar cuáles delitos se pretenden prevenir se incluyen los siguientes:

> Art. 3: Delitos Concretos Objeto de la Prevención. La prevención policial del delito en el espacio cibernético procurará el conocimiento de posibles conductas delictivas cuyo acaecimiento sea previsible en función de la emergencia pública en materia sanitaria […] en virtud de la Pandemia declarada por la Organización Mundial de la Salud (OMS) en relación con el coronavirus COVID-19; atendiendo al desarrollo de la criminalidad vinculada a la comercialización, distribución y transporte de medicamentos apócrifos y de insumos sanitarios críticos; a la venta de presuntos medicamentos comercializados bajo nomenclaturas y referencias al COVID-19 o sus derivaciones nominales, sin aprobación ni certificación de la autoridad competente; y a los ataques informáticos a infraestructura crítica —especialmente a hospitales y a centros de salud—; […]
>
> Asimismo, en tanto se advierta que resulten sensibles al desarrollo de la emergencia pública en materia sanitaria […] podrán definirse como objeto de las tareas de prevención policial con uso de fuentes digitales abiertas, posibles conductas delictivas cuyo medio comisivo principal o accesorio incluya la utilización de sistemas informáticos con el fin de realizar acciones tipificadas penalmente como la trata de personas; el tráfico de estupefacientes; el lavado de dinero y terrorismo; conductas que puedan comportar situaciones de acoso y/o violencia por motivos de género, amenaza y/o extorsión de dar publicidad a imágenes no destinadas a la publicación; y delitos

> relacionados con el *grooming* y la producción, financiación, ofrecimiento, comercio, publicación, facilitación, divulgación o distribución de imágenes de abuso sexual de niñas, niños y adolescentes.

Es de destacar que la normativa se haya preocupado por establecer claramente, tanto en el Protocolo como en la Resolución que lo aprobó, que las acciones no podían vulnerar el derecho a la privacidad y los datos personales. Sin embargo, las tareas que habilitan a las fuerzas de seguridad para ocuparse de un amplio espectro de actividades de prevención no brindan las garantías adecuadas para la protección de la privacidad.

La preocupación por esta normativa fue advertida tanto por organizaciones no gubernamentales como por la propia autoridad de control en Argentina, la Agencia de Acceso a la Información Pública, AAIP.

En un comunicado oficial, Amnistía Internacional expresó que:

> Luego de un proceso de consulta con diversos actores y organizaciones, el Ministerio de Seguridad de la Nación aprobó un nuevo protocolo para la prevención policial del delito con uso de fuentes digitales abiertas a través de la **resolución 144/2020**, publicada en el Boletín Oficial. El protocolo, vigente durante el período de la emergencia sanitaria, establece principios, criterios y directrices generales para las actuaciones de prevención del delito que desarrollan los cuerpos policiales y fuerzas de seguridad mediante el uso de fuentes digitales abiertas.
>
> El nuevo protocolo aprobado incorpora muchas de las recomendaciones sugeridas por la sociedad civil como por ejemplo principios de transparencia y rendición de cuentas, así como la responsabilidad por uso abusivo y violatorio de las tareas de investigación. También establece que la capacitación y formación a las personas encargadas de estas tareas incluyan perspectiva de derechos humanos.
>
> Sin embargo, la guía aprobada aún autoriza a las fuerzas de seguridad a realizar actividades de investigación preliminar o prevención de delitos en lugar de restringirlas a casos en los que existe un marco judicial aplicable a una investigación concreta. Este tipo de actividad generalizada de vigilancia puede afectar el derecho a la privacidad y a la libertad de expresión. Por esta razón, la investigación en fuentes abiertas debería aplicarse en situaciones muy excepcionales, con el debido marco legal, y con un amplio debate parlamentario con participación social.

El Centro de Estudios Legales y Sociales, CELS, concluyó en un detallado estudio[10] que:

> El Ministerio de Seguridad señaló en la presentación del protocolo que el "ciberpatrullaje" tiene como fin el control del aislamiento social preventivo y obligatorio. El proyecto además circunscribe el protocolo a la vigencia del DNU 297/2020. Sin embargo, no está realmente explicado por qué este protocolo es una herramienta específica para intervenir en estos momentos de emergencia. Las fuerzas de seguridad tienen herramientas normativas suficientes para hacer cumplir las medidas sanitarias. Si lo que se necesita es mejorar la prevención e investigación de delitos informáticos, no parece ser esta tampoco la herramienta correcta, tal como lo demuestran los casos relevados. Si de lo que se trata es de mejorar las capacidades de inteligencia criminal para la detección de fenómenos concretos, tampoco es este el protocolo adecuado. Tampoco parece necesario instrumentar regulaciones de emergencia que puedan afectar el derecho a la

10 Véase en: https://www.cels.org.ar/web/wp-content/uploads/2020/04/CELS-sobre-protocolo-ciberpatrullaje.pdf. Última consulta: 23 de agosto de 2021.

privacidad y a la libertad de expresión sin un debate público y legislativo.

