Tipo de documento: Tesina de Grado de Ciencias de la Comunicación

Título del documento: Tensiones en torno a la protección de datos personales durante la pandemia por COVID-19 : un análisis comparado entre las aplicaciones Cuidar (Argentina) y CoronApp (Chile)

Autores (en el caso de tesistas y directores):

María Florencia, Antueno

Bernadette Califano, tutora

Fernando Amdan, co-tutor

Datos de edición (fecha, editorial, lugar,

fecha de defensa para el caso de tesis): 2023

UNIVERSIDAD DE BUENOS AIRES
FACULTAD DE CIENCIAS SOCIALES
CARRERA DE COMUNICACIÓN SOCIAL

Tensiones en torno a la protección de datos personales durante la pandemia por COVID-19

Un análisis comparado entre las aplicaciones
Cuidar (Argentina) y CoronApp (Chile)

TESINA DE GRADO

Alumna: Antueno María Florencia

Tutora: Bernadette Califano

Cotutor: Fernando Amdan

Agradecimientos

A mi mamá y a Orlando por su apoyo incondicional.

A Bernadette y Fernando por su tiempo y dedicación.

Índice

1. Introducción

El desarrollo de las tecnologías de la información y las comunicaciones (TIC) y el rápido avance de la globalización han permitido que el intercambio de información y el tratamiento de datos personales en Internet se vuelvan cotidianos. Estos fenómenos, asociados a las llamadas nuevas tecnologías, han profundizado la transferencia internacional de datos, planteando constantemente nuevos retos para su protección.

La presente tesina tiene por objetivo principal analizar comparativamente si los términos y condiciones de las aplicaciones Cuidar (Argentina) y CoronApp (Chile) respetan los principios de protección de datos personales establecidos en las leyes N° 25.326 (Argentina) y N° 19.628 (Chile). Para ello, se plantean objetivos específicos:

- Examinar comparativamente cómo se incluyen los principios de consentimiento; finalidad, exactitud, minimización, limitación de conservación, transferencia internacional de datos, cesión, responsabilidad y seguridad, en las leyes vigentes de protección de datos personales de cada país;
- Analizar comparativamente en qué medida se incluyen estos principios en los términos y condiciones de cada aplicación;
- Identificar las tensiones emergentes de la comparación de las experiencias argentina y chilena.

En ese sentido, se procurará indagar en qué medida estas iniciativas públicas, pueden llegar a suscitar prácticas de vigilancia que colisionen con las leyes vigentes de protección de datos personales y/o con el marco interamericano de protección de los derechos humanos, en un contexto de pandemia.

Según la Organización Mundial de la Salud (2020) el 31 de diciembre de 2019 fue notificado el primer brote de la enfermedad en la ciudad de Wuhan, China. Tres meses después, la Organización Mundial de la Salud (OMS) declaró el estado de pandemia. Para marzo de 2020 el virus se había expandido rápidamente, con reportes de los primeros casos en los continentes europeo y americano. En ese breve lapso de tiempo se produjeron alrededor de 170 muertes y más de 100 casos en 20 lugares por fuera de China, lo que derivó en la declaración de la emergencia internacional de salud pública por parte de la OMS. Los contagios se propagaron también por América Latina; fue Brasil el primer país en registrar el primer caso positivo, para luego replicarse rápidamente en otros países de la región.

En Chile, el primer caso detectado fue el 3 de marzo de 2020 y la pandemia irrumpe en el marco de un fuerte estallido social, caracterizado por una ola de protestas donde la consigna máxima era la necesidad de la reforma de la Constitución diseñada durante la dictadura de Augusto Pinochet (Heiss, 2020). Sin embargo, las protestas también nucleaban reclamos de carácter heterogéneo como el acceso a la salud, la precarización laboral, el fin del sistema privado de pensiones, entre otros. Como consecuencia del estallido, la administración del ex Presidente Sebastián Piñera (2018-2022) tuvo que enfrentar el desafío de la pandemia con un 6% de imagen positiva (Heiss, 2020).

En Argentina, luego de cuatro años de gobierno de Mauricio Macri (2015-2019), el 27 de octubre de 2019 se desarrollaron las elecciones generales con seis candidatos a la Presidencia en donde la fórmula Alberto Fernandéz - Cristina Fernandéz de Kirchner por el Frente de Todos se impuso, en primera vuelta, con el 48,10% (12.473.709 votos), logrando el triunfo en 18 de los 24 distritos electorales del país, por sobre Mauricio Macri y Miguel Ángel Pichetto

(Juntos por el Cambio) quienes obtuvieron un 40,37% (10.470.607 votos) (“Elecciones 2019…”, 2019).

Volviendo a Chile, la pandemia irrumpió en el segundo año del segundo mandato de la Presidencia de Sebastián Piñera, quien asumió el 11 de marzo de 2018. Se consagró electo en primer lugar en las elecciones primarias desarrolladas el 2 de julio de 2017 en donde se presentaron 8 candidatos a presidentes. Allí se impusieron con la mayor cantidad de votos Sebastián Piñera con un 36,6% (2.418.540 votos) y Alejandro Guillier con un 22,7% (1.496.540 votos), según Diario Emol (“Resultados elecciones”, 2017). La segunda vuelta se desarrolló el 17 de diciembre 2017 en donde de un total de 43.048 de mesas escrutadas, correspondientes al 100% dio como resultado el triunfo de Piñera con el 54,7 por ciento (3.795.896 votos) por sobre Guillier con un 45,43 por ciento –(3.160.225 votos), (Resultados definitivos, 2017).

En esos escenarios, la pandemia originada por el virus SARS-CoV-2 trajo consigo una serie de desafíos de políticas públicas para ambos gobiernos. Ambos países se encontraron ante la necesidad de contener la rápida expansión del COVID-19 con medidas asociadas a los objetivos de lograr el aislamiento y el distanciamiento físico de sus poblaciones. A nivel mundial, China, Corea del Sur y Singapur fueron los primeros países en utilizar sistemas de vigilancia para garantizar la eficacia de las medidas y frenar la propagación del virus. El gobierno singapurense fue el pionero en desarrollar, bajo iniciativa gubernamental, una aplicación denominada TraceTogether, la cual fue de código abierto (open source) para que los desarrolladores de todo el mundo pudieran utilizarla de forma gratuita, modificarla y redistribuirla (“Singapur lanzará una nueva aplicación…”, 2020). La misma utilizaba un

sistema de rastreo de contactos por tecnología Bluetooth y fue retomada por Asia, Europa y América Latina, mediante modificaciones y adecuaciones a cada contexto.

Dado el rápido avance y desarrollo de estas aplicaciones móviles por parte de gobiernos de todo el mundo, diversas organizaciones civiles manifestaron públicamente sus preocupaciones. Amnistía Internacional, Human Rights Watch, Access Now, Center for Digital Democracy y Privacy International, entre otras, difundieron una Declaración conjunta de la sociedad civil (2020) en la que alertaron sobre la posible vulneración de derechos humanos relativos a la privacidad y a la protección de datos personales. En este documento señalaron sobre los riesgos de estos sistemas de vigilancia masiva, y establecieron una serie de recomendaciones basadas en los principios de protección de datos personales para desarrollar tecnologías digitales que respeten plenamente los derechos humanos. Estos postulados hacen hincapié en el requerimiento de que toda medida de vigilancia sea necesaria, desarrollada de forma proporcionada, legítima, con un límite preciso en el tiempo de su aplicación y garantizando la protección necesaria para la información sensible otorgada por los ciudadanos, a fin de evitar abusos y discriminaciones. También han resaltado la necesidad de que los usuarios cuenten con información clara y precisa acerca del tratamiento que fueran a recibir dichos datos.

1.2 Las aplicaciones COVID-19 en Argentina y Chile

En Argentina, el 23 de marzo de 2020 la Secretaría de Innovación Pública, órgano que depende de la Jefatura de Gabinete de la Nación, lanzó una aplicación denominada “Autoevaluación de síntomas de Coronavirus COVID-19”. La aplicación fue relanzada junto con la comunidad científica, el sector público y empresas del sector privado (Fundación

Sadosky, el CONICET, Hexacta, Globant, G&L Group, C&S, QServices, GestiónIT, Intive, Finnegans y Faraday (nucleadas en la Cámara de la Industria Argentina del Software -CESSI-); ARSAT; Amazon Web Services), el lunes 27 de abril bajo el nombre Cuidar (El Gobierno relanza CUIDAR, 2020). Desde sus inicios fue presentada como una aplicación de autoevaluación de síntomas para el público en general, facilitando un diagnóstico rápido y una alerta temprana a las autoridades sanitarias ("Sistema y aplicación Cuidar", 2020).

Por su parte, Chile lanzó el 16 de abril de 2020 la CoronApp la cual fue desarrollada por la división Gobierno Digital[1]. La misma también fue promocionada como una herramienta para poder realizar autoevaluación de síntomas, alertar a las autoridades y se suman algunas funciones más como informar y/o denunciar conductas de alto riesgo y brindar o solicitar ayuda a los vecinos.

Si bien se avanzará con una descripción y análisis detallados más adelante, cabe anticipar algunos aspectos claves sobre Cuidar y CoronApp. Las dos plataformas solicitan que el usuario suministre para el registro datos, tales como tipo y número de documento, número de teléfono, dirección y fecha de nacimiento, entre otros. Al mismo tiempo, las aplicaciones requieren de la aceptación de permisos para acceder a otros datos personales previamente registrados y almacenados en el dispositivo móvil, como la ubicación vía GPS (en los dos casos es opcional pero con la advertencia de que si no se habilita algunos servicios que se ofrecen pueden no estar disponibles), el acceso a la cámara de fotos para escaneo del documento y foto de perfil.

[1] Gobierno Digital es la División encargada de la Transformación Digital del Estado, tiene como objetivo coordinar y asesorar a los órganos de la Administración del Estado en el uso estratégico de las tecnologías digitales.

Frente al almacenamiento y tratamiento de datos personales y sensibles y la habilitación de acciones, como en el caso de CoronApp, de denuncia por aglomeraciones e incumplimiento de cuarentena, nos preguntamos si las tecnologías han sido desarrolladas siguiendo un correcto lineamiento con los principios de protección de datos personales, de manera tal que promuevan el cuidado de la salud y la protección de la privacidad. A este respecto, la jurisprudencia interamericana ha desarrollado el test tripartito a fin de entender si las restricciones a la libertad de expresión y acceso a la información son legítimas o no (Chocarro, 2017). A tal fin, se han establecido tres puntos necesarios para considerar tales restricciones, la primera es que deben estar previstas por ley; segundo, deben perseguir objetivos imperiosos de la Convención (la protección de los derechos de los demás, la protección de la seguridad nacional, del orden público o de la salud o moral públicas); y tercero, ser necesarias en una sociedad democrática y proporcionales al fin perseguido.

Teniendo en cuenta la emergencia ocasionada por la pandemia en donde los Estados deben priorizar la salud pública pero así también lograr un equilibrio en las limitaciones de otros derechos, surgen algunas tensiones y preguntas que se indagarán en esta tesina: ¿Los términos y condiciones de las aplicaciones se ajustan a las legislaciones vigentes, en un marco de excepcionalidad por la pandemia? ¿Los datos recolectados y almacenados son adecuados, relevantes y limitados a las finalidades declaradas? ¿Cumplen los Términos y Condiciones con los principios de protección de datos personales? ¿Qué contrastes y similitudes pueden apreciarse entre los casos de Cuidar y CoronApp?

1.3 Metodología y estructura

En esta investigación se recurre a una metodología cualitativa, con el estudio de casos comparados. Entendiendo con Sautu (2003) que el estudio de casos se caracteriza por tres rasgos, siendo el primero el ser particularístico, "es decir está focalizado sobre una situación, hecho, programa, fenómeno en particular, aún cuando en su elección se tenga en cuenta que es un caso entre otros con los que comparte ciertos rasgos" (p.42), característica que nos permitirá centrar el análisis en la comparación de dos aplicaciones móviles desarrolladas para el control y contención de la pandemia. El segundo rasgo es su alto contenido descriptivo, el cual permite mostrar las complejidades de los casos elegidos y que permitirá identificar cómo se incorporan los principios de protección de datos personales seleccionados en los términos y condiciones de cada aplicación. En tanto, su tercera característica, la cualidad heurística, posibilitará relevar las tensiones surgidas en la comparación de ambas experiencias..

Se utilizaron fuentes normativas de distinta jerarquía, tales como leyes, decretos y resoluciones, y se recurrió a fuentes secundarias entre las que se hallan informes, bibliografía, información institucional e información periodística; también se realizaron dos entrevistas en profundidad a especialistas en la materia. Las dos entrevistas se realizaron, dado el contexto de pandemia, vía videollamada con la intención de conocer la opinión de especialistas en materia de tecnologías de la información y comunicación (TIC), y protección de datos personales de ambos países. A fin de entender la particularidad del desarrollo de cada caso e indagar en qué medida incorporan los términos y condiciones los principios de protección de datos personales seleccionados.

El presente trabajo está estructurado en seis capítulos. El primer capítulo es la presente introducción. El segundo se desarrolla el marco conceptual desde el cual se aborda el objeto

de estudio, con hincapié en las nociones de políticas estatales (Oszlak y O'Donnell, 1984), capitalismo informacional (Castells, 1995), capitalismo de plataformas (Srnicek, 2018), capitalismo de vigilancia (Zuboff, 2020) y sociedad de control (Deleuze, 1995). Todo esto con el fin de observar críticamente la respuesta a la crisis mediante el despliegue de estas tecnologías digitales, y su inserción, diálogo y conflicto con los marcos institucionales y normativos vigentes, buscando dar cuenta de los riesgos inherentes al despliegue de las tecnologías de la información y la comunicación (TIC) sin un lineamiento claro con los derechos humanos.

En el capítulo 3 se detallan los contextos regulatorios, donde se exponen los acuerdos internacionales vigentes en materia de protección de datos personales en Argentina y Chile, dentro de los que se encuentra la Guía Legislativa sobre la Privacidad y la Protección de Datos personales en las Américas desarrollado por la OEA, donde se actualizan los principios de protección de datos personales y, por último, al finalizar el capítulo se retoma la declaración llevada a cabo durante el 2020 por organizaciones de la sociedad civil a los Estados para el respeto de los derechos humanos en el despliegue de tecnologías digitales para el combate de la pandemia.

Luego se avanza hacia el capítulo 4 donde se realiza un análisis comparado de las leyes N°19.628 sobre Protección de la Vida Privada de Chile y N° 25.326 sobre Protección de los Datos Personales de Argentina, desde los siguientes principios: consentimiento; finalidad, exactitud y minimización; limitación de conservación, transferencia internacional de datos y cesión; seguridad y responsabilidad.