La Asociación por los Derechos Civiles (ADC) también manifestó en un estudio[11] una serie de preocupaciones sobre el Protocolo porque:

- Legitima la prevención policial de expresiones, no de conductas. Esta actividad ha sido denominada coloquialmente "ciberpatrullaje" ya que se la pretende asimilar a las tareas de prevención que la Policía realiza en los espacios públicos (calles, plazas, parques, etc.). Sin embargo, esta identificación omite una diferencia sustancial. La prevención policial tiene como objeto principal la disuasión de conductas ilícitas que puedan tener una consecuencia directa e inmediata en la vida, la integridad física o la propiedad de una persona. Tenemos policías en la calle para que actúen en caso de que una persona agreda a otra, le apunte con una pistola para asaltarla, destruya un negocio, intente entrar a una casa para robar, etc. Por el contrario, el ciberpatrullaje se enfoca principalmente en el discurso, es decir, en comentarios, mensajes, posteos y demás formas de comunicación en internet. Es decir, el objeto de la vigilancia son expresiones que en general, no ponen en riesgo de manera inmediata los bienes e intereses de una persona […]

- Dificulta que las fuerzas de seguridad respondan por su accionar. El control ciudadano de las fuerzas de seguridad es esencial para que las personas mantengan la confianza en el sistema. […] No hay forma de saber si en este momento la Policía está revisando nuestros comentarios. […] No tenemos información acerca de las páginas que se visitan y si la tenemos, solo nos queda confiar en la palabra de las autoridades. La esperanza de que una ciudadana o una periodista registre un posible caso de abuso es ínfima. El ciberpatrullaje posee un secretismo intrínseco a su modo de funcionamiento. Por eso, debemos tener mucho cuidado con su utilización.

- Supone que los datos provenientes de fuentes de acceso público no merecen un alto nivel de protección.

11 Véase en: https://adc.org.ar/wp-content/uploads/2021/07/ADC-La-protecci%C3%B3n-del-espacio-c%C3%ADvico-en-l%C3%ADnea-07-2021.pdf. Última consulta: el 23 de agosto de 2021.

La autoridad de control para la protección de datos personales, AAIP, entendió que, a efectos de cumplir con la regulación vigente en materia de protección del derecho humano a la privacidad, el Protocolo debía ser revisado y sugirió la suspensión de la aplicación del Protocolo hasta tanto se revisara su adecuación a la normativa en materia de protección de datos personales[12].

Por lo expuesto puede concluirse que esta regulación podría estar vulnerando de manera abusiva la privacidad y los datos personales.

En Chile, como consecuencia de la emergencia sanitaria decretada por el Decreto No. 104, cuando se declaró Estado de Excepción Constitucional de Catástrofe que se menciona más arriba, se dispuso la limitación de garantías constitucionales, donde el desplazamiento solo fue posible para aquellas personas habilitadas a través de permisos temporales, salvoconductos y permisos únicos de uso colectivo, los cuales a partir de marzo de 2020 se obtenían a través del sitio web www.comisariavirtual.cl.

En lo que va desde la declaración del Estado de Excepción Constitucional, el sitio web de Comisaría Virtual se ha transformado en un elemento fundamental para el control y

12 Véase en: https://www.argentina.gob.ar/sites/default/files/no-2020-47326285-apn-aaip.pdf. Última consulta: 23 de agosto de 2021.

fiscalización del cumplimiento de las medidas sanitarias que ha impuesto la autoridad. A partir de la información que mantienen en sus registros, sumado a otras fuentes de información se puede identificar a las personas infractoras al artículo 318 del Código Penal, que sanciona al "... que pusiere en peligro la salud pública por infracción de las reglas higiénicas o de salubridad, debidamente publicadas por la autoridad, en tiempo de catástrofe, epidemia o contagio, será penado con presidio menor en su grado mínimo o multa de seis a veinte unidades tributarias mensuales".

El Consejo para la Transparencia elaboró un informe sobre la posible afectación de distintos derechos mediante la utilización de esa plataforma[13]. En ese informe se concluye que:

> A partir del análisis de los permisos temporales individuales y los salvoconductos individuales y de uso colectivos entregados en el periodo comprendido entre el 22 de marzo y el 13 de junio de 2020, se observa una gran cantidad de datos personales, tales como domicilio, fecha de nacimiento, nacionalidad, nombres, apellidos, RUN, correo electrónico, estados de salud, empleador, etc., con los que se puede concluir sobre hábitos personales, los que revisten el carácter de dato sensible.
>
> De acuerdo a la naturaleza de los datos almacenados, el amplio espectro de los mismos y el universo infinito de personas a quien está dirigida, se observa una tardía inscripción o registro del banco de datos, por parte te Carabineros de Chile, en los términos que establece la Ley 19.628, que aun cuando sea una norma que carece de actualización acorde a los avances tecnológicos, constituye el marco normativo básico, que debe ser respetado por los organismos del Estado; sin embargo, la inscripción se realizó a casi 5 meses desde la declaración, a través del decreto supremo No. 104, de 18 de marzo de 2020, del Ministerio del Interior y Seguridad Pública, del estado de excepción constitucional de catástrofe, por calamidad pública, en todo el territorio nacional.
>
> Por otro lado, la política de privacidad del sitio web de Comisaría virtual, contiene información genérica respecto del sistema "SIMPLE", cómo se usa, métodos de recolección de información, finalidad de la recolección de datos y sustento jurídico del tratamiento de los datos personales. En sentido, se constatan deficiencias al respecto, toda vez que no existe información en cuanto a posibles transferencias de datos, derechos de los titulares de los datos y tiempo de conservación de la información, pese al deber de informar que tienen los organismos de la administración del Estado.

13 Véase en: https://www.consejotransparencia.cl/wp-content/uploads/2020/12/Informe-FF-Comisari%CC%81a-Virtual.pdf. Última consulta: 23 de agosto de 2021.

En definitiva, los sistemas de ciberpatrullaje implementados durante la pandemia, aún llevados adelante como consecuencia de buenas intenciones y buena fe, han demostrado un peligroso uso de las tecnologías que lo permitían en relación con una adecuada protección del derecho a la privacidad.

2.3 Pandemia y aplicaciones para geolocalización y control de la salud

En los tres países analizados se desarrollaron aplicaciones en el marco de la emergencia sanitaria y tal como lo explica una regulación de la República Argentina, resultó necesario "hacer uso de la tecnología con el fin de facilitar […] el cuidado de la población en su totalidad".

Estas aplicaciones fueron cuestionadas desde distintos sectores, aunque no siempre esos cuestionamientos fueron avalados por las autoridades de control de los respectivos países.

Desde la perspectiva del "consentimiento" como base legal para permitir el tratamiento de los datos personales, resulta importante analizar la situación planteada en la República Argentina a partir de regulaciones que impusieron la obligatoriedad de la utilización de la aplicación COVID-19-Ministerio de Salud (conocida luego como "*Cuidar*").

Esta aplicación fue implementada por la Decisión Administrativa No. 432 del jefe de Gabinete de Ministros del 23 de marzo de 2020 (DA 432/2020). Esta normativa facultó a la Dirección Nacional de Migraciones a "requerir previamente al ingreso al país a los viajeros y las viajeras que regresen desde el exterior, la adhesión a esta Aplicación o en su defecto a la página web, debiendo ponerlos en conocimiento de las Bases y Condiciones de utilización de la misma".

De las Bases y Condiciones (en realidad, el título cuando se accede es "Términos y Condiciones")[14], hay un capítulo especial denominado "Políticas de Privacidad".

Entre otras cuestiones, se explica lo siguiente:

> El Usuario que utilice el sitio web podrá proporcionar algunos datos personales a efectos de mantenerse en contacto y recibir información respecto de servicios que se pongan a disposición de la persona en relación a los servicios utilizados. […]
>
> En ningún caso proporcionar los datos personales es condición para el uso del sitio web y sus servicios vinculados. No obstante, si el Usuario decide voluntariamente proporcionar sus datos personales debe brindar datos veraces, exactos y completos. La inexactitud de los mismos puede suponer dificultades para establecer un vínculo directo con el Administrador.

14 Véase en: https://www.argentina.gob.ar/terminos-y-condiciones#2. Última consulta: 10 de agosto de 2021.

Si bien es cierto que en las Bases y Condiciones de la aplicación el tema del consentimiento para el otorgamiento de datos aparecía suficientemente explicado como voluntario, no lo es menos que al reglamentar la obligatoriedad del uso de la aplicación, se pone en duda que el otorgamiento del consentimiento fuera de manera libre, lo cual, como vimos, es una característica fundamental para que se constituya como una base legal legítima para el tratamiento de los datos personales.

El ejemplo más claro surge de la Disposición No. 1771/2020 del 25 de marzo de 2020 de la Dirección Nacional de Migraciones que estableció que:

> Toda persona que ingrese al país a partir del dictado de la presente medida, deberá por el plazo mínimo de CATORCE (14) días contados a partir de su ingreso, adherir y utilizar la aplicación denominada COVID-19-Ministerio de Salud en su versión para dispositivos móviles, que podrá descargarse en forma gratuita de las tiendas de aplicaciones oficiales de Android e iOS, o en su versión web, accesible a través de https://argentina.gob.ar/coronavirus/app.

Nótese que no se da opción: para ingresar a la República Argentina cualquier persona debía utilizar la aplicación. Es decir, a partir de esta norma puede concluirse que el supuesto consentimiento no puede ser considerado libre, salvo que se argumente que la disyuntiva está entre usar la aplicación o ingresar al territorio argentino. Esta disyuntiva cae toda vez que la norma incluye también a ciudadanos y ciudadanas argentinos que tienen un derecho garantizado por la Constitución de ingresar y transitar por el territorio. Por lo tanto, el ejercicio de ese derecho constitucional dudosamente puede ponerse en juego si alguna persona decidiera no utilizar la aplicación. En otras palabras, la obligatoriedad del uso hace que el consentimiento no sea libre porque era necesario para ejercer un derecho constitucional.

Este cuestionamiento puede llevar a la conclusión sobre una posible vulneración al derecho a la protección de los datos personales de acuerdo con los estándares que se han expuesto en esta investigación. Sin embargo, la autoridad de control en Argentina, al analizar la situación, entendió que[15]:

> §18. Resulta indudable que existen poderosas razones de interés público para exigirles a las personas que arriban desde el exterior que se sometan a la evaluación sintomatológica prevista en Cuidar por el plazo de CATORCE (14) DÍAS HÁBILES, cumpliendo así con las exigencias de "ley" e "interés general" contenidas en los Artículos 5, inciso 2.b y 7, inciso 2 de la Ley No. 25.326.
>
> En consecuencia, la cuestión no se centra en si el consentimiento fue libre o no, sino directamente en si se puede exceptuar la solicitud del consentimiento bajo ciertas circunstancias. Por ello se evaluó una excepción que permite la ley para requerir el consentimiento para el tratamiento de los datos personales que establece la ley de Argentina:
>
> ARTICULO 5° - (Consentimiento).
>
> […]
>
> 2. No será necesario el consentimiento cuando:
>
> b) Se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal;
>
> Y,
>
> ARTICULO 7° - (Categoría de datos).