Con este recorrido avanzamos hacia el quinto capítulo donde se realizó una descripción de las aplicaciones Cuidar y CoronApp, y un análisis comparado de sus términos y condiciones

desde los principios de protección seleccionados; y se detallan las tensiones surgidas en la comparación entre las experiencias de Argentina y Chile. Finalmente se plantean una serie de conclusiones.

Capítulo 2: Marco conceptual

El marco conceptual de la presente tesina está estructurado en tres subtemas. En un primer momento se retoma la noción de Estado de O'Donnell (1977) para poder comprender las políticas públicas partiendo de la noción de políticas estatales de Oszlak y O'Donnell (1984). Luego se avanza en distintas conceptualizaciones del capitalismo, empezando por el concepto de capitalismo informacional donde se da cuenta del surgimiento y funcionamiento del modo de desarrollo informacional, según Castells (1995). Luego se retoman los conceptos de capitalismo de plataformas de Srnicek (2018) y capitalismo de la vigilancia de Zuboff (2020) a fin de comprender la importancia de los datos y su mercantilización en la etapa superior del capitalismo. Finalmente se analizan los derechos que se ponen en tensión con la temática abordada, como el derecho a la privacidad y a la protección de datos personales.

2.1 Introducción al concepto de Estado

Para analizar los casos Cuidar y CoronApp se retoman los conceptos de Estado y políticas públicas porque se entienden ambos casos como instrumentos de una política pública más amplia en materia de salud pública, impulsada por el Estado argentino y el Estado chileno.

Para poder entender las políticas públicas se elige partir de la noción de Estado planteada por O'Donnell (1977) para luego avanzar con el concepto de políticas estatales trabajado por Oszlak y O'Donnell (1984) a fin de analizar qué acciones fueron necesarias para poner en funcionamiento estos sistemas.

Partimos de la noción de Estado propuesta por O'Donnell (1977), quien reflexiona particularmente sobre el Estado capitalista. El autor entiende por Estado al "componente

específicamente político de la dominación en una sociedad territorialmente delimitada" (p.2), de ahí comienza a desarmar esa definición y explica que entiende "lo político (...) como una parte analítica del fenómeno más general de la dominación: aquella que se halla respaldada por la marcada supremacía en el control de los medios de coerción física en un territorio excluyentemente delimitado" (p.2-3). Va a decir que el Estado es una forma de vinculación entre sujetos sociales. Esta relación entre sujetos es desigual a causa del control diferencial de ciertos recursos, entre los cuales nombra: los medios de coerción física, los recursos económicos, el control de la información y el control ideológico. En la sociedad capitalista, el entramado fundamental, aunque no el único, son las relaciones de producción. La relación que se establece entre capitalistas y trabajadores asalariados, al ser un acto de explotación, es conflictiva y contradictoria, y el Estado es una parte, o aspecto, de dicha relación social. Es decir, el Estado es el organizador de las relaciones capitalistas, en el sentido de que tiende a ser mediador en dichas relaciones y a aportar elementos para su reproducción. O'Donnell (1977) explica que:

> La garantía que presta el Estado a ciertas relaciones sociales, incluso las relaciones de producción (...) no es una garantía externa ni a posteriori de dicha relación. Es parte intrínseca y constitutiva de la misma, tanto como otros elementos- económicos, de información, de control ideológico- que son aspectos que sólo podemos distinguir analíticamente en dicha relación (p.7).

Es así que se elige retomar el concepto desarrollado por el autor particularmente porque entiende al Estado como una relación social, es decir, como un producto histórico delimitado territorialmente que se objetiva en el derecho y las instituciones públicas. Es así que el Estado aparece como el lugar donde se elaboran las políticas estatales, las cuales tienen como

característica ser el resultado de las interacciones de diferentes actores, con variados intereses y distintas posiciones en el campo más amplio de la dominación.

2.1.1 El Estado y las políticas públicas

Al definir al Estado como un aspecto de las relaciones de producción, las cuales son conflictivas y contradictorias, este no queda exento de estar atravesado por contradicciones sociales. En distintos momentos diferentes sectores de la sociedad se movilizan y expresan en torno a distintas problemáticas sociales; algunas de ellas logran captar la atención y movilización de más de una clase y actores de la sociedad civil que exigen alguna decisión al respecto, y se convierten en lo que lo que Oszlak y O'Donnell (1984) van a denominar como la cuestión. El Estado responde a estas exigencias mediante políticas estatales, las cuales son definidas como "un conjunto de acciones y omisiones que manifiestan una determinada modalidad de intervención del Estado en relación con una cuestión que concita la atención, interés o movilización de otros actores de la sociedad civil" (p.10). Son una toma de posición por parte del Estado con respecto a una cuestión y cuál es la forma más adecuada de resolverla.

En la búsqueda de resolución de estas cuestiones, el Estado suele aparecer como un actor más y se observa que los otros que deciden involucrarse pueden no estar directamente afectados por la cuestión pero entienden que su propuesta de resolución puede servir a sus intereses, mejorar su apoyo político o bien les ayuda a disolver tensiones que resultan amenazantes a su poder. La toma de posición del Estado en algún momento del curso de desarrollo de una cuestión inevitablemente influye en las relaciones de fuerzas de los demás actores involucrados, es por esto que nos interesa centrarnos en ella ya que

> (...) a) cuentan con el respaldo de normas de cumplimiento supuestamente obligatorias y de una última ratio fundada en el control de superiores medios de coacción física, y b) porque en general repercuten sobre la sociedad más extensamente que las políticas privadas (Oszlak y O'Donnell, 1984, p.16).

Es así que se retoma la noción de Estado, primero, y la de políticas estatales, después, porque para entender estas últimas resulta necesario partir de una noción de Estado. Se decide partir del concepto desarrollado por O'Donnell (1977) porque permite comprender su aspecto relacional en donde participan diferentes actores y, por lo tanto, a las políticas públicas como la toma de posición del Estado frente a una cuestión, resultado de sus interacciones con los diferentes sectores involucrados. Así se observa que las políticas públicas llevadas a cabo durante la pandemia por la COVID-19 no fueron iniciativas aisladas sino más bien un conjunto de respuestas que manifiestan la postura de los Estados que las han llevado a cabo frente a la cuestión de contener los sistemas de salud a través de garantizar el cumplimiento de las medidas de aislamiento y prevención para mitigar la propagación del virus. Al mismo tiempo, se advierten las interacciones que han surgido con el resto de los actores involucrados, entendiendo que las decisiones de los Estados están influidas por las posiciones e intereses de estos actores. En los casos de estudio seleccionados retomar estos dos conceptos permite comprender que en el desarrollo de las aplicaciones Cuidar y CoronApp estuvieron presentes varios actores e intereses y dar cuenta de qué "toma de partido" reflejan las decisiones que se tomaron en la elaboración de sus términos y condiciones.

2.2 Capitalismo informacional, de plataformas o de vigilancia

Anteriormente se observó con O'Donnell (1977) que en la sociedad capitalista el entramado fundamental son las relaciones de producción y que el Estado es un actor clave que contribuye a la reproducción de las mismas. A partir de ahí, de ahora en adelante se desarrollará una breve historización de los conceptos de capitalismo para entender algunas particularidades del sistema capitalista en el cual tiene lugar la pandemia y se lanzan las *coronapps*. Se inicia retomando el concepto de capitalismo informacional de Castells (1995) donde nos enfocaremos en el surgimiento del modo de desarrollo informacional, luego se avanza al capitalismo de plataformas definido por Srnicek (2018), para entender el rol de los datos como materia prima principal en el proceso productivo actual, y por último se retoma el concepto de capitalismo de vigilancia de Zuboff (2020) a fin de comprender la extracción sistemática de los "datos conductuales" a escalas cada vez más crecientes orientados ya no solo a predecir de la conducta, si no a moldearla e intervenir en ella.

Para comenzar a entender en qué etapa del capitalismo nos encontramos se parte por comprender con Manuel Castells (1995) que nos encontramos en lo que él denominó como capitalismo informacional. La forma en la que se organiza la actividad económica de una sociedad está definida por su modo de producción, según Castells (1995) en el modo de producción capitalista el objetivo está orientado hacia la maximización del beneficio. El autor explica que hacia finales del siglo XX el capitalismo ha sufrido un proceso de reestructuración profunda, se ha dado paso de una economía de escala a una economía global. La misma se caracteriza por una descentralización y flexibilización de la gestión de las empresas, una integración e interconexión global de los mercados financieros, donde los actores económicos se mueven por una red global que elimina las fronteras nacionales, lo que

da paso a una economía informacional global y como resultado una nueva relación entre economía, Estado y sociedad. Para el autor, la economía a escala mundial que se desarrolló en las últimas décadas es una economía "informacional y global". Es informacional porque "la fuente de la productividad estriba en la tecnología de la generación del conocimiento, el procesamiento de la información y la comunicación de símbolos" (p. 17). Es global porque tanto la producción, el consumo, la circulación y sus componentes (capital, trabajo, materias primas y mercados) están organizados a esa escala.

Esto se da producto de que en 1970 el modelo keynesiano llegó a su límite expresado con una alta inflación, lo cual hizo que se empiecen a suceder una serie de reformas en donde la innovación tecnológica y el cambio organizativo pasaron a tener un rol principal para asegurar la reestructuración. En el prólogo de su libro *La era de la información: economía sociedad y cultura*, explica:

> Así, la nueva sociedad que surge de ese proceso de cambio es tanto capitalista como informacional, aunque presenta una variación considerable en diferentes países, según su historia, cultura, instituciones y su relación específica con el capitalismo y la tecnología de la información (Castells, 2006, p. 13).

Esta reestructuración implicó que el modo de desarrollo, esto es las fórmulas tecnológicas que caracterizan la productividad en el proceso de producción, cambie. Cada modo de desarrollo se define por el elemento técnico principal que determina el trabajo en ese proceso productivo. En particular, en el modo de desarrollo informacional, la información pasa a ser este elemento y el factor principal de maximización del excedente en donde se constituye tanto en la materia como en el producto. Lo específico de este modo de desarrollo, según Castells (1995), es que "el conocimiento actúa sobre el conocimiento en sí mismo con el fin

de generar una mayor productividad" (p. 7). Toda esta reestructuración económica y técnica ha tenido su correlato en el ámbito político y social, ya que los procesos tienen la característica de incorporarse a todas las actividades, determinando en última instancia el comportamiento humano y la organización social. El académico lo explica como el hecho de que "por primera vez en la historia, la mente humana es una fuerza productiva directa, no solo un elemento decisivo del sistema de producción" (p. 3).

Es así que la noción de capitalismo informacional y con ella la de modo de desarrollo informacional permiten comprender el surgimiento de un modo de producción capitalista que basa su productividad en la incorporación de tecnologías de la información, en donde los datos pasan a ser la materia prima por excelencia de maximización del beneficio y, por lo tanto, de poder.

Dos décadas después, el economista Nick Srnicek (2018) coincide con Castells en la importancia de los datos en lo que él llama el "capitalismo de plataformas", entendido como un emergente de esta etapa del sistema capitalista, que tiene como característica principal la creación de ecosistemas basados en la información y el procesamiento de datos. El autor va a definir a las plataformas como "infraestructuras digitales que permiten que dos o más grupos interactúen" (p.45). Este modelo de negocio ha sido consecuencia de tendencias económicas profundas que son caracterizadas en tres momentos históricos: la respuesta a la recesión de los años 1970; la caída de las punto-com durante la década de 1990; y la respuesta global a la crisis mundial del 2008. Cada uno de estos momentos fue sentando las bases para el surgimiento y consolidación de una economía digital, que tiene como actores principales a las plataformas las cuales se enfocan en la extracción y explotación de un tipo particular de materia prima: los datos.

Si Castells (1995) decía que lo particular de este modo de desarrollo informacional es que el conocimiento actúa sobre sí mismo a fin de generar mayor productividad, Srnicek (2018) lo va reformular diciendo que en el capitalismo de plataformas el propio análisis de datos produce nuevos datos, en un proceso que se retroalimenta continuamente. Es importante al análisis la distinción que hace el autor con respecto a los datos y el conocimiento:

> En primer lugar distinguiremos datos (información de algo que sucedió) de conocimiento (información acerca de por qué algo sucedió). Los datos pueden implicar conocimiento, pero no es una condición necesaria. (...) Como entidad grabada, cada dato requiere sensores para ser capturado y enormes sistemas de almacenamiento para su mantenimiento (...) También deberíamos ser cautelosos con pensar que la recopilación y el análisis de datos no tienen complicaciones o son procesos automatizados. La mayor parte de los datos precisa limpieza y se la debe organizar en formatos estandarizados para que sean utilizables (Srnicek, 2018, p.41).

En este sentido, el autor va a decir que esto ha derivado en una nueva forma de competencia capitalista donde entran en juego la cantidad de datos que capturan las empresas y el análisis que hacen de ellos; en donde la clave no está tanto en cómo se generan esos datos sino en quien tiene la capacidad para procesarlos. Esto resulta relevante al análisis en el sentido de que las aplicaciones seleccionadas recopilan una enorme cantidad de datos que suponen de infraestructura y grandes sistemas de organización para su uso.

Por otro lado, para entender cómo opera el control en nuestras sociedades, se retoma a Gilles Deleuze (1995) en su texto *Post-scriptum sobre las sociedades de control* donde explicó el pasaje de las sociedades disciplinarias a las de control. Las sociedades disciplinarias fueron descritas por Michel Foucault (1975), las cuales se caracterizaban por operar mediante

grandes centros de encierro, en donde el individuo pasa de uno a otro a lo largo de toda su vida: la familia, la escuela, la fábrica, el hospital y la cárcel. En estas sociedades disciplinarias descritas por Foucault el objetivo eran los individuos. En su libro *Vigilar y Castigar* (1975), el filósofo va a explicar dos imágenes de las disciplinas en estas sociedades; por un lado, la disciplina-bloqueo "la institución cerrada, establecida en los márgenes, y vuelta toda ella hacia funciones negativas: detener el mal, romper las comunicaciones y suspender el tiempo" (p. 193); y por el otro lado, la disciplina-mecanismo "un dispositivo funcional que debe mejorar el ejercicio del poder volviéndolo más rápido, más eficaz, más ligero, un diseño de las coerciones sutiles para una sociedad futura" (p.193). En estas sociedades el disciplinamiento se ejerce al trazar el límite del exterior anormal, a través de la norma. Partiendo de estas investigaciones, Guilles Deleuze (1995) va a explicar el pasaje de la sociedad disciplinaria a la de control, afirmando que si en las sociedades disciplinarias siempre se estaba empezando de nuevo al pasar de una institución a otra, "en las sociedades de control nunca se termina nada: la empresa, la formación, el servicio son los estados metaestables y coexistentes de una misma modulación, como un deformador universal" (p. 2). El individuo está inmerso en sociedades que adoptan el control "al aire libre", en donde la organización ya no se ejerce en sistemas cerrados, sino que los mismos constituyen una modulación, "(...) una suerte de molde auto deformante que cambia constantemente y a cada instante, como un tamiz cuya malla varía en cada punto" (p.2). Esto es la consecuencia de una profunda mutación del capitalismo, en donde la vigilancia y el control social han pasado a ejercerse mediante las tecnologías, las que marcan o prohíben el acceso a la información. Uno de los aspectos más importantes de las sociedades de control, vistas con relativa independencia de las disciplinares, es el incremento y la colonización de la tecnología en los

espacios más recónditos de la cotidianeidad. Desde esta perspectiva, la vigilancia continuaría ahora, ya adentrados en el siglo XXI, vinculada a las tecnologías y no a los centros de encierro y las instituciones.