15 Véase en: https://www.argentina.gob.ar/sites/default/files/if-2020-47292017-apn-dnpdpaaip_0.pdf.

> […]
>
> 2. Los datos sensibles sólo pueden ser recolectados y objeto de tratamiento cuando medien razones de interés general autorizadas por ley. También podrán ser tratados con finalidades estadísticas o científicas cuando no puedan ser identificados sus titulares.

Un análisis técnico muy profundo fue realizado por la Asociación por los Derechos Civiles, ADC, en el informe "En caso de emergencia: descargue una app"[16], de donde se pueden inferir algunos problemas que se encontraron en la utilización de la app durante 2020. El informe incluyó recomendaciones que se remitieron a la Secretaría de Innovación, responsable del tratamiento de los datos para mejorar los problemas técnicos encontrados y que se vinculaban fundamentalmente con vulnerabilidades de la aplicación que podían afectar la seguridad de los datos personales que se recolectaban.

En definitiva, aun compartiendo este análisis, la excepción al consentimiento libre e informado para el tratamiento de datos debe ser siempre evaluada bajo un escrutinio muy estricto.

En Chile la aplicación se denominó *CoronApp*[17] y fue formalmente puesta a disposición de las personas el 16 de abril de 2020. Fue el propio presidente Sebastián Piñera quien hizo el anuncio a través de las redes sociales, expresando que:

> La tecnología nos permite, pese a la distancia, estar informados y cerca de nuestros seres queridos. Queremos entregarles más herramientas para informarse del #COVID19. Los invito a descargar la App #CoronApp para más info:

16 Véase en: https://adc.org.ar/2020/05/21/en-caso-de-emergencia-descargue-una-app/. Última consulta: 23 de agosto de 2021.

17 Véase en: https://coronapp.gob.cl/. Última consulta: 23 de agosto de 2021.

- https://t.co/7Oj3Nmlcbe

- https://t.co/gFPovkSeWT pic.twitter.com/Af3KlB6npB

— Sebastián Piñera (@sebastianpinera) April 16, 2020.

Como informaron algunos medios de comunicación, el hashtag #CoronApp fue rápidamente *"trending topic"* en la plataforma Twitter en Chile.

Esta aplicación fue desarrollada por el Ministerio de Salud con apoyo de un equipo de la División de Gobierno Digital, en función de los Decretos que habían declarado la emergencia sanitaria que se han mencionado más arriba. Al ingresar a las "Políticas de Privacidad"[18] de la aplicación se puede leer que:

> El Ministerio de Salud y sus organismos relacionados se encuentran facultados por ley para requerir, recolectar, ceder o procesar información de salud, conforme a las competencias explícitas que les han sido conferidas y que están contenidas en:
>
> - DFL No. 1/2006, Salud que fija texto refundido, coordinado y sistematizado del Decreto Ley No. 2.763, de 1979 y de las leyes No. 18.933 y No. 18.469, que le faculta mantener registros de datos personales en materias de su competencia.
>
> - Ley 19.628 sobre protección a la vida privada y que fija normas sobre tratamiento de datos por parte de organismos públicos.
>
> - Ley 20.584 que establece derechos y deberes de los pacientes.
>
> - Decreto con Fuerza de Ley No. 725, Código Sanitario, la autoridad sanitaria responsable del aislamiento de toda persona que padezca una enfermedad de declaración obligatoria, especialmente en caso de amenaza de epidemia.
>
> - Decreto No. 4/2020 Salud, que decreta alerta sanitaria por el período que se señala y otorga facultades extraordinarias que indica por emergencia de salud pública de importancia internacional (ESPII) por brote del nuevo coronavirus (2019-NCOV).
>
> - Decreto N 9/2020 Salud, establece coordinación por emergencia de salud pública de importancia internacional que indica y designa ministro coordinador.
>
> - Decreto 158/2020 Salud, reglamento sobre notificación de enfermedades transmisibles de declaración obligatoria.
>
> - Decreto 136/2005 Salud, Reglamento Orgánico del Ministerio de Salud.
>
> - Decreto 41/2012 Salud, aprueba reglamento sobre fichas clínica.

Para justificar la finalidad del procesamiento de datos personales, se dice que *CoronApp* es una aplicación gratuita de información y monitoreo de síntomas de COVID-19.