Esto permite introducir el concepto de capitalismo de vigilancia desarrollado por la académica Shoshana Zuboff (2020), a través del cual ha explicado que hoy nos adentramos en una nueva era de la economía política la cual "reclama unilateralmente para sí la experiencia humana, entendiéndola como una materia prima gratuita que puede traducir en datos de comportamiento" (p. 21). Esto es definido como una mutación del capitalismo, el cual fue y es propiciado por la ideología y las políticas neoliberales e impensable por fuera del "medio ambiente digital" (p. 23). Lo particular de este capitalismo de la vigilancia, como una variante del capitalismo informacional, es que aspira a predecir y modificar la conducta humana para producir mayores ganancias y el control de los mercados.

A partir del desarrollo del capitalismo de vigilancia, dado por una cantidad cada vez más abundante de datos e información a procesar, se ha descubierto que los datos más predictivos son aquellos que provienen de la intervención en la acción humana; es decir, aquellos que mediante su manipulación pueden modificar nuestros comportamientos. En tanto el objetivo no se basa en imponer nuevas formas de comportamiento sino más bien en producir una conducta que dé por resultado los fines comerciales buscados.

La autora explica que a diferencia del capitalismo industrial donde se requería de economías escala en la producción para así poder reducir los costes en los productos ofrecidos; en el capitalismo de la vigilancia las economías de escalas son requeridas para la extracción del excedente conductual (Zuboff, 2020). El objetivo aquí es obtener la mayor cantidad de datos ya no sólo para predecir la conducta sino para modificarla en base a los imperativos del

mercado. A su vez, para producir el excedente económico, estos datos necesitan ser analizados mediante un análisis predictivo que permita revelar movimientos e intenciones a gran escala con el fin de asegurar ganancias y predicciones cada vez más acertadas. Es la convergencia que nombra Srnicek (2018) entre vigilancia y actividad lucrativa.

La presente tesina se propone indagar sobre la protección de los datos personales, en un contexto en donde las tecnologías de la información han pasado a ser el elemento principal del nuevo capitalismo informacional, haciendo que la generación, procesamiento y transmisión de información sean, no sólo los elementos claves para garantizar la productividad, sino también elementos de vigilancia y control social. En un escenario atípico como la pandemia por COVID-19, en donde la vigilancia y el rastreo a través del desarrollo de aplicaciones se convirtió en una de las herramientas para afrontar la propagación de la enfermedad, encontramos pertinente problematizar la protección de los datos personales de los individuos y revisar las pautas de seguridad, términos y condiciones de privacidad de estas dos aplicaciones móviles. El acceso a ciertos datos como los de geolocalización, su recolección y tratamiento pueden resultar efectivos y necesarios en el combate de la pandemia, pero también corren el riesgo de constituirse, sin un correcto alineamiento con los derechos humanos, en nuevas fuentes de control social y amenazas contra la privacidad y otros derechos por parte de los ciudadanos.

2.3 Derecho a la privacidad y a la protección de los datos personales

El derecho a la privacidad y a la protección de los datos personales son otros de los aspectos claves para analizar las aplicaciones Cuidar y CoronApp. El análisis comparativo de los términos y condiciones de ambas aplicaciones, a la luz de los marcos normativos vigentes en

Argentina y Chile, permitirá indagar sobre las tensiones suscitadas a partir del desarrollo de estas herramientas tecnológicas. Como se vio anteriormente con Oszlak y O'Donnell (1984) las políticas estatales son producto de un proceso social en torno a un tema socialmente problematizado, en esta caso la cuestión era contener el sistema de salud a partir de que la población cumpliera con el aislamiento social, preventivo y obligatorio. Siguiendo a los autores, el estudio de las mismas implica tener en cuenta la temporalidad en la que se inscriben, el ámbito de acción social y los actores que participan. Es así que para entender el contexto en el que se insertan las aplicaciones Cuidar y CoronApp, se empieza por abordar cómo han evolucionado y se encuentran legislados los derechos a la privacidad y protección de datos personales en Argentina y Chile.

Los derechos a la intimidad y a la privacidad son considerados derechos universales. Así lo establecen el artículo 12 de la Declaración Universal de Derechos Humanos y el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos, adoptados por la Asamblea General de las Naciones Unidas[2]:

> Nadie será objeto de injerencias arbitrarias en su vida privada, ni su familia, ni cualquier entidad, ni de ataques a su honra o su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques.

Así también, en el ámbito regional, el artículo 11 de la Convención Americana sobre Derechos Humanos del año 1969, refiere a que toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad y que por tanto nadie deberá ser objeto de

[2] La Asamblea General, establecida en 1945, es el principal órgano deliberativo, de formulación de políticas y representativo de la Organización de las Naciones Unidas.

intromisiones arbitrarias o abusivas en su vida privada, familia, domicilio, ni deberá sufrir ataques ilegales a su honra o reputación.

Cerda Silva (2012) explica que el derecho a la protección de datos personales surge en la década de los setenta del siglo XX, cuando el desarrollo de las tecnologías de la información y su creciente uso por parte de organismos públicos y privados suscitó la necesidad de establecer un límite a la creciente transmisión y procesamiento de la información. En un primer momento, la legislación fue formulada en torno al derecho a la vida privada, ya que el interés primero era resguardar la información personal, hasta cobrar plena autonomía en la década de los ochenta cuando surge la doctrina de la "autodeterminación informativa". Esta se refiere a un derecho que "faculta a las personas para controlar la información que les concierne, siendo irrelevante a efectos de su protección si dicha información es privada o pública" (p.168). De tal forma, esto otorga al titular de los datos una serie de facultades para el control de los mismos frente a su almacenamiento, tratamiento y procesamiento.

De este modo, el derecho a la protección de datos personales ha logrado una entidad autónoma, como también lo explica Molina Quiroga (2003):

> La fundamentación jurídica del derecho a la protección de datos personales, sin duda puede y debe relacionarse con el tradicional derecho a la intimidad, pero lo excede ya que también alcanza a datos públicos, incide en otros derechos personalísimos como el honor, la imagen o la identidad, y lo que es más decisivo para nuestra hipótesis, es que no solo se vincula con personas físicas, sino también con personas jurídicas (p.5).

Para el desarrollo de esta investigación es necesario comprender que el derecho a la protección de los datos personales tiene una entidad autónoma, esto permite que se

adjudiquen normas constitucionales y procedimientos judiciales específicos (acciones de amparo o hábeas data) para su protección a fin de garantizar a las personas el control sobre sus datos, más allá de su eventual conexión con la vida privada. Al mismo tiempo, también es importante comprender que al igual que sucede con el derecho a la libertad de expresión, los derechos a la privacidad y a la protección de datos personales no son absolutos y pueden existir ocasiones en las que sea necesario establecer limitaciones. El Pacto Internacional de Deberes Civiles y Políticos (1966) por la Asamblea General de las Naciones Unidas establece en su art. 19.3 que el derecho a la libertad de expresión conlleva deberes y responsabilidades, dejando expreso:

> Puede estar sujeto a ciertas restricciones, que deberán, sin embargo, estar expresamente fijadas por la ley y ser necesarias para:
>
> a) Asegurar el respeto a los derechos o a la reputación de los demás;
>
> b) La protección de la seguridad nacional, el orden público o la salud o la moral públicas (p.21).

Al respecto, la Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos (CIDH) desarrolló un test tripartito para evaluar que las limitaciones sean legítimas. En primer lugar, deben cumplir con el principio de legalidad, "la ley que establezca una limitación a la libertad de expresión sólo puede referirse a la exigencia de responsabilidades ulteriores" (Chocarro, 2017, p.18). Segundo, deben ser legítimas, es decir, estar orientadas a la protección de derechos de los demás, de la seguridad nacional, o de la salud o moral públicas. Tercero, deben ser necesarias y proporcionales, "la limitación debe ser necesaria en una sociedad democrática para el logro de los fines imperiosos que se buscan; estrictamente proporcionada a la finalidad perseguida; e idónea

para lograr el objetivo imperioso que pretende lograr" (Chocarro, 2017, p.18). Es decir, para los casos aquí estudiados es relevante considerar que la emergencia en salud pública supuso que se establezcan limitaciones a otros derechos, como el de privacidad, pero que también resulta importante tener en cuenta que dichas limitaciones no sean excesivas.

Retomando el análisis sobre el modelo de protección de datos personales que predomina en América Latina, el mismo se ha caracterizado por tener como base principal el derecho fundamental del habeas data, que:

> Además de ser un derecho fundamental, es una herramienta de protección jurídica de los titulares de los datos creada con el fin de conseguir la protección frente al tratamiento indebido o ilegal de sus datos de carácter personal por parte de bases de datos o archivos públicos o privados (Villegas Carrasquilla, 2012, p.130).

Frente al gran incremento de los datos gestionados tanto por entidades públicas como privadas, resultado de una nueva reestructuración del capitalismo que vira hacia la extracción y uso de los datos como materia prima para la generación de excedente (Srnicek, 2018), es pertinente a los fines de la investigación comprender que en la región el derecho a la privacidad y a la protección de datos personales funcionan como categorías jurídicas diferentes en donde ambos son reconocidos, por separado, como derechos fundamentales bajo garantía constitucional. Por un lado, el derecho a la privacidad será entendido como la potestad que tiene toda persona de decidir qué aspectos de su vida privada quiere compartir con otros y el reconocimiento de las garantías de protección frente a ataques o injerencias que pudieran afectar su honra y reputación. Por el otro, el derecho a la protección de datos personales se comprende como diferenciado al derecho a la privacidad pero relacionado, en el sentido de que el mismo prevé una serie de condiciones en el tratamiento de datos personales

que tiene como fin proteger otros derechos y libertades fundamentales. Este "garantiza a las personas el control sobre la información que les concierne, independientemente de su conexión con la vida privada, aspecto que, de hecho, se soslaya" (Cerda Silva, 2012, p.171).

Si bien ambos derechos están íntimamente relacionados, el que sean entendidos como derechos fundamentales bajo categorías jurídicas diferentes permite que puedan ser desarrollados en toda sus especificidades y que los individuos no queden desamparados de la ley frente a los progresos técnicos que permiten asociarlos con determinados datos. Asimismo, se entiende que tanto el derecho a la privacidad como el de la protección de los datos personales contienen sus limitaciones, considerando que la Comisión Interamericana de Derechos Humanos ha establecido que siempre que se produzcan injerencias a la vida privada de las personas, las mismas deben: estar previstas por ley; perseguir un fin legítimo; y ser idóneas, necesarias y proporcionales.

Es así que se nos hace presente indagar los términos y condiciones de las aplicaciones, lanzadas por los gobiernos de Argentina y Chile, como herramientas de salud pública, con el objetivo de analizar comparativamente cómo incorporan los principios de protección de datos personales seleccionados y las tensiones que emergen de la comparación, considerando el contexto de emergencia mundial.

Capítulo 3: Contextos regulatorios

A fin de conocer el recorrido histórico en materia de regulación de datos personales en Argentina y Chile, se hará una revisión a la adhesión a diversos tratados internacionales para luego observar las legislaciones vigentes y poder realizar el análisis comparativo de los términos y condiciones de las aplicaciones con el objetivo de observar si se protegen los datos personales de los usuarios, cómo se incluyen los principios de protección de datos seleccionados y qué tensiones se observan a partir de la comparación.

3.1 Acuerdos internacionales

En 1980 el Consejo de Europa sancionó una guía para la protección de la privacidad y el flujo transfronterizo de datos que completó las bases para que el año siguiente se sancionará en la ciudad de Estrasburgo el Convenio 108 (1981), para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, estableciendo:

> El fin del presente Convenio es garantizar, en el territorio de cada Parte, a cualquier persona física sean cuales fueren su nacionalidad o su residencia, el respeto de sus derechos y libertades fundamentales, concretamente su derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona (p.2).

Sin embargo, como explica Cerda Silva (2012), al no lograr gran cantidad de países signatarios a ese Convenio y por no poder resolver el problema del flujo transfronterizo de datos, el 24 de octubre de 1995 se aprueba la Directiva 95 N° 95/46/CE del Parlamento Europeo y del Consejo, logrando una regulación comunitaria vinculante para los países

miembros. La Directiva establecía la protección de datos personales de las personas físicas, la libre circulación de los mismos y que los Estados miembros sólo permitían la transferencia de datos personales a un país tercero siempre y cuando proporcionara un nivel de protección adecuado.

Es así que los países latinoamericanos, siguiendo la Directiva Europea y bajo este nuevo requisito de la necesidad de una adecuada protección, formularon legislaciones específicas para la protección de datos personales, motivo que lleva, en el año 2001, a Argentina y a Uruguay a ser declarados como "países adecuados" por la Comisión Europea, dando cuenta de que sus sistemas de protección de datos se encontraban alineados con los estándares previstos por la directiva 95/46/CE.

En el año 2018, con motivos de reforzar la protección de datos personales debido a los nuevos desafíos a la privacidad provenientes del desarrollo de las TIC, al gran aumento en la circulación de la información y la globalización del procesamiento de la misma, el Consejo Europeo adoptó un protocolo adicional denominado Reglamento General de Protección de Datos. Este documento establece que el tratamiento de los datos personales tiene que realizarse conforme a unos criterios o principios que lo legitimen y que deberá existir una autoridad de control independiente que se encargue de supervisar el respeto de las normas acerca de la materia.

En el año 2018 se aprobó la adhesión de la República Argentina al Convenio 108 (1981) relativo a la Protección de Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal, y así se convirtió en el tercer país de la región en formar parte del mismo junto a México y Uruguay. Argentina suscribió al último Protocolo Actualizado del Convenio, conocido como Convenio 108+ y se adentró en un proceso de reforma para

reemplazar la ley N° 25.326 de Protección de Datos Personales a través de un proyecto presentado por el Poder Ejecutivo (Argentina se suma al Convenio 108+, 2019). Según el informe desarrollado por la Agencia de Acceso a la Información Pública el proyecto de ley presentado durante el 2018 incorporaba los estándares y recomendaciones establecidos en el Reglamento General de Protección de Datos Personales de la Unión Europea. Sin embargo, debido a que no fue tratado perdió estado parlamentario, por lo que se ha abierto una instancia de consultas públicas para la presentación de un nuevo proyecto de ley ("Hacia una nueva protección…", 2022).

Por su parte, el 11 de enero de 2010, Chile firmó el Convenio de Adhesión de la Organización para la Cooperación y el Desarrollo Económico (OCDE). La misma supone la adopción constante de medidas que son consideradas claves para el desarrollo social y económico. Desde ese momento, diversas han sido las recomendaciones del organismo en materia de protección de datos personales y numerosos han sido los proyectos presentados para la modificación de la ley sobre Protección de la Vida Privada N° 19.628. En sus rasgos generales los proyectos presentados buscaban atender al equilibrio entre la protección de la privacidad y la transferencia de los datos. Dado el acelerado intercambio de información, se buscaba lograr el equilibrio balanceando miradas económicas, jurídicas y políticas, a fin de establecer un marco regulatorio que permita resguardar el derecho de las personas en el tratamiento de los datos personales sin entorpecer la libre circulación de la información.

En el 2018, se sancionó la ley que consagra el Derecho a la Protección de Datos Personales N° 21.096 la cual modifica el artículo 19 N° 4 de su Constitución y otorga carácter constitucional al derecho a la protección de datos personales, reconociéndolo como un derecho fundamental que tienen todos sus ciudadanos por el simple hecho de ser personas.

Otra normativa relevante al análisis es la adhesión por parte de Chile y Argentina junto a otros cinco países al documento titulado Recomendación del Consejo de la OCDE sobre Inteligencia Artificial. El documento "proporciona un conjunto de principios y recomendaciones acordados internacionalmente que pueden promover una respuesta a las crisis impulsada por la IA que sea confiable y respete los valores democráticos y centrados en el ser humano" ("Cuarenta y dos países…", 2019). Asimismo, se recomienda a los gobiernos invertir en investigación en Inteligencia Artificial, a crear políticas que faciliten la implementación de sistemas confiables y a adaptar los marcos normativos para promover la innovación y competencia.

Además, en junio de 2020, Chile firmó junto a Nueva Zelanda y Singapur el primer Acuerdo de Asociación de Economía Digital (DEPA, por sus siglas en inglés). El mismo tiene el objetivo de potenciar el flujo de exportaciones de productos y servicios en la economía digital, mediante el libre flujo de datos y la no discriminación a productos digitales, la inteligencia artificial y la interoperabilidad entre los sistemas de los países firmantes. El acuerdo está fuertemente centrado en los beneficios económicos y sociales del desarrollo de la economía digital y el comercio de datos entre los países mediante un marco amigable para las empresas donde puedan exportar sus productos y servicios.

Se observa que en Chile en particular, se están generando una variedad de iniciativas y adhesión a acuerdos internacionales que se desarrollan en paralelo a la actualización de la legislación sobre protección de datos personales.

3.1.2 Principios de protección de datos personales

Como dijimos anteriormente muchas de las legislaciones específicas sobre protección de datos personales en la región, y en particular las de Argentina y Chile, estuvieron inspiradas en la Directiva 95 N° 95/46/CE del Parlamento y del Consejo Europeo, debido a que la misma establecía que sólo se permitía la transferencia internacional de datos con aquellos países que garantizarán un adecuado nivel de protección en sus normativas. Eso hizo que ambas legislaciones incorporen los principios de protección establecidos en la mencionada Directiva: consentimiento, lealtad, legalidad, transparencia, exactitud, seguridad y responsabilidad. La Directiva europea fue derogada en 2018 por el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de Europa, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a su libre circulación, en donde recupera, amplía y actualiza los principios contenidos.

A su vez, la Organización de los Estados Americanos (OEA)[3] ha trabajado desde el año 1996 en diferentes resoluciones relativas a la protección de datos personales, instando a los Estados miembros a tomar determinadas acciones en la materia. En particular, en 2012 el Comité Jurídico Interamericano[4] aprobó una "Propuesta de Declaración de Principios de Privacidad y Protección de Datos Personales en las Américas", luego en 2015 emitió una Guía Legislativa sobre Privacidad y Protección de Datos Personales en donde se disponen doce principios[5] que

[3] La OEA es un organismo regional creado en 1948 con el objetivo de lograr en sus Estados Miembros "un orden de paz y de justicia, fomentar su solidaridad, robustecer su colaboración y defender su soberanía, su integridad territorial y su independencia". En el Artículo 1 de la Carta de la OEA. Argentina y Chile son parte de los miembros originales.

[4] El Comité Jurídico Interamericano es el cuerpo consultivo de la Organización en asuntos jurídicos, tiene como finalidad promover el desarrollo progresivo y la codificación del derecho internacional, estudiar los problemas jurídicos de los países en desarrollo del continente y la posibilidad de uniformar sus legislaciones en cuanto parezca conveniente.

[5] Estos principios son: Propósitos legítimos y justos, Claridad y Consentimiento, Pertinencia y Necesidad, Uso limitado y retención, Confidencialidad, Protección y Seguridad, Fidelidad de los datos, Acceso y Corrección, Responsabilidad, Flujo transfronterizo de datos, Publicidad de las excepciones, Condiciones para el procesamiento de datos.

deben regir en el ámbito público y privado para una adecuada protección de los datos personales.

Según los principios desarrollados en esta Guía Legislativa (2015), las leyes de los Estados Miembros deben contemplar que los titulares de los datos expresen su consentimiento para el tratamiento de los mismos. El **consentimiento** debe ser: libre, informado y no debe dar lugar a dudas o ambigüedades. Para eso, los titulares deben contar con la información sobre las personas o entidades que recopilan los datos, los fines para los cuales se recaban, los mecanismos de protección y cómo pueden ejercer esos derechos. A su vez, deben garantizar que los datos sean recogidos con propósitos legítimos y por medios legales. Se debe garantizar la **exactitud, la pertinencia y la necesidad**. Esto es que los datos personales recogidos sean, por una lado correctos, exactos y completos; por otro, guarden relación con los fines para los cuales son recolectados; y que sean necesarios para brindar el producto o servicio a la persona que los brinda. Asimismo, en el documento se garantizan dos principios fundamentales más con respecto a la retención de datos personales:

> 1) deben mantenerse y utilizarse de manera legítima y que no sea incompatible con el fin para el cual se hayan recopilado (lo cual se denomina a veces el "principio de finalidad" o "limitación del propósito"); y 2) no deben mantenerse por un periodo de tiempo mayor al necesario para su propósito y de conformidad con la legislación nacional correspondiente (p. 21).

En cuanto al principio de **finalidad**, mencionado en el punto 1 de la cita, se establece que se pueden considerar excepciones siempre que los titulares de los datos otorguen su consentimiento o una ley lo disponga. En relación con la **responsabilidad y seguridad** de los

datos, el informe plantea que las leyes deben incorporar medidas de seguridad que garanticen la integridad, confidencialidad y disponibilidad de los datos. Así, se explica que:

> Los datos personales deben protegerse, independientemente de la forma en que se mantengan, por medio de salvaguardias razonablemente concebidas para prevenir que las personas sufran daños considerables como consecuencia del acceso no autorizado a los datos o de su pérdida o destrucción (p. 25).

Además, se establece que las medidas de seguridad adoptadas deben estar basadas en los métodos técnicos vigentes más avanzados y se debe tener en consideración que los datos sensibles requieren un mayor nivel de protección. Los **datos sensibles** son considerados como todos aquellos que de divulgarse o manejarse de forma indebida pueden vulnerar otros derechos fundamentales como el honor y la intimidad, o producir discriminaciones ilícitas y arbitrarias causando graves perjuicios para la persona.

En lo referente a los derechos de los individuos, la Guía menciona que el titular de los datos debe contar con los derechos conocidos como derechos ARCO: de **acceso**, **rectificación, corrección y omisión**. "Las personas (...) deben tener acceso a esos datos a fin de que puedan impugnar su exactitud y pedir al controlador de datos que modifique, revise, corrija o elimine los datos en cuestión" (p.29). Asimismo, se establece que estos derechos no son absolutos y pueden existir excepciones al acceso a los mismos, las cuales deben estar especificadas por ley y disponibles al público.

En cuanto a la **transferencia internacional de datos y cesión**, expresa que si bien la reglamentación cambia de acuerdo a la jurisdicción nacional, se deben buscar medidas que protejan los datos sin obstaculizar el libre flujo de información, de manera tal que no se conviertan en restricciones. En particular, con respecto a los controladores de datos se hace

hincapié en que los mismos deben garantizar un grado continuo de protección a través de las fronteras. La Guía Legislativa (2015) en este punto rescata que previo a que se realice una transferencia de datos a terceros, los titulares deben estar informados al respecto, así como de los medios que disponen para ejercer sus derechos con respecto a la protección de sus datos personales.

Por último, se retoman los principios de uso limitado y retención, también conocidos como **minimización de uso** y **limitación a la conservación**, los cuales en el documento son definidos como aquellos que exigen que los datos personales sean mantenidos y tratados solamente bajo el fin o fines para los cuales se recopilaron y que no se conserven por más tiempo del necesario para el propósito que motivó que su recolección (Guía Legislativa, 2015). Estos principios garantizan que los datos no sean objeto de tratamiento indebido y que no se conserven de manera ilimitada, ni más tiempo del necesario para cumplir con el objetivo buscado.

Con esta declaración de principios, se busca que los Estados adopten leyes nacionales que contengan todos los aspectos de la protección de los datos personales, tanto para el sector público como para el privado. Su intención es proteger a las personas de la recopilación, el uso, la retención y la divulgación ilícita o innecesaria de datos personales. Los Estados Miembros deberían buscar la forma de reglamentar la autorización para interceptar, recabar, analizar y conservar los datos; fijar límites claros y precisos sobre la utilización de los datos recabados; fijar medidas de seguridad que garanticen la conservación de los mismos en las mejores condiciones de seguridad posibles, el anonimato y la destrucción apropiada y permanente. Al mismo tiempo que garantizan que las personas puedan beneficiarse del libro flujo de la información y del acceso a la economía digital.

3.2 Declaración conjunta para la protección de datos personales en el empleo de tecnología digital para combatir la pandemia

Como se observó, desde el inicio de la pandemia diferentes países del mundo desarrollaron y lanzaron aplicaciones móviles para frenar la propagación del virus y ayudar a contener los sistemas de salud. Todas estas tecnologías se han basado en diferentes objetivos entre los que predominaron: rastrear las zonas de contagio, brindar sistemas de autodiagnóstico, asistencia, información y recomendaciones, monitoreo de casos positivos y de registro de contactos estrechos, así como también dar aviso o realizar denuncias por incumplimiento de cuarentena.

Frente al despliegue masivo de las mismas, en consonancia con los principios de protección de datos personales y con el objetivo de recordar que en momentos de crisis los derechos humanos siguen siendo aplicables, más de cien organizaciones de la sociedad civil de todo el mundo, entre las que se encuentran Privacy International, Fundación Vía Libre, Human Rights Watch, Derechos Digitales, Amnistía Internacional, Center for Digital Democracy, etc., realizaron una declaración conjunta, titulada "Los Estados deben respetar los derechos humanos al emplear tecnologías de vigilancia digital para combatir la pandemia". El objetivo era instar a los gobiernos para que dichas tecnologías de rastreo y monitoreo de la población se implementen respetando los derechos humanos evocando que:

> El marco de derechos humanos tiene por objeto garantizar un cuidadoso equilibrio de los distintos derechos para proteger a las personas y a las sociedades en general. Los Estados no pueden desatender sin más derechos como la privacidad y la libertad de expresión con el pretexto de gestionar una crisis de salud pública. Al contrario, la protección de los derechos humanos también promueve la salud pública (Declaración conjunta de la sociedad civil, 2020, p.1).

A tal fin redactaron siete puntos que deben funcionar como condiciones que las tecnologías que se desarrollen deberían respetar: (i) las medidas adoptadas deben cumplir con los principios de legalidad, exactitud, transparencia, lealtad y licitud; (ii) las mismas deben tener una duración en el tiempo limitada y precisa; (iii) los datos recolectados deben ser exactos, proporcionales y relevantes al fin de responder a la pandemia y almacenados solamente el tiempo que dure la emergencia sanitaria; (iv) los gobiernos deben garantizar la seguridad y confidencialidad de los datos adoptando medidas de seguridad con información clara y transparente; (v) todas las medidas que se tomen deben tener en cuenta los riesgos y evitar la profundización en la desigualdad, la discriminación y los abusos de derechos contra las minorías y poblaciones marginadas; (vi) la cesión de datos personales con otras entidades públicas o privadas debe hacerse basándose en la ley, con información clara al usuario y garantizando toda medida de protección necesaria para garantizar el respeto a la privacidad y a los derechos humanos. En particular las empresas del sector privado deben ser capaces de garantizar que dichos datos no serán utilizados para fines comerciales o empresariales; (vii) toda medida debe incorporar mecanismos de rendición de cuentas adecuados y estar sujetos a la supervisión de los órganos adecuados para ofrecer y garantizar a la población la posibilidad de impugnar, acceder, corregir y/o eliminar los datos que se hayan recabado; (viii) toda medida que se tome y recopile datos deben contar con la participación libre y activa de profesionales de la salud, minorías y poblaciones marginadas (“Declaración conjunta de la sociedad civil”, 2020).

Como se observa, el documento parte de recuperar los principios de protección de datos personales al fin de recordar a los Estados que las tecnologías de rastreo y monitoreo deben cumplir con el objetivo de ser herramientas que ayuden a controlar la propagación del virus y

contener los sistemas de salud, y estar desarrolladas bajo la garantía de protección de la privacidad, los datos personales y la libertad de expresión para no funcionar como instrumentos de control que terminen profundizando o causando más daños en las personas. En el siguiente capítulo se retoman algunos de los principios de protección de datos personales mencionados en esta Declaración con el fin de analizar comparativamente si se encuentran y cómo en las legislaciones vigentes de cada país.

Capítulo 4: Leyes vigentes sobre protección de datos personales en Argentina y Chile

Para empezar se ha indicado anteriormente que ambos países tomados en análisis consagran en sus Constituciones el reconocimiento a la protección de datos personales quedando amparado por el recurso de *habeas data.*

Particularmente Argentina en el año 1994, con la reforma de la Constitución, introdujo el artículo N° 43 con el cual fijó la acción de *habeas data* la cual establece que "toda persona podrá interponer acción para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos o privados destinados a proveer informes." Este artículo ha sido luego desarrollado en sus alcances por la ley N° 25.326 de Protección de Datos Personales, que tiene por objeto "la protección integral de los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean éstos públicos, o privados destinados a dar informes." La ley fue reglamentada un año después mediante el Decreto N°1.558/01, el cual estableció las normas de aplicación y clarificó algunos aspectos que permitían diferentes interpretaciones.