En cuanto a los datos concretos que se accede, la "Política de Privacidad" los detalla de la siguiente manera:

> Para evitar duplicidad de usuarios y hacer un seguimiento óptimo de la información de síntomas solicitada, la aplicación solicita el ingreso con clave única o el registro de los siguientes datos personales:
>
> - Tipo de documento

18 Véase en: https://coronapp.gob.cl/politicas.html. Última consulta: 23 de agosto de 2021.

- RUN o pasaporte del usuario
- Correo electrónico, opcional
- Número telefónico
- Nombre completo
- Edad para verificar que el usuario es mayor de edad y para monitoreo de síntomas
- Comuna donde vive

Para el monitoreo de síntomas la aplicación solicita lo siguiente:

- Fiebre y los grados
- Tos seca
- Dificultad para respirar
- Respiración rápida
- Flema amarilla o verdosa
- Dificultad para tragar
- Cansancio y fatiga
- Dolores musculares
- Dolor de tórax
- Diarrea
- Labios azules
- Pérdida de olfato

- Contacto con contacto confirmado
- Para utilizar la funcionalidad de Ayuda vecina deberá ingresar:
- Una fotografía para identificarlo entre los vecinos cuando solicita y entrega ayuda
- Dirección
- Para ubicar la posición actual en el mapa:
- Ubicación GPS para obtener la posición actual cuando se usan mapas para reportar aglomeraciones, buscar centros de salud o solicitar ayuda. Esto es opcional. *CoronApp* no almacena estos datos.

Como complemento de la "Política de Privacidad", otro documento ("Términos y Condiciones"), describe los términos de uso aplicables al acceso y uso de la aplicación "*CoronApp*"[19].

En relación con el consentimiento brindado por el titular de los datos se aclara en la "Política de Privacidad" que:

> La descarga de la aplicación es voluntaria y para mayores de 18 años. Con su consentimiento informado y específico accederemos a los datos que nos proporciona. De acuerdo a nuestros términos y condiciones el usuario es responsable de garantizar el buen uso de la aplicación, la completitud, veracidad, exactitud y precisión de sus datos y los de los terceros que ingresa. Además, y respecto de la geolocalización, se aclara que "El usuario opcionalmente podrá utilizar la ubicación GPS para obtener su posición actual cuando se usan mapas para reportar aglomeraciones, buscar centros de salud o solicitar ayuda. CoronApp no almacena estos datos.

19 Véase en: https://coronapp.gob.cl/terminos.html. Última consulta el 23 de agosto de 2021.

Por su lado, en los "Términos y Condiciones" se establece que:

> Mediante el uso de la aplicación, el usuario acepta la utilización de la información tratada por aquella, en los términos y condiciones establecidos en éstos. Asimismo, al hacer uso de estos servicios, el usuario accede a vincularse a estos Términos.
>
> El Usuario declara haber leído y aceptado los términos y condiciones. En caso que el usuario no esté de acuerdo con estos términos, deberá abstenerse de utilizar los servicios que proporciona la aplicación, sea que la desinstale o simplemente deje de usarla.

Y sobre la permanencia del consentimiento manifestado se dice que:

> "El usuario entiende y acepta que los términos pueden ser modificados en cualquier momento, sin notificación o autorización previa del usuario y al sólo arbitrio de la Subsecretaría de Redes Asistenciales. Sin perjuicio de lo anterior, cualquier nuevo servicio, modificación, supresión o ampliación de los servicios será informado en la aplicación. La utilización del sistema con posterioridad a la publicación de una modificación, constituye aceptación de la misma".

La descripción de *CoronApp* que hemos visto, permite, en lo que interesa a esta investigación, determinar que se ha implementado una tecnología que, sobre la base legal del consentimiento del usuario, permite el tratamiento de datos personales. El consentimiento aparece como suficientemente informado, y el desacuerdo con el tratamiento de los datos habilita sin más a la no utilización de la aplicación que se declara como de utilización voluntaria.

Sin embargo, una vez otorgado el consentimiento, los términos de uso pueden cambiar sin requerirse un nuevo consentimiento dado que, una vez informado el titular de los datos personales, la utilización de la aplicación opera como una suerte de consentimiento tácito sobre los cambios que pudieran haberse realizados. Ello, por la importancia que reviste el consentimiento, resulta problemático.

Es importante destacar que organizaciones especializadas de la sociedad civil realizaron críticas a la aplicación.

La ONG "Derechos Digitales" la calificó de "sumamente problemática, riesgosa y, en última instancia, muy poco útil"[20].

Entre otras cosas, y en relación con el consentimiento, "Derechos Digitales" entendió que: "La autoridad pretende salvar la cuestión del uso de los datos través de un consentimiento que los titulares de los dispositivos deben otorgar para poder utilizar la app, y que simplemente no existe en el caso de la información referida a terceros, que potencialmente pueden llegar a incluir hasta al vecino".

Se encuentra también una suerte de dislocamiento entre la finalidad por la cual se recogen los datos y los datos efectivamente recogidos. Del análisis de "Derechos Digitales" surge que:

> La información entregada por las usuarias de la aplicación —su condición de salud, patologías preexistentes y condiciones de riesgo específicas (contacto con personas infectadas o viajes a zonas de riesgo)— no necesita ser combinada con datos de identificación individual para hacer una contribución efectiva al diagnóstico. La app podría recoger toda esa información y

20 Véase en: https://www.derechosdigitales.org/14387/coronapp-la-inutilidad-del-atajo-tecnologico-desplegado-por-el-gobierno-y-sus-riesgos/. Última consulta: 23 de agosto de 2021.

> entregar recomendaciones en forma anónima o seudónima (si la persona crea un perfil con un avatar y alias), con exactamente la misma efectividad. La información de identificación individual requerida no cumple función alguna y solo expone a sus titulares a que terceros, dentro o fuera del Estado, accedan a estos datos con fines distintos a los estipulados por la app, y con consecuencias múltiples, que incluyen ser objeto de distintas formas de discriminación, tanto en el presente como en el futuro; algunas manifestaciones de este fenómeno ya se han hecho visibles: vecinos incómodos con la presencia de funcionarios de la salud o contagiados en sus edificios, condominios o barrios, a las que podrían sumarse o acciones de discriminación en oportunidades de empleo basadas en el desarrollo de anticuerpos o la determinación de primas de salud futuras por posibles secuelas, entre muchas otras.

En otro informe, el Centro de Investigación Periodística, CIPER[21], luego de un análisis de la política de privacidad y de los "términos y condiciones" de *CoronApp*, detectó:

> Vacíos y el uso de lenguaje impreciso al momento de fijar las reglas de la app y los derechos de los usuarios. Argumentan que esto puede permitir que los datos sean usados para fines que sus titulares no dimensionan. "Las palabras de los contratos nunca son elegidas al azar por los abogados", explican. En el caso del negocio de los datos esa vaguedad busca "dejar abierta la posibilidad de recolectar más datos de los expresamente señalados y/o poder usarlos con fines distintos a las informados". Eso es inaceptable para una aplicación del estado, argumentan.

21 Véase en: https://www.ciperchile.cl/2020/04/22/problemas-de-proteccion-de-los-datos-personales-de-la-aplicacion-coronapp/. Última consulta: 23 de agosto de 2021.

Asimismo, el Consejo para la Transparencia, CPLT[22], remitió un oficio el 7 de mayo de 202 al ministro Secretario General de la Presidencia y al Ministro de Salud, donde refieren expresamente que:

> La aplicación de *CoronaApp* requiere, para la ejecución de sus funcionalidades, la recopilación, almacenamiento y procesamiento de una gran cantidad de datos personales, en especial, datos de carácter sensible, tanto de sus usuarios enrolados como de terceros. A este respecto, suscita especial preocupación el adecuado tratamiento de los datos suministrados por los usuarios o que sean recabados a partir de su actividad o interacción con esta herramienta digital, el que debe ajustarse en todo momento a los principios, derechos y deberes contemplados en nuestra normativa de protección de datos personales.

Consecuente con esta preocupación manifestada, el CPLT expresó que, dada la cantidad de datos que se recogerían, debía evaluarse si resultaban excesivos o desproporcionados en función de los fines para los cuales se declamaba su tratamiento. Sin decirlo, parecería que, a juicio del CPLT, había una recolección que no cumplía con el principio de proporcionalidad en la recopilación de datos para cumplimiento del fin que se propone.

Además, manifestó una preocupación al advertir que se recopilaban datos de carácter sensible sin que quedara clara la base legal para hacerlo, remarcando que en la normativa chilena existe una prohibición general para su tratamiento.

22 Para esta investigación fue consultado sobre su análisis de la *CoronaApp*, recibiéndose información al respecto. Se tomaron en cuenta solo algunos aspectos de la información recibida que se consideraron útiles para el objeto de esta investigación. Se agradece al CPLT la colaboración con el IIDH.

En el oficio, pidió que se facilitara el ejercicio de los derechos que les caben a los titulares de datos personales que son objeto de tratamiento.

En concordancia con lo expuesto más arriba, el CPLT se pronunció con preocupación ante la falta de una base legal de tratamiento de datos de terceros "dependientes" a los que no se los informa y a quienes no se les requiere consentimiento.

En la República Oriental del Uruguay, la aplicación que se estableció lleva el nombre de *Coronavirus UY*[23].

De acuerdo con la descripción oficial, la aplicación:

> *Coronavirus UY* permite conectar a los ciudadanos con posibles síntomas del coronavirus COVID-19 con los prestadores de salud, a fin de reducir los tiempos de espera de consultas y atención ante la emergencia sanitaria. Toda la información recogida estará amparada según las condiciones previstas por la Ley No. 18.331 y en la política de privacidad de la aplicación. Como parte de su evolución, la aplicación ha incorporado distintas funcionalidades, como la visualización de información sobre el estado de la pandemia en Uruguay, el reporte de síntomas, consulta por telemedicina y la alerta de exposición, entre otras.

Resulta destacable como buena práctica, prevista desde el inicio, la auditabilidad del código fuente, estableciéndose que:

> Con el objetivo de brindar una total transparencia y garantías sobre el manejo de la información recolectada, en esta primera etapa, se pone a disposición de instituciones nacionales (academia, industria, sociedad civil organizada), la posibilidad de auditar la documentación y código fuente de la aplicación *Coronavirus UY*, incluyendo sus funcionalidades de alerta de exposición.
>
> Las instituciones interesadas podrán ponerse en contacto a través del correo electrónico coronavirusuy@agesic.gob.uy, indicando el propósito de las actividades a realizar, así como los responsables a contactar para realizar la coordinación y acceso a la documentación y código fuente.

23 Véase en: https://www.gub.uy/ministerio-salud-publica/politicas-y-gestion/informacion-sobre-aplicacion-coronavirus. Última consulta: 23 de agosto de 2021.

Relacionado con la implementación de esta aplicación, aunque no expresamente sobre ella, la Unidad Reguladora de Control y Protección de Datos Personales de AGESIC, en la Resolución No. 35 del 20 de junio del 2020, se había ocupado del tema vinculado con la utilización de sistemas de rastreo de contacto (*"contact tracing")* mediante aplicaciones móviles.