Por su parte, Chile consagró el 16 de junio de 2018 mediante la ley N° 21.096 el derecho a la protección de datos personales modificando el artículo 19 N° 4 de su Constitución Política estableciendo:

> El respeto y protección a la vida privada y a la honra de la persona y su familia, y asimismo, la protección de sus datos personales. El tratamiento y protección de estos datos se efectuará en la forma y condiciones que determine la ley (Ley N° 21.096).

El país trasandino cuenta, a su vez, con la ley N° 19.628 sobre Protección de la Vida Privada sancionada en agosto de 1999, donde se establece que las personas afectadas pueden acudir a tribunales a fin de resguardar sus derechos en lo relativo al tratamiento de sus datos personales siguiendo la acción denominada *habeas data*.

4.1 Ley N° 25.326 de Protección de Datos Personales y ley N° 19.628 sobre Protección de la Vida Privada: Principios de las normativas

En este apartado se observarán las similitudes y diferencias presentes en las legislaciones de Argentina y Chile respecto si incluyen y cómo, los principios de protección de datos personales de consentimiento, finalidad, exactitud, minimización, limitación de conservación, cesión, transferencia internacional, seguridad y responsabilidad, a fin de poder analizar luego, en qué medida se encuentran en los términos y condiciones de las aplicaciones Cuidar y CoronApp.

Las leyes vigentes en ambos países incorporaron al momento de su elaboración algunos de los principios esbozados en la Directiva 95 N° 95/46/CE, basándose principalmente en que la licitud del almacenamiento y tratamiento de los datos personales está dada por el consentimiento del titular. A su vez, la Directiva establecía definiciones de datos personales y distinguía, en particular, los datos personales sensibles. Ambas categorías fueron recogidas en las leyes argentina y chilena, desde una perspectiva amplia, que incluye la protección de cualquier dato propio de personas físicas o de existencia ideal, identificadas o identificables, que se encuentren en registros o bancos de datos públicos o privados; y la categoría de datos sensibles para todos aquellos datos que refieren al origen racial y étnico, opiniones políticas, convicciones y creencias religiosas, filosóficas o morales, afiliación sindical e información

referente a la salud física, psíquica y a la vida sexual. En este punto y relativo a los objetivos de estudio de esta tesina, la ley argentina N° 25.326 establece en su artículo 8° que los datos relativos a la salud podrán ser tratados por instituciones sanitarias y profesionales de la salud siempre que se mantenga el secreto profesional. En cuanto a la ley chilena N° 19.628, su artículo 10° refiere a que los datos sensibles no podrán ser objeto de tratamiento a no ser que medie una disposición legal, exista consentimiento del titular o sean necesarios para otorgar beneficios de salud a los titulares.

Ambas legislaciones consideran una definición amplia de datos personales, al considerarlos como aquellos que refieren a personas identificadas o identificables; lo mismo sucede con la definición que otorgan de tratamiento de datos, el cual consideran como cualquier operación que utilice procedimientos electrónicos y/o automatizados que permitan grabar, almacenar, recolectar, transferir, etc. No obstante, la normativa chilena hace referencia tan sólo a datos personales de personas naturales, dejando de lado la categoría de personas jurídicas, en cambio, la normativa argentina va un poco más allá al considerar en el artículo 2° a las personas de existencia ideal[6]. Es decir, refieren a todo tipo de elemento que permita identificar a una persona: nombre, apellido, DNI, profesión, número de celular, correo electrónico, dirección, fotos, videos, geolocalización, entre otros.

Partimos desde estas definiciones de datos personales que otorgan las legislaciones para avanzar hacia la comparación de los principios que integran y cómo lo hacen. La elección de los principios se refiere a aquellos que fueron retomados por las organizaciones de la sociedad civil en su Declaración conjunta de la sociedad civil (2020) titulada “Los Estados deben

[6] Las personas de existencia ideal son personas que no pueden ser denominadas “personas jurídicas” pero que poseen personalidad jurídica. Por otro lado, la persona jurídica o sujeto de derecho, es titular de derechos y obligaciones. Todos los seres humanos son personas jurídicas.

respetar los derechos humanos al emplear tecnologías de vigilancia estatal para combatir la pandemia"; estos son: principio de consentimiento, finalidad, exactitud, minimización, transferencia internacional de datos, limitación de conservación, cesión, responsabilidad y seguridad.

Empezaremos por el **consentimiento**, puesto que éste es el principio más importante del que parten ambas leyes para garantizar la licitud del tratamiento, estableciendo la necesidad de que el titular de los datos personales consienta expresamente en ello. Dicho consentimiento debe ser en todos los casos libre, expreso, informado y por escrito, dejando de lado la validez referida a consentimientos tácitos o no informados. Ambas leyes disponen que no será necesario el consentimiento cuando los datos se obtengan de fuentes accesibles al público, e incorporan una distinción particular para el tratamiento de los datos personales sensibles. Por un lado, la ley N° 25.326 de Protección de Datos Personales establece, en primer término, que nadie podrá ser obligado a proporcionar datos sensibles. Luego en su art. 7° inciso 2, agrega: "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". En cuanto a los datos relativos a la salud de los pacientes, garantiza que pueden ser tratados por entidades públicas o privadas, respetando el secreto profesional.

Por otro lado, la ley chilena N° 19.628 en su art. 10° declara: "No pueden ser objeto de tratamiento los datos sensibles, salvo cuando la ley lo autorice, exista consentimiento del titular o sean datos necesarios para la determinación u otorgamiento de beneficios de salud que correspondan a sus titulares". Es decir, en el caso chileno el tratamiento de datos sensibles, al igual que con los datos personales, es lícito cuando medie una ley y la

autorización del titular. En ambas leyes se establece una salvedad importante para el análisis, la cual refiere a que los organismos públicos podrán recolectar y tratar datos personales sin necesidad de consentimiento, siempre que sean relativos a la materia de su competencia, con sujeción a las reglas precedentes, medie una autorización legal y se recaben para el ejercicio de funciones propias de los poderes del Estado.

Siguiendo con el **principio de finalidad**, el primero refiere a que los objetivos y fines para los cuales se recolectan y tratan los datos deben estar especificados de forma clara, transparente y precisa. La ley N° 25.326 incluye este principio en su art. 4° inciso 3 donde afirma que los datos no pueden ser utilizados para fines distintos de los establecidos, y en el art. 6° explica que cuando se recaben los datos, el titular debe contar con información precisa acerca de: la finalidad para la que serán tratados, el responsable de dichos datos, donde se van a alojar (archivos, registros), las consecuencias de proporcionar los datos, las de no hacerlo y de la inexactitud de los mismos, así como también de las opciones disponibles con la que cuentan los titulares para acceder a los derechos de acceso, rectificación y supresión.

En cuanto a la ley chilena, en su art. 4° establece "La persona que autoriza debe ser debidamente informada respecto del propósito del almacenamiento de sus datos personales y su posible comunicación al público" y luego en el artículo 9° agrega que los datos recolectados podrán utilizarse sólo para los objetivos propuestos y declarados.

En cuanto al **principio de minimización** que indica que el tratamiento de los datos personales debe ser adecuado, pertinente y limitado al fin para el que fueron recolectados; sólo la ley argentina N° 25.326 lo incorpora en su artículo 4° inciso 1 que expresa que los datos personales que se recolecten "deben ser ciertos, adecuados, pertinentes y no excesivos en relación al ámbito y finalidad para los que se hubieren obtenido".

El cuarto principio que aquí nos interesa retomar es el de **exactitud**, el cual establece que los datos personales que se recolectan deben ser exactos, proporcionales y relevantes a los fines que motivaron su recolección. En la ley chilena, el artículo 9°, el mismo que indica que los datos no pueden utilizarse para otros fines que no sean aquellos para los que fueron recolectados, también refiere a que en todos los casos "la información debe ser exacta, actualizada y responder con veracidad a la situación real del titular de los datos". Mientras que en el artículo 6° añade que los datos erróneos, inexactos, incompletos o desactualizados deberán ser modificados por los responsables del archivo o banco de datos.

Por su parte, la ley argentina N° 25.326 incluye un artículo específico donde desarrolla este principio, es en su art. 4° inciso 4 donde indica: "Los datos deben ser exactos y actualizarse en el caso de que ello fuere necesario". A su vez se debe garantizar que los titulares de los datos puedan acceder a ellos para modificarlos y/o actualizarlos en caso de ser necesario.

En cuanto a los principios relativos a **la limitación de conservación y transferencia internacional de datos** se refleja una diferencia notable entre las normativa argentina y la chilena, ya que esta última no incluye ninguno de estos principios, por lo que el responsable de los datos no tiene obligación legal de establecer tiempos específicos para la conservación, ni enfrenta límites en lo que respecta a la transferencia internacional de datos.

Con respecto al **principio de limitación de conservación**, la ley argentina N° 25.326 establece en su art. 21° que todo archivo, registro, base de datos debe inscribirse en el Registro que habilite el organismo de control y cumplir, entre otros requisitos, con brindar la información del tiempo de conservación durante el cual serán almacenados los datos personales recolectados. En cuanto a la **transferencia internacional,** el artículo 12° de la ley establece que queda prohibida con todos aquellos países u organismos que no cuenten con un

nivel de protección adecuado pero la prohibición no rige cuando sean realizadas por motivo de cooperación judicial internacional, en casos de transferencia bancarias o acuerdo internacionales, y en los caso de intercambios de carácter médico "cuando así lo exija el tratamiento del afectado, o una investigación epidemiológica". Es decir, que para el caso argentino aquí estudiado esta última excepción habilitaría la transferencia internacional de los datos médicos almacenados en la aplicación.

Por último, en cuanto a los principios de **seguridad, responsabilidad y cesión** las leyes de protección de datos personales que rigen actualmente en Chile y Argentina incorporan en muy diferentes grados estos principios.

Se empezará con el principio de **cesión de datos**, el cual se incorpora en la N° 25.326 desde el artículo 11° que expresa:

> Los datos personales objeto de tratamiento sólo pueden ser cedidos para el cumplimiento de los fines directamente relacionados con el interés legítimo del cedente y del cesionario y con el previo consentimiento del titular de los datos, al que se le debe informar sobre la finalidad de la cesión e identificar al cesionario o los elementos que permitan hacerlo (p.4).

En tanto que en la ley N°19.628 desde su art. 5° admite la transmisión automatizada de datos siempre que se resguarden los derechos de los titulares y "la transmisión guarde relación con las tareas y finalidades de los organismos participantes". Al mismo tiempo, el responsable del archivo debe dejar constancia de los datos de quien requiere la transmisión, el motivo y fin de la petición, y el tipo de datos que se transmiten. Se observa así que ambas leyes incluyen este principio.

En lo relativo a los principios de **responsabilidad y seguridad**, la Guía Legislativa (2015) define que los controladores de datos deberán adoptar las medidas necesarias para garantizar el cumplimiento de estos principios. Las leyes nacionales deberían ser claras al expresar las medidas de protección necesarias que deben tomar los responsables de la recopilación, procesamiento y almacenamiento de datos personales y brindar algún mecanismo frente al cual los controladores de datos deban rendir cuentas y demostrar el cumplimiento de los principios de protección de datos personales (Guía Legislativa, 2015). Ambas legislaciones definen como *responsable* a la persona física, jurídico privada o pública titular de algún archivo o base de datos. En particular, en la ley chilena N° 19.628 queda establecido que quienes realicen el tratamiento de los datos personales son legalmente responsables del cumplimiento de los principios, obligaciones y deberes en conformidad con la ley, pero no establece el deber de adoptar medidas técnicas, administrativas, físicas y/o legales que resguarden los datos frente a posibles daños, pérdidas, alteración, destrucción y acceso no autorizado. Esta ley únicamente establece el deber de responder indemnizando el daño patrimonial y moral causado por el tratamiento indebido de los datos, "sin perjuicio de proceder a eliminar, modificar o bloquear los datos de acuerdo con lo requerido por el titular o lo ordenado por el tribunal". En resumen, la ley chilena incorpora el principio de responsabilidad pero no así el de seguridad; mientras que la ley argentina incorpora ambos.

Uno de los puntos más importantes de la ley argentina en lo relativo a estos principios, es que con su sanción estableció la creación de la Dirección Nacional de Protección de Datos Personales (DNPDP) como órgano de aplicación y fiscalizador, dependiente de la Subsecretaría de Asuntos Registrales del Ministerio de Justicia. Funcionó como tal desde el año 2001 hasta el 2017, año en que se sancionó la Ley de Acceso a la Información Pública N°

27.275 en donde se estableció la creación de la Agencia de Acceso a la Información Pública. La misma es un ente autárquico, opera con autonomía funcional en el ámbito de la Jefatura de Ministros y actualmente es la autoridad encargada de velar por el cumplimiento de la ley, según se informa en su portal web.

Por su parte, la legislación chilena no hace referencia a la creación de una autoridad que controle y fiscalice el cumplimiento de la misma. Sin embargo, tal como indica Pablo Viollier (2017) en el artículo titulado "El estado de la Protección de Datos Personales en Chile", en el año 2008 se promulgó la ley N° 20.285 sobre Acceso a la Información Pública con la cual se creó el Consejo para la Transparencia el cual tiene entre sus funciones y atribuciones "velar por el adecuado cumplimiento de la ley N° 19.628, de protección de datos de carácter personal, por parte de los órganos de la Administración del Estado" (p. 27). La ley otorga atribuciones muy poco específicas de parte de este organismo para poder garantizar un efectivo cumplimiento, sumando a que no hace referencia a los organismos privados. A este respecto, hemos consultado a la entrevistada para la tesina, Michelle Bordachar, analista de políticas públicas en la organización Derechos Digitales, acerca de qué implica que Chile no cuente con una autoridad específica de aplicación de la ley y nos comentó lo siguiente:

> El Consejo de la Transparencia dentro de sus facultades, atribuciones y funciones está la de fiscalizar que los organismos del Estado hagan un tratamiento adecuado de los datos personales. Cada cierto tiempo el Consejo para la Transparencia saca una circular, donde advierte sobre posibles abusos en el tratamiento de datos y envía una recomendación al respecto pero la misma no tiene ninguna validez porque no tiene facultad de sanción, ni nada. Es decir, solo puede hacer recomendaciones, entonces desde el Gobierno hacen cualquier cosa con los datos. Tampoco cuenta con personal

> capacitado en materia de protección de datos, con una autoridad de aplicación específica eso no pasaría (Entrevista a Bordachar, 2021).

Esto dificulta enormemente el ejercicio de los otros instrumentos que sí se encuentran contemplados en la ley, como la posibilidad de indemnización establecida en su art. 23°:

> La persona natural o jurídica privada o el organismo público responsable del banco de datos deberá indemnizar el daño patrimonial y moral que causare por el tratamiento indebido de los datos, sin perjuicio de proceder a eliminar, modificar o bloquear los datos de acuerdo a lo requerido por el titular o, en su caso, lo ordenado por el tribunal (Ley N° 19.628).

Siendo así, se observa que uno de los principales obstáculos que enfrentan hoy las personas para garantizar su derecho en Chile es de carácter operativo y evidencia que la falta de institucionalidad deja a los titulares de los datos con la única opción de recurrir a la justicia en caso de verse afectados por un tratamiento no autorizado de sus datos.

Cuadro comparativo: Principios incluidos en las leyes N° 25.326 de Argentina y N° 19.628 de Chile

Principios / Legislación vigente en cada país	**Argentina: Protección de los Datos Personales N° 25.326**	**Chile: Protección de la Vida Privada N° 19.628**
Consentimiento	El consentimiento debe ser libre, expreso y por escrito, habiendo informado previamente al titular la finalidad para la que serán tratados los datos personales solicitados. No se necesitará consentimiento cuando los datos personales se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal (Art. 5° 1 y 2).	La persona titular de los datos debe estar debidamente informada del propósito que motiva el almacenamiento de sus datos personales y de su posible comunicación al público. El consentimiento otorgado debe constar por escrito y podrá ser revocado por el mismo medio. No necesitará consentimiento del titular, aquellos tratamientos de datos personales que se realicen por parte de organismos públicos relativos a las materias de su competencia (Arts. 4° y 20°).
Finalidad	Los datos personales recolectados no pueden ser utilizados para finalidades distintas o incompatibles de aquellas que se declararon y el titular debe contar, previo a la recolección de los datos, con la información precisa acerca de los fines que motivan el tratamiento (Arts. 4° y 6°).	Los datos deben utilizarse solo para los fines para los cuales fueron recolectados (Art. 9°).
Exactitud	Los datos deben ser exactos y actualizarse en el caso de que sea necesario, en el caso de que estén incompletos o desactualizados deberán ser sustituidos, completados o suprimidos por el responsable del banco o archivo de datos o por el titular, el cual debe contar con la	Los datos deben ser exactos, actualizados y responder con veracidad a la situación actual del titular. Deberán ser modificados cuando sean erróneos, inexactos e incompletos. En casos de inexactitud, el responsable del banco de datos deberá proceder a su

	información necesaria para acceder a ellos (Arts. 4° 4 y 5).	eliminación, modificación o bloqueo de los datos sin requerimiento del titular (Arts. 6° y 9°).
Minimización	Los datos personales recolectados deben ser ciertos, adecuados, pertinentes y no excesivos en relación al ámbito y finalidad para los que se hubieren obtenido (Art. 4° 1).	No incluye el principio de minimización.
Limitación de conservación	Los datos deben ser destruidos cuando hayan dejado de ser necesarios o pertinentes a los fines para los cuales fueron recolectados. Al momento de la formación del archivo de datos se deberá informar el tiempo de conservación (Arts. 4° 7 y 21° h).	No establece indicación acerca de establecer límite a la conservación de los datos personales que se recolecten.
Transferencia internacional	Queda prohibida la transferencia internacional con todos aquellos países que no garanticen un adecuado nivel de protección. Dicha prohibición no rige, entre otros casos, para los intercambios de carácter médico en beneficio del afectado o por motivo de investigación epidemiológica (Art. 12°).	No incluye el principio de transferencia internacional.
Cesión	Los datos personales recolectados sólo pueden ser cedidos para el cumplimiento de fines relacionados con el interés previamente declarado y con el previo consentimiento del titular, el cual debe contar con la identificación del cesionario (Art. 11°).	Se permite la transmisión automatizada siempre que la misma guarde relación con las tareas y finalidades de los organismos participantes. Se debe informar al titular, los datos de quien requiere la transmisión, el motivo y fin de la petición, y el tipo de datos que se transmiten (Art. 5°).

Responsabilidad	El órgano de control será el responsable de realizar y garantizar todas las acciones necesarias para el cumplimiento de los objetivos y demás disposiciones de la presente ley (Art. 29).	El responsable de los registros o bases donde se almacenen datos personales deberá cuidar de ellos, haciéndose responsable de los daños. En caso de tratamiento indebido deberá indemnizar al titular, sin perjuicio de proceder a eliminar, modificar o bloquear los datos de acuerdo a lo requerido por el titular o lo ordenado por el tribunal (Art. 11° y 23°).
Seguridad - Autoridad de aplicación	Se establece la necesidad de adopción de medidas técnicas y organizativas para garantizar la seguridad y confidencialidad de los datos personales, y que permitan detectar desviaciones, intencionales o no, de información, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado (Art. 4° 5). El órgano de control (Agencia de Acceso a la Información Pública) será el responsable de realizar y garantizar todas las acciones necesarias para el cumplimiento de los objetivos y demás disposiciones de la presente ley (Art. 29).	No incluye el principio de seguridad. En el año 2008 se creó el Consejo para la Transparencia el cual entre sus funciones tiene la de velar por el cumplimiento de la ley N° 19.628 por parte de los órganos de la Administración del Estado pero con atribuciones muy poco específicas acerca de sus facultades y capacidades de fiscalización.

Fuente: Elaboración propia

Para finalizar se observa en la comparación de la ley N° 19.628 y la ley N° 25.326 que la norma argentina incluye una mayor cantidad de principios de protección de datos personales, incorporando los principios de limitación de la conservación, minimización, transferencia

internacional, cesión, seguridad y un aspecto fundamental que es el relativo a la creación de una autoridad de control, la cual se indica como responsable de fiscalizar el respeto a los derechos y obligaciones contenidos en la ley. En contraste con la ley N° 19.628 que define como responsable al titular del banco o archivos de datos sin una autoridad que fiscalice que estos titulares cumplan la ley y sin promover que las personas puedan ejercer plenamente su derecho a la protección de sus datos personales.

En el próximo capítulo se analizarán comparativamente los términos y condiciones de las aplicaciones Cuidar y CoronApp a la luz de estos principios de protección, a fin de observar en qué medida se encuentran presentes y qué tensiones surgen de la comparación.

Capítulo 5: Análisis comparado de las aplicaciones Cuidar y CoronApp

El 11 de marzo de 2020 la Organización Mundial de la Salud (OMS) declaró que la enfermedad por el SARS-CoV-2 se caracterizaba como una pandemia, como resultado de que se registraron más de 118.000 casos en 110 países.

Particularmente en Chile y Argentina ese mismo mes se habían registrado los primeros casos positivos, lo que llevó en los días posteriores a ambos países a declarar el estado de cuarentena; en Argentina mediante el Decreto N°297/2020, y en Chile mediante el Decreto N° 104. Esta medida, junto con el cierre de fronteras y de comercios no esenciales, fueron tomadas por la gran mayoría de los países de la región teniendo como referencia las experiencias de algunos países asiáticos y europeos (China, Taiwán, Tailandia, Reino Unido, Francia, Italia, etc.) en los cuales el contagio se había dado en meses anteriores y ya contaban con una gran cantidad de casos positivos y fallecidos.

Esta crisis sanitaria a nivel mundial trajo aparejada la necesidad de acceder y brindar datos e información para que las personas pudieran tomar decisiones informadas sobre su salud. Ante esta necesidad y la de contener los sistemas sanitarios, los gobiernos de diferentes países del mundo desarrollaron aplicaciones móviles para brindar información relevante a la evolución de la pandemia, así como la posibilidad de realizar autodiagnósticos sin recurrir a una institución sanitaria, acceder a instrucciones sobre cómo proceder en caso de síntomas y, en algunos casos, hacer rastreo de contactos y seguimiento de cuarentena. A nivel mundial fueron China, Corea del Sur y Singapur los primeros países en desarrollar y utilizar sistemas

de vigilancia masivos para seguir la propagación del virus y detectar y limitar la exposición de las personas a zonas de focos de contagio (“El uso de las aplicaciones…”, 2020). En particular en América Latina fue Bolivia el primer país en lanzar una *coronapp,* seguido por Colombia y Uruguay (Aguerre, 2020).

Las aplicaciones Cuidar y CoronApp fueron desarrolladas por Argentina y Chile como parte de las políticas públicas desplegadas para el control y combate de la pandemia y están disponibles para su descarga en las tiendas de Google Play y Apple Store.

En Argentina, el gobierno lanzó la aplicación denominada como “COVID-19 Ministerio de Salud” el 23 de marzo de 2020, la cual fue desarrollada por la Secretaría de Innovación Pública dependiente de la Jefatura de Gabinete de Ministros. El 27 de abril del mismo año se la relanzó bajo el nombre Cuidar declarando que en su diseño intervinieron empresas del sector privado, la comunidad científica y el sector público (Fundación Sadosky, el CONICET, Hexacta, Globant, G&L Group, C&S, QServices, GestiónIT, Intive, Finnegans y Faraday (nucleadas en la Cámara de la Industria Argentina del Software -CESSI-); ARSAT; Amazon Web Services (“Sistema y aplicación Cuidar”, 2020). La misma está disponible en las tiendas de Google Play y Apple Store y es compatible con dispositivos Android 5.0 y posteriores, Iphone 13.0 o anteriores. Desde un inicio la aplicación fue anunciada desde la Secretaría de Innovación Pública como un servicio que “complementa y asiste las políticas de prevención y cuidado de la población y, en particular, brinda elementos e insumos concretos para la intervención sanitaria de los ministerios de Salud en todo el territorio nacional” (“Sistema y aplicación Cuidar”, 2020). Sus objetivos declarados en sus términos y condiciones son ayudar a prevenir la propagación del virus, brindar información fidedigna a los usuarios, dar intervención a las autoridades sanitarias, así como también, colaborar a partir de los datos

recolectados en el desarrollo de políticas públicas e investigaciones que permitan mitigar el desarrollo de la enfermedad, ampliar y mejorar técnicas sanitarias y preventivas relacionadas con la salud de la población (Términos y condiciones Cuidar, 2020). En octubre de 2022 la aplicación tenía más de diez millones de descargas en Google Play[7], mientras que Apple Store no publica la cantidad de descargas.

Por su parte, CoronApp fue lanzada el 16 de abril del 2020 por la división Gobierno Digital del Ministerio Secretaría General de la Presidencia (SEGAPRES)[8]. En sus términos y condiciones declara ser una herramienta digital ofrecida por la Subsecretaría de Redes Asistenciales dependiente del Ministerio de Salud y se la define como "una aplicación gratuita de información y monitoreo de síntomas de COVID-19", aunque a continuación proclama brindar los servicios de monitoreo de síntomas, conectar al usuario con sitios oficiales del gobierno, centros de salud y un chatbot informativo, así como también, acceder al servicio de Comisaría Virtual[9] para reportar incidentes y aglomeraciones; funciones que terminaban excediendo el alcance de su primera definición como una aplicación de información y monitoreo de síntomas. La aplicación obtuvo más de cien mil descargas (Nájeray Ricaurte, 2020) y al cierre de este trabajo no se encuentra disponible para su descarga en dispositivos Android o iOS.

Ambas aplicaciones fueron lanzadas como de uso voluntario y gratuito, requiriendo para sus descargas de dispositivos móviles con acceso a Internet el cual debía ser, en todos los casos,

[7] https://play.google.com/store/apps/details?id=ar.gob.coronavirus&hl=es_AR&gl=US

[8] Gobierno Digital es la División encargada de la Transformación Digital del Estado, tiene como objetivo coordinar y asesorar a los órganos de la Administración del Estado en el uso estratégico de las tecnologías digitales.

[9] Es una plataforma web de Carabineros de Chile que permite dejar constancia sobre temas como: pérdidas de documentos, pensión de alimentos, régimen de visitas, entre otros; y durante períodos de contingencia es la plataforma desde donde se tramitan permisos, salvoconductos y reciben denuncias con el fin de derivarlas al Ministerio Público.

provisto por el usuario. Pueden ser utilizadas por todas aquellas personas mayores de 18 años que cuenten con Documento Nacional de Identificación en caso de Argentina, y con Rol Único Nacional (RUN) o pasaporte en caso de Chile, y hayan prestado su consentimiento a los términos y condiciones.

Anteriormente se indicó que en cuanto a la dimensión política de estas aplicaciones se considera a las mismas como parte de las políticas públicas llevadas a cabo por los Estados Nacionales para el combate a la pandemia, las cuales ofrecen y generan información en tiempo real con el fin de monitorear y predecir el curso de la enfermedad y contener los sistemas de salud. Retomando a Oszlak y O'Donnell (1984), en la búsqueda de los Estados por dar respuesta a asuntos socialmente problematizados no se plantea una sola iniciativa sino que la misma suele ser una suma de decisiones de una o más organizaciones. Esto se manifiesta observando los diferentes actores que intervinieron en el desarrollo de ambas aplicaciones, por un lado en Cuidar donde el Estado argentino llevó a cabo la iniciativa desde la Secretaría de Innovación Pública, la cual depende de la Jefatura de Gabinete de Ministros de la Nación, junto con el Ministerio de Salud de la Nación, el Ministerio de Ciencia y Tecnología, la comunidad científica y el sector privado. Por el otro, CoronApp la cual fue llevada a cabo por la División de Gobierno Digital del Ministerio Secretaría General de la Presidencia (SEGAPRES)[10], la Subsecretaría de Redes Asistenciales del Ministerio de Salud (MINSAL) e intermediarios privados como Amazon Web Services.

En ambos casos se observa lo expresado por Castells (2006) en cuanto a que los Estados tienen un rol central "(...) ya sea deteniendo, desatando o dirigiendo la innovación

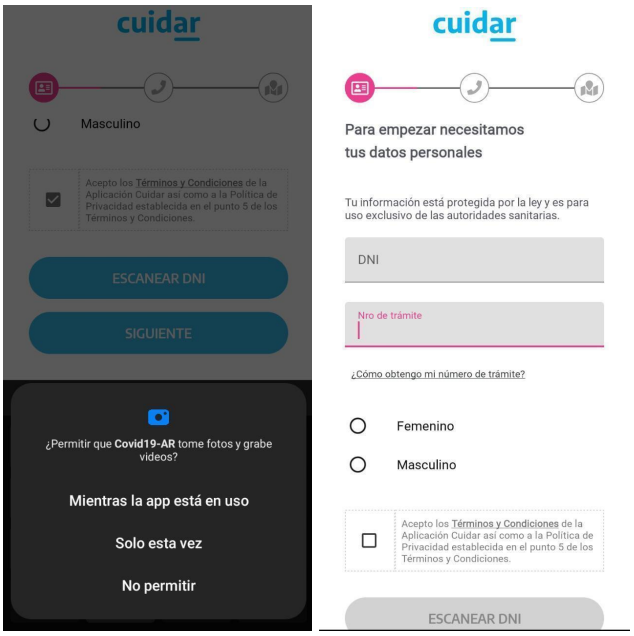
10 https://obtienearchivo.bcn.cl/obtienearchivo?id=documentos/10221.1/79593/1/boletin_coronavirus_10.1_FINAL.pdf

tecnológica (...) ya que expresa y organiza las fuerzas sociales y culturales que dominan en un espacio y tiempo dados." Fue mediante la iniciativa de los Estados que estas aplicaciones pudieron ser desarrolladas y administradas en tiempo récord debido a la urgencia que suponía detener el avance de la enfermedad, garantizar el cumplimiento de las medidas de aislamiento y contener los sistemas de salud. En el mismo sentido, la entrevistada para la tesina Natalia Zuazo, periodista especializada en tecnología, explicaba que no necesariamente los Estados tienen que encargarse de todo el desarrollo tecnológico sino que también pueden funcionar como articuladores entre distintos sectores:

> El Estado puede hacerlo con sus propias capacidades estatales desarrollando sus propios softwares, sus propios servidores, su propia infraestructura o puede hacerlo con otras empresas. De hecho, gran parte de la aplicación Cuidar se hizo así, desde organismos estatales y con otros externos (Entrevista a Zuazo, 2021).