En la Resolución, la Unidad estableció que:

1. En cuanto a los sistemas de rastreo de contactos, aconsejar los que implican un almacenamiento descentralizado de los datos por resultar menos invasivos para la privacidad de las personas.

2. Señalar la pertinencia de realizar en forma previa una evaluación de impacto en la protección de datos; la inscripción de la base generada en caso de contener datos personales, o en su caso, actualizar la preexistente; y la suscripción de acuerdos que garanticen el cumplimiento de la normativa en caso en que se aplique sistemas provistos por terceros así como analizar y evaluar especialmente los aspectos técnicos vinculados con seguridad, considerando especialmente los lineamientos del Centro Nacional de Respuesta a Incidentes de Seguridad Informática (CertUy) de la Agencia para el

Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento.

3. En caso que el rastreo de contactos se adicione como funcionalidad a aplicaciones preexistentes que recolecten otro tipo de información, deberán extremarse las medidas de seguridad, atendiéndose otras alternativas en el marco de la necesaria evaluación de impacto a la protección de datos.

4. Corresponde asegurarse la obtención del consentimiento previo y expreso de los usuarios mediante la descarga y aceptación de términos de la aplicación, o en caso de que se agregue como funcionalidad a aplicaciones preexistentes, de las nuevas funcionalidades y actualizaciones que se propongan incluir en el sistema.

5. Deberá establecerse una adecuada granularidad del consentimiento ante distintas acciones propuestas a los titulares de los datos, y prever la posibilidad que estos puedan revocar su consentimiento para el uso del rastreo de contacto, aun sin tener que eliminar la aplicación.

6. Procede asegurarse que el sistema sólo pueda ser aplicado por el Ministerio de Salud Pública en el marco de la emergencia sanitaria en su calidad de responsable de tratamiento de datos, y con fines de alertar a potenciales contagiados, del contacto con una persona positiva por COVID-19. Adicionalmente, no debe emplearse para realizar un monitoreo individual de los usuarios.

7. La información debe almacenarse en centros seguros y en territorio nacional. En casos debidamente justificados de transferencia internacional, deberá solicitarse la autorización a esta Unidad, salvo que se transfiera a territorios adecuados. Los respaldos deberán cumplir con las recomendaciones

indicadas en el presente y deberán ser eliminados en las mismas condiciones que las bases originales.

8. En caso de conservarse información en forma centralizada –fuera de los dispositivos de los usuarios– se debe contar con los mecanismos de seguridad pertinentes para evitar incidentes y ser eliminada una vez cumplida la función para la cual fue recolectada.

9. Como corolario de lo anterior, y en caso de que se agregue el rastreo de contacto a una aplicación preexistente, mantenerse independiente la información vinculada a este, de la que resulte de otras funcionalidades de la aplicación.

10. No deberá proporcionarse información personal de casos positivos a potenciales contagiados por la enfermedad; tal información solo puede remitirse al Ministerio de Salud Pública con el consentimiento expreso del titular del dato y a efectos del seguimiento de su situación de salud. Cuando el rastreo de contactos se adicione a una aplicación preexistente, la comunicación de confirmación de un caso positivo debe efectuarse con el consentimiento expreso del titular del dato.

11. Deberá ponerse a disposición de los interesados las especificaciones de la aplicación a efectos de garantizar un tratamiento transparente de los datos y un eventual consentimiento informado. En particular, especificarse la forma de habilitar o deshabilitar el rastreo de contactos y la información sobre el uso de *bluetooth*; si ésta se adiciona a una aplicación preexistente, deberá aclararse expresamente y en forma separada las condiciones de tratamiento de otras funcionalidades de la aplicación.

12. Procede informarse expresamente a los titulares de los datos sobre situaciones de potencial contagio y los parámetros de

tiempo y distancia, así como eventuales modificaciones, en el marco de la necesaria y permanente transparencia.

13. Deberá minimizarse la recolección de información, en especial cuando refiere a informaciones de terceros; en su caso, esta solo podrá remitirse al Ministerio de Salud Pública para su gestión conforme los protocolos que se elaboren al respecto, manteniéndose separadas de la información derivada del rastreo de contactos. También eliminarse toda la información finalizada la emergencia sanitaria, salvo que sea debidamente anonimizada y su conservación autorizada por la Unidad. La información recolectada debe ser periódicamente revisada en función de los objetivos específicos considerando un criterio de minimización de los datos.

Resulta importante destacar que muchas de estas recomendaciones fueron tomadas en cuenta, tal como surge de las políticas de privacidad que se publican, relacionadas con la aplicación uruguaya que se crearon poco tiempo después de las recomendaciones de la Unidad[24].

Ese documento explica, en primer lugar, que el registro en la aplicación es voluntario y se requiere el consentimiento del titular de los datos. Respecto del tratamiento de los datos, una vez otorgado el consentimiento, el documento establece que:

> Los datos personales recabados y accedidos para el registro en la aplicación, incluyendo los declarados por el usuario en la funcionalidad de seguimiento, serán tratados por el Ministerio de Salud Pública con la finalidad de relevamiento y contención relacionada a la pandemia coronavirus (COVID-19) y

24 Véase en: https://www.gub.uy/ministerio-salud-publica/comunicacion/publicaciones/politica-privacidad-app-coronavirusuy. Última consulta: 23 de agosto de 2021.