Estas herramientas tecnológicas, requieren para su funcionamiento de la recolección y tratamiento de datos personales y sensibles. Al abrir la aplicación Cuidar por primera vez son solicitados para ingresar: DNI y número de trámite[11], género (femenino o masculino), acceso a la cámara para escanear DNI y aceptar los términos y condiciones.

[11] El número de trámite es un número único e intransferible de 11 dígitos que se encuentra en la parte inferior del DNI tarjeta.



Primera y segunda pantalla de solicitud de datos personales para registro e ingreso a Cuidar.

Fuente: Aplicación Cuidar.

En el caso de CoronApp ofrece dos formas de ingreso: una opción es el ingreso con clave única[12] y Rol Único Nacional[13] (RUN), y la segunda opción con Rol Único Tributario[14] (RUT) o pasaporte, opción que exige que el usuario se registre proporcionando los siguientes datos: cédula de identidad, RUN o pasaporte, número de documento, nombre completo, número de teléfono, edad, comuna, correo electrónico (opcional), y una contraseña.

[12] La Clave Única sirve para obtener en línea diversos servicios y beneficios que ofrece el Estado.

[13] Es el número identificatorio único e irrepetible que posee todo chileno, residente o no en Chile, y todo extranjero que permanezca, temporal o definitivamente, con una visa distinta a la visa de turista en dicho país. Es el equivalente al DNI en Argentina.

[14] Número de identificación Tributaria coincidente con el RUN.

Pantallas de solicitud de datos personales para el registro e ingreso a CoronApp.

Fuente: Twitter Sebastián Piñera @sebastianpinera.

Junto con estos datos de acceso, para utilizar la función de autodiagnóstico ambas aplicaciones requieren que el usuario responda preguntas sobre si posee síntomas como ser: tos, pérdida de olfato o gusto, dolor de garganta, flema amarilla o verdosa, tos; también si ha tenido contacto, vive o trabaja con una persona caso confirmado COVID-19; si tuvo contacto estrecho en los últimos diez días; que indique la temperatura corporal; y en el caso de Cuidar se suman las preguntas relativas a si la persona ha estado embarazada, y si posee enfermedades preexistentes como: cáncer, diabetes, enfermedad hepática, renal crónica y/o respiratoria.

Srnicek (2018) explica que "cada dato como entidad grabada requiere sensores para ser capturado y enormes sistemas de almacenamiento" (p.41), es aquí donde plataformas como Google y Amazon suelen aparecer como intermediarias ya que el procesamiento y almacenamiento de estos datos supone de grandes inversiones en infraestructura y desarrollo tecnológico. En el caso de CoronApp, por ejemplo, sus términos y condiciones indican que la información recolectada se almacena y replica bajo la administración del Ministerio de Salud en una nube privada de Amazon Web Services, ubicada en Virginia, Estados Unidos. Ante

esto se consultó con la entrevistada para la tesina, Michelle Bordachar quien indicó: “probablemente esa decisión haya sido tomada por cuestiones económicas, pensando en que esos servidores seguramente son más seguros que los nuestros” (Entrevista a Bordachar, 2021).

Si bien en los términos y condiciones se afirma que la confidencialidad y privacidad de la información de los usuarios se somete a las leyes chilenas, esto no sería tal porque como se vio anteriormente la ley N° 19.628 no contempla ningún punto relativo a la transferencia internacional de datos y tampoco existe ley específica que regule al respecto en el país.

En el caso de Cuidar, los términos y condiciones declaran que la aplicación cumple con el principio de legalidad al tener registrada su base de datos y que la misma es responsabilidad de la Subsecretaría de Gobierno Abierto y País Digital de la Secretaría de Innovación Pública de la Jefatura de Gabinete de Ministros de la Nación. A diferencia de la aplicación chilena, la Subsecretaría reglamentó a través de la Disposición 3/2020 la creación de una base de datos denominada “COVID-19 Ministerio de Salud” con el objetivo de centralizar los datos recabados por la aplicación sin la utilización de plataformas nubes externas.

Se observa así que frente al mismo asunto los países han tomado decisiones opuestas, por un lado la de almacenar los datos en una nube de Amazon Web Services con jurisdicción en Estados Unidos; por el otro, constituir una base de datos propia. Independientemente de cual sea la opción elegida, la entrevistada, Natalia Zuazo, explicó que en cuanto al almacenamiento:

> El principio que debe aplicar siempre es el de minimización de tiempo, el mínimo tiempo posible para los fines recomendados por el Ministerio de Salud y autoridades sanitarias (...) Por supuesto que siempre es mejor tener infraestructura propia para

> almacenar pero a veces cuando estás desarrollando tecnología en el momento no tenés esa infraestructura disponible (Entrevista a Zuazo, 2021).

Otro punto relevante al análisis es el tratamiento de los datos sensibles, caracterizados como aquellos que entre otras cosas revelan información referente a la salud, y que en ambas leyes gozan de protección especial. Se observa que en los términos y condiciones de la aplicación argentina se contempla su protección indicando que los mismos serán almacenados únicamente el período que dure la pandemia y que luego podrán preservarse para fines científicos siempre que sean anonimizados, hecho que hace que dejen de ser considerados como datos personales. En los términos y condiciones de la aplicación chilena se establece que los datos sensibles son "toda la información que surja, tanto de la ficha clínica, como de los estudios y demás donde se registren procedimientos y tratamientos a los que fueron sometidas las personas" (Términos y condiciones CoronApp, 2020), y que el tratamiento de dichos datos están prohibido por el artículo 10° de la ley N°19.628 a no ser media el consentimiento del titular o que una ley lo disponga. Es decir, en ningún punto se hace referencia a algún mecanismo de protección particular de estos datos sino que únicamente se indica que su tratamiento es lícito porque se cumple con la condición de consentimiento establecida en la ley. Sobre este punto Natalia Zuazo explicó en la entrevista realizada, el riesgo de dejar expuesta una base de datos sensibles:

> Si se deja expuesta una base de datos de una persona que tuvo Covid y esa persona el día de mañana quiere conseguir un trabajo, el empleador se fija en esa base de datos y por eso elige no contratarlo, se están afectando directamente sus derechos. Claramente cuando un desarrollo local o provincial no toma en cuenta las medidas de protección y seguridad adecuadas está exponiendo a su población a estas violaciones de derechos (Entrevista a Zuazo, 2021).

Observado esto, se advierte que la solicitud de datos personales para ingresar a ambas aplicaciones es muy similar pero no así lo que se indica en los términos y condiciones con respecto al almacenamiento de los mismos. Por un lado, el Estado argentino al momento del desarrollo de Cuidar decidió constituir un base de datos personales bajo responsabilidad de la Subsecretaría de Gobierno Abierto y País Digital e indicar en los términos que los datos sensibles recolectados serán almacenados durante el período que dure la pandemia y luego se podrán conservar anonimizados para funciones científicas. Por su parte, el Estado chileno tomó la decisión de almacenar los datos personales recolectados en una nube de Amazon Web Services con domicilio en Virginia, Estados Unidos; y si bien en sus términos expresa que dicho archivo deberá someterse a las normativas chilenas, la actual ley N° 19.628 no contiene ningún artículo referido a la transferencia internacional de datos, ni a las medidas de seguridad necesarias que debería adoptar el responsable del banco para garantizar una adecuada protección de los datos personales almacenados.

A continuación, se procede al análisis comparativo de los términos y condiciones de las aplicaciones desde los principios de protección seleccionados.

5.1 Consentimiento

Como se observó anteriormente, tanto en la ley N° 25.326 de Protección de Datos Personales de Argentina como en la N° 19.628 relativa a la Protección de la Vida Privada de Chile, se establece que el tratamiento de datos es lícito siempre que el titular brinde su consentimiento al haber sido informado del propósito del almacenamiento y que el mismo debe ser expresado de forma clara y por escrito. Ambas leyes disponen que no será necesario el consentimiento

cuando los datos se obtengan de fuentes accesibles al público, e incorporan una distinción particular para el tratamiento de los datos personales sensibles. La diferencia sustancial entre ambas es que la ley argentina establece que los datos de salud podrán ser recolectados y tratados cuando medien razones de interés general, y para fines científicos siempre que sus titulares no puedan ser identificados. En cambio, la ley chilena establece que se podrán recolectar y tratar datos sensibles, siempre que exista consentimiento del titular o una ley lo autorice; y no prevé la toma de ninguna medida especial para su tratamiento.

Los términos y condiciones de ambas aplicaciones establecen como primera condición la necesidad de que las personas presten su consentimiento, y que en caso de que no estén de acuerdo con ellos se abstengan de utilizar la aplicación. En ambos términos se indica que los datos de salud podrán ser tratados con fines científicos y epidemiológicos, bajo previa anonimización; es decir, se cumple con lo establecido en las leyes sobre la necesidad de asegurar protección especial a los datos sensibles.

Sin embargo, en los términos y condiciones de CoronApp se observan algunas particularidades, por un lado, en la sección 7 se indica que el Ministerio de Salud "podrá ser requerido de entregar acceso o divulgar los datos a terceros" (Términos y Condiciones CoronApp, 2020), lo cual está prohibido por el artículo 24° de su ley, que expresa que los datos de salud son considerados datos reservados y que los mismo sólo pueden ser entregados a terceros mediante consentimiento por escrito del titular. En este sentido, si bien el titular presta su consentimiento a los términos y condiciones de la aplicación, en los mismos no se explicita, ni especifica si esos terceros que podrían acceder a los datos solicitarían nuevamente el consentimiento al titular o con el otorgado previamente es suficiente, sobre

todo considerando que los datos recolectados y, sobre todo los sensibles, no deberían ser tratados con otra finalidad que la prevista en los términos.

Por otro lado, en la sección 2 se indica que "con el objeto de proporcionar a los usuarios un mejor servicio, puede resultar necesario recopilar y procesar cierta información (...)" (Términos y condiciones CoronApp, 2020) y en ningún lugar de todo el documento se detalla a qué se refiere la expresión "cierta información". Michelle Bordachar, a quien se entrevistó para esta tesina, indicó: "(...) de partida, no cumplía con el principio de la ley de que el consentimiento debe ser informado porque uno no estaba consintiendo con algo que uno estuviera informado porque no te informaban que datos exactamente iban a recabar" (Entrevista a Bordachar, 2021).

En conclusión, ambas aplicaciones incorporan el principio de consentimiento. En el caso de la aplicación argentina, el mismo es desarrollado tal como se prevé en la ley; en el caso de la aplicación chilena, el mismo es incluido pero se advierten ciertas irregularidades como que no se especifica claramente su alcance al tratarse de datos sensibles y se deja ciertas cláusulas muy poco específicas con respecto a qué datos recopila la aplicación; dos cuestiones frente a las cuales se considera que no se debe dejar lugar a interpretaciones azarosas.

5.2 Finalidad, exactitud y minimización

Se retoma el **principio de finalidad** que, como se observó anteriormente, establece que los datos personales deberán ser recogidos en base a fines explícitos y legítimos y no podrán ser tratados con propósitos contrarios a estos.

En los términos y condiciones de CoronApp de Chile se establece como primera finalidad que la misma "es una aplicación gratuita de información y monitoreo de síntomas" (Términos

y condiciones CoronApp, 2020). A su vez, a lo largo del texto se agregan otras finalidades, como que los datos previamente anonimizados podrán ser tratados por el Ministerio o por terceros "con fines históricos, estadísticos, científicos y de estudios o investigaciones en el área sanitaria"; una vez anonimizados los datos dejan de ser considerados datos personales y por lo tanto dejan de estar bajo el amparo de la ley. Además de esto, los términos y condiciones también indican que "con el objeto de proporcionar a los usuarios un mejor servicio, puede resultar necesario recopilar y procesar cierta información, la cual se obtendrá del dispositivo móvil en donde se ha instalado la aplicación", todo esto con el objetivo de "realizar mejoras en la aplicación que la optimicen y fortalezcan" (Términos y condiciones CoronApp, 2020).

Se observa así que queda añadida una nueva finalidad pero bajo unos términos muy vagamente expresados, al no especificar qué se indica con "mejor servicio" y si el titular será informado previamente de esto. Como se detalló en el apartado anterior, en la sección 7 se hace referencia a que el Ministerio de Salud podrá entregar datos a terceros en virtud de una orden judicial o administrativa, pero no se indica si estos terceros tienen la obligación de tratar los datos con los mismos fines previstos en la aplicación o si podrán usarlos con otros frente a los cuales el titular no otorgó su consentimiento.

Por último, la aplicación también cuenta con las funciones de "ayuda vecina", "reportar incidentes o aglomeraciones" y "conectar con la Comisaría Virtual"; las cuales se observa que no se enmarcan dentro de las finalidades declaradas de brindar información o monitoreo de síntomas sino que se agrega una más que es la de realizar "acciones útiles de seguimiento de pacientes para la protección de la salud públicas, durante la vigencia de la emergencia

sanitaria", para la cual la aplicación solicita acceso a la geolocalización declarando que "CoronApp no almacena estos datos" (Términos y condiciones CoronApp, 2020).

En cuanto al **principio de exactitud y minimización**, de los cuales el primero refiere a que los datos sean correctos, exactos y actualizados; y el segundo, con respecto a que sean adecuados, pertinentes y necesarios a los objetivos especificados, se indicó que la ley de protección de datos personales vigente en Chile incluye el de exactitud pero no así el de minimización. Esto también se advierte en los términos y condiciones de la aplicación chilena donde al aceptarlos, el usuario "se compromete a mantener la información en su cuenta de forma veraz, exacta, completa y actualizada" (Términos y Condiciones CoronApp, 2020) y que en caso de no ser así estará imposibilitado de utilizar los servicios previstos. La Guía Legislativa (2015) indica que quien recopile o procese los datos debe establecer mecanismos para asegurarse que los datos provistos por los titulares sean correctos, exactos, completos y actualizados; en relación a esto en los términos y condiciones se brinda una dirección de correo electrónico a través del cual los usuarios pueden solicitar acceso a sus datos para actualizarlos, rectificarlos y/o eliminarlos.