> comunicados en el marco de lo dispuesto por el Decreto No. 93/020, de 13 de marzo de 2020, relativo a la emergencia sanitaria.
>
> Los datos personales se encuentran en una base de datos inscrita ante la Unidad Reguladora y de Control de Datos Personales, titularidad del Ministerio de Salud Púbica, y cuentan con medidas de seguridad adecuadas que garantizan su integridad, disponibilidad y confidencialidad (Resolución Nuevo Sistema No. 64/020 del Consejo Ejecutivo de la Unidad).
>
> Solo se realizarán comunicaciones de datos autorizadas por la Ley No. 18.331, a Instituciones Públicas o Privadas que ejerzan las mismas competencias asistenciales y resulten necesarias para la efectiva prestación de asistencia del titular de los datos. Para la funcionalidad de tele consulta, se comunicará la información al prestador indicado por el usuario y la información resultante quedará incorporada en su historia clínica.

Finalmente, resulta pertinente agregar que esta aplicación incluyó como herramienta un sistema de "Alertas de exposición"[25] pero el sistema solo funciona si el usuario acepta activarlo, e incluso luego de hacerlo se requerirá su permiso y participación para acciones específicas. Luego de otorgar el permiso inicial para activar el sistema de alertas, podrá desactivarlo en cualquier momento.

25 Véase en: https://www.gub.uy/ministerio-salud-publica/sites/ministerio-salud-publica/files/2020-06/disen%CC%83o%20gacetilla%20coronavirus%202%20copia_0.pdf. Última consulta: 23 de agosto de 2021.

3. Conclusiones y recomendaciones

Las medidas adoptadas en los tres países fueron similares, pero ofrecen diferencias que repercuten de manera distinta en cualquier análisis de la situación, en cada uno de ellos, referida al respeto de derechos fundamentales. El modo, tiempo y extensión de las medidas no fue igual en los tres países.

La utilización de herramientas tecnológicas se aceleró en 2020 y ello fue habilitado por la declaración de emergencia sanitaria en los tres países estudiados.

Sin perjuicio que podrían encontrarse otros campos de impacto, la tecnología fue utilizada para habilitar lo que se denomina "teletrabajo", la "telemedicina" y el desarrollo de aplicaciones de uso en teléfonos móviles que tenían como objeto colaborar con las personas tanto para la detección como la asistencia ante casos de potenciales contagios del virus que provocaba la enfermedad.

Quedó evidenciado que en el campo de las regulaciones que habilitaron el "teletrabajo", en general no se prestó la debida atención a la protección de los datos personales de quienes elegían o se les impuso esa modalidad de trabajo.

Algo similar ocurrió con la "telemedicina" donde pudo advertirse una falta de regulación concreta sobre la tecnología utilizada, sobre todo aquella vinculada con la selección de las plataformas para consulta médica o para el intercambio de datos personales de salud que son considerados, en los tres países, datos de carácter sensible sobre los cuales hay que prestar una atención más profunda cuando de ellos se hace tratamiento.

En consecuencia, debido al aumento de estas prácticas de atención médica, o de modalidades de trabajo fuera de los lugares

habituales, que específicamente se habilitaron por regulaciones que tenían como excusa la emergencia sanitaria, hubiera sido deseable que esas regulaciones tomaran en cuenta no sólo desde una posición declarativa, sino concreta, la necesaria protección de la privacidad de los sujetos involucrados, cuestión que, como se ha visto, no fue abordada debidamente, incluida la seguridad de los datos personales y los temas que se mencionan a continuación.

Es por esta razón que sería recomendable generar regulaciones apropiadas para la protección de derechos fundamentales sin que ello pueda ser entendido como un obstáculo de la utilización de las tecnologías vigentes para el "teletrabajo", la "telemedicina" o incluso para la asistencia de las personas en cuestiones de salud que hacen a la emergencia sanitaria.

Más específicamente, y de acuerdo a lo que surge en esta investigación, dos son los temas que merecieron atención: por un lado, las cuestiones relacionadas con el otorgamiento del consentimiento de los titulares de los datos personales que se trataron; y, por otro lado, la proporcionalidad, en función de la finalidad específica que se declamaba, de la recolección de datos personales.

Ambas cuestiones (consentimiento y proporcionalidad) están íntimamente vinculadas con el desarrollo de las tres aplicaciones que se mencionan en esta investigación –*CuidAR*, de Argentina; *CoronApp* de Chile, y *CoronavirusUy* de Uruguay–.

Dadas las interpretaciones que se aportan más arriba en este estudio, es posible concluir que las aplicaciones diseñadas en los tres países estudiados tuvieron claroscuros, dado que en algunos casos es dudoso que el consentimiento se hubiera otorgado de manera libre e informada, y en otros es cuestionable la cantidad de datos recolectada.

Como ejemplos de lo mencionado se da la obligatoriedad impuesta en Argentina, en algunos casos, de otorgar el consentimiento por la simple aceptación de los términos y condiciones de la aplicación en los tres casos estudiados; y la cantidad de datos que se recolectaban, por ejemplo, en el caso chileno, que fuera explicado más arriba.

Para terminar, sería recomendable que se revise el diseño de estas aplicaciones, se aplique el estándar de "privacidad desde el diseño" y, particularmente, se solicite de una manera más clara e inequívoca el consentimiento del titular para el tratamiento de sus datos personales.