En cuanto al principio de minimización no se incorpora en los términos y esto se observa cuando se indica que se podrá recolectar del dispositivo móvil del usuario "cierta información", sin dar detalles al respecto. La abogada y entrevistada para la tesina, Michelle Bordachar indicaba lo siguiente:

> El tema es que si uno leía los términos y condiciones de partida no te pedían solo los datos que necesitaban sino que además podrían pedirte otros, la lista no era taxativa sino más bien abierta "vamos a pedirte datos tales como…" y en derecho cuando sale un "tales como" eso significa cualquier cosa (Entrevista a Bordachar, 2021).

A modo de resumen de estos primeros principios observados en la aplicación chilena, se advierte que en los términos y condiciones se incluye el **principio de finalidad** pero al igual que con el de consentimiento se dejan algunos vacíos al momento de especificar qué obligaciones y para qué fines podrán utilizar los datos en caso de ser accedidos por terceros. No se cumple con el **principio de minimización**, el cual tampoco se encuentra en la ley. Se incorpora el **principio de exactitud** en base a cómo está establecido en la ley N° 19.628.

Ahora se pasará a observar cómo se incluyen estos tres principios en los términos y condiciones de la aplicación Cuidar para concluir el apartado con una conclusión comparativa de ambas.

Para empezar, en la sección 5.2 de los términos y condiciones de Cuidar se declara que cumple con el **principio de finalidad** "dado que la Secretaría utiliza los datos personales recabados únicamente para el fin que fueron recolectados" (p.5). En cuanto al primer fin que se declara se indica que "brinda información sobre diversos temas referentes a los síntomas y/o prevención del virus COVID- 19 con la finalidad de ayudar a prevenir la propagación del virus, como así también erigirse en una fuente de información" (p.1). Estos no son los únicos ya que más adelante se agrega que el acceso a la geolocalización tiene como fin dar intervención a las autoridades sanitarias o bien permitir el desarrollo de políticas públicas que contribuyan a la prevención y mitigación de la propagación de la enfermedad; y en la sección 1.5 se agrega que "la Secretaría podrá incluir funcionalidades en la Aplicación que permitan entre otras cosas, recibir asistencia online o asistencia audiovisual sobre los cuidados, etc.", dejando abierta posibles futuras funcionalidades, sin saber qué datos personales serán

requeridos para ellas. Por último, se indica que para fines científicos o epidemiológicos todos los datos sensibles y de geolocalización deberán ser anonimizados.

En lo que refiere al **principio de exactitud** en la sección 2.3 de los términos y condiciones se observa que, al igual que en la aplicación chilena, el titular de los datos debe garantizar "que todos los datos personales suministrados en el proceso de registro son verdaderos, completos y se encuentran actualizados" (p.2); y tal como prevé la ley en el artículo 4° inciso 6[15] se garantiza que el usuario pueda acceder, rectificar y suprimir sus datos personales a fin de mantenerlos actualizados, solicitándolo a través del mail (covid19app@jefatura.gob.ar) de la Subsecretaría de Gobierno Abierto. Es decir, al igual que en los términos y condiciones de CoronApp, se otorga un mecanismo para que el usuario pueda acceder a actualizar sus datos. En cuanto al **principio de minimización**, se observa con respecto a los datos recolectados para los fines previstos que uno de los más problemáticos es el relativo a la solicitud de ingresar el número de trámite junto con el número de DNI que figura en el carnet del usuario. Gauna (2020) en el artículo "En caso de emergencia: descargue una app - Parte II", indicaba que "al ser datos que se encuentran en el documento físico, el principal riesgo es que esa información puede llegar a ser obtenida por un tercero"; además de que la aplicación no sólo solicita que el usuario brinde los números sino también una foto de frente y dorso de su DNI. La entrevistada para la tesina, Natalia Zuazo, también se refería a esto indicando: "Hubieron cosas que podrían haberse hecho mejor, sobre todo la parte del uso del número de trámite que me parece que es un problema que se sigue acarreando desde la app MiArgentina y en algún momento hay que rever" (Entrevista a Zuazo, 2021); es decir que solicitar estos datos de

[15] Los datos deben ser almacenados de modo que permitan el ejercicio del derecho de acceso de su titular.

forma conjunta para acceder a una aplicación conlleva un grado alto de inseguridad al poder ser difundidos por terceros.

Para concluir con el apartado, los tres principios de datos personales aquí analizados se incluyen dentro de las aplicaciones pero en distintos grados. Por un lado, en cuanto al **principio de finalidad**, ambas detallan cuáles son los fines de las aplicaciones, donde se advierte que en ambos casos exceden los objetivos de brindar información y monitoreo de síntomas. Por otro lado, en lo relativo al **principio de minimización** se observa que CoronApp no lo cumple debido a que deja abierto, sin especificar, que se podrá recolectar "cierta información" del dispositivo móvil del usuario. En tanto que Cuidar sí lo cumple, pero se indicó como punto problemático la solicitud referida al ingreso del número de trámite y DNI, lo cual pueden causar graves daños a la privacidad del titular en caso de ser accedidos y/o difundidos por terceros. Por último, ambas incluyen el **principio de exactitud** dejando al titular de los datos como el responsable de garantizar que los mismos estén completos, actualizados y sean verdaderos. Ambas aplicaciones brindan direcciones de correo electrónico a través de las cuales los titulares de los datos pueden acceder a corregirlos, actualizarlos, rectificarlos o suprimirlos.

5.3 Limitación a la conservación, transferencia internacional y cesión de datos personales

En este apartado analizaremos en qué medida se incluyen los principios de **limitación a la conservación, transferencia internacional de datos y cesión** en las aplicaciones aquí analizadas.

Para empezar, se retoma el principio **de limitación de conservación**, también conocido como minimización de tiempo, el cual refiere a que los datos personales recolectados "pueden mantenerse solo el tiempo que sea necesario para el fin para el cual se hayan recopilado" (Guía Legislativa, 2015, p.22). Anteriormente en el apartado 4.1 del presente trabajo se indicó que la ley vigente en Chile N° 19.628 no cuenta con un artículo específico que incorpore este principio; sin embargo en los términos y condiciones de CoronApp se indica que:

> La alerta sanitaria que habilita la recopilación de estos datos, tiene una duración de un año contado desde el 05 de febrero de 2020, sin perjuicio de la facultad de las autoridades de ponerle término anticipado si las condiciones sanitarias así lo permiten o de prorrogarla en caso de que estas no mejoren. Los datos serán almacenados y tratados durante el periodo de tiempo que se mantenga la alerta sanitaria. Para fines históricos, estadísticos, científicos y de estudios o investigaciones los datos serán anonimizados (Términos y condiciones Coronapp, 2020).

Se advierte así que se establece un tiempo límite a la conservación, contemplando que este pueda cambiar según evolucione la pandemia y la enfermedad. El Ministerio de Salud decretó en septiembre del 2022, a través de la resolución N° 1339, la extensión del periodo de Alerta Sanitaria por lo que hasta esa fecha los datos personales recolectados pueden ser almacenados y tratados.

Al igual que con el **principio de limitación a la conservación**, se ha detallado que la ley N°19.628 tampoco incluye **el principio de transferencia internacional de datos**, el cual, según la Guía Legislativa (2015), no debería indicar "requisitos relativos a la localización de los datos" sino más bien establecer "medidas de cooperación" (p.11); aunque para ciertas circunstancias particulares indica que "las leyes nacionales podrían restringir justificadamente

el flujo transnacional de datos y requerir que los datos se almacenen y procesen localmente, siempre por razones imperiosas"(p. 40). En los términos y condiciones de la aplicación chilena se indica que los datos recolectados se almacenan en una base de datos de Amazon Web Services, ubicada en Virginia, Estados Unidos y que "la utilización de esta tecnología respeta la confidencialidad y privacidad de la información de sus usuarios de acuerdo a las leyes chilenas y se somete a la legislación de nuestro país en caso de controversias" (Términos y condiciones CoronApp, 2020). En este sentido, la entrevistada Michelle Bordachar expresaba que de todos los puntos problemáticos de la aplicación, este era el menos importante debido a que Chile no cuenta con una norma específica sobre transferencia internacional de datos, pero que, sin embargo, enviar datos personales afuera siempre tiene la complicación de no saber quiénes pueden acceder a ellos (Entrevista a Bordachar, 2021). A este punto, Natalia Zuazo también comentaba en la entrevista realizada que la inversión en infraestructura para el almacenamiento de grandes cantidades de datos, debería ser una política pública a largo plazo por parte de los Estados, para no depender de plataformas extranjeras y que en ocasiones de emergencias y tratamiento de datos sensibles a gran escala, se garantice que queden almacenados bajo jurisdicción y protección legal del país.

Por último, en cuanto al **principio de cesión** el cual en la Declaración conjunta de la sociedad civil (2020) se retoma indicando que:

> Si los gobiernos firman acuerdos para compartir datos con otras entidades públicas o del sector privado, deben hacerlo basándose en la ley, y la existencia de tales acuerdos, así como la información necesaria para evaluar su impacto en la privacidad y los derechos humanos, debe revelarse públicamente, por escrito, con las cláusulas

> de suspensión y con supervisión pública y otras salvaguardias por defecto (Declaración conjunta de la sociedad civil, 2020).

Al analizar los términos y condiciones de CoronApp, se observa en el apartado 7 que los datos recolectados serán accedidos tanto por el Ministerio de Salud, como por otras entidades establecidas por ley y el MINSAL podrá "ser requerido a entregar acceso o divulgar los datos a terceros, en virtud de una orden judicial, esto es por los tribunales de justicia, o administrativa, en el caso de sumarios sanitarios" (Términos y condiciones CoronApp, 2021). Es decir, si bien se indica que debe existir alguna disposición legal o administrativa para el acceso de los datos personales recolectados por parte de terceros, no se detalla cómo se informará al titular de los datos de esto y cómo se supervisará que los terceros que accedan cumplan con lo estipulado en la ley y en los términos y condiciones.

A continuación se releva como se incluyen estos tres principios en los términos y condiciones de la aplicación argentina para poder realizar la comparación entre ambos.

En cuanto al **principio de limitación a la conservación**, a diferencia de la ley chilena, la ley argentina N° 25.326 de Protección de Datos Personales incorpora a través de su artículo 21 inciso h que todo registro de archivo de datos debe incluir el tiempo de conservación. En los términos y condiciones de Cuidar únicamente se indica en la sección 5.9 que los datos sensibles y aquellos referidos a la geolocalización "se preservarán únicamente mientras sean necesarios y dure la emergencia sanitaria" (p.7), sin indicar qué sucederá con los datos personales que no son considerados sensibles. En diciembre del 2021 el presidente Alberto Fernandéz determinó por medio del Decreto N° 867/2021 la prórroga de la emergencia sanitaria hasta diciembre del 2022, por lo que se entiende que se almacenan y no se procedió a anonimizarlos hasta esa fecha.

Con respecto a los **principios de transferencia internacional de datos y cesión,** la ley argentina N° 25.326 también incluye, a diferencia de la ley N° 19.628, artículos específicos sobre ello. En particular, en el art. 21 se indica que "es prohibida la transferencia de datos personales de cualquier tipo con países u organismos internacionales o supranacionales, que no proporcionen niveles de protección adecuados", con algunas excepciones como los datos de carácter médico que sean necesarios para la asistencia del afectado, o con que se utilicen para investigación epidemiológicas, con la exigencia de que se aplique en dichos datos sensibles algún procedimiento de disociación de la información de modo que los titulares no puedan ser identificados. En relación a esto, en los términos y condiciones de Cuidar se indica en la sección 5.5 que la Subsecretaría podrá ceder información "únicamente a otras entidades estatales y/o establecimientos sanitarios nacionales, provinciales o municipales, para que estos puedan contener y/o mitigar la propagación del virus COVID19, ayudar a prevenir la sobreocupación del sistema sanitario argentino" (p.1), excluyendo así toda transferencia internacional y garantizando que los terceros que reciben estos datos pertenecen al ámbito sanitario y persiguen los mismos fines que motivan la recolección de datos personales desde la aplicación. Asimismo, los términos agregan que la Subsecretaría deberá informar las cesiones que haga de datos personales no disociados, siempre que el titular así lo solicite (Términos y condiciones Cuidar, 2020); esto brinda una garantía más para que el titular tenga control sobre sus datos personales y cumple con lo decretado en la ley.

Para concluir con este apartado, se observa que los tres principios de protección de datos personales aquí analizados se incluyen en ambas aplicaciones y en distintos grados. Empezando con el **principio de limitación a la conservación**, en los términos y condiciones de CoronApp, si bien no se exige mediante la ley, se lo incluye indicando que los datos se

conservarán durante el tiempo que dure la emergencia sanitaria, el cual es considerado como un año desde febrero de 2020 pero que dicho plazo podrá variar en función de cómo evolucione la enfermedad. A su vez, se indica que luego de finalizado este periodo se podrán conservar los datos recolectados, con fines científicos y/o estadísticos siempre que sean anonimizados. En cuanto al mismo principio en la aplicación Cuidar, se indica que los datos sensibles y de geolocalización deberán eliminarse una vez que finalice la emergencia sanitaria pero no se explicita qué se hará con el resto de los datos personales recabados. A saber, se puede decir que en ambos términos y condiciones se incluye el principio pero sin mayores especificaciones y se dejan algunos puntos sin resolver.

Ahora en cuanto al **principio de transferencia internacional y cesión de datos**, se observó que CoronApp permite la transferencia con terceros, sin hacer distinción entre entidades públicas y/o privadas, nacionales o internacionales, siempre que exista una disposición legal o administrativa que lo respalde pero sin detallar en ningún lugar si estos terceros deberán cumplir con alguna obligación o fines relativos a los perseguidos con la aplicación, ni si el titular podrá acceder a dicha a información. Los mismos principios en la aplicación Cuidar se encuentran de forma muy distinta, primero se excluyen las transferencias internacionales de datos al establecer que la Subsecretaría de Gobierno Abierto sólo podrá ceder información a otras entidades estatales o establecimientos sanitarios del país que tengan como fin evitar la propagación del virus, y se agrega que el usuario podrá solicitar a la Subsecretaría que informe acerca de las sesiones de datos personales no anonimizados que se hayan realizado. Esto último cumple con el punto 7 de la Declaración conjunta de la sociedad civil que dice que “se debe ofrecer a las personas la oportunidad de conocer e impugnar toda medida que se tome en relación con la COVID-19 para recopilar, agregar, conservar y emplear datos”

(Declaración conjunta de la sociedad civil, 2020). Para resumir, se concluye que los términos y condiciones de Cuidar brindan mayor protección a los datos personales, y ambas aplicaciones, con la excepción de los que sucede con el principio de limitación en la aplicación CoronApp, cumplen con los principios de protección tal como se exige mediante las leyes de protección de datos personales vigentes.

5.4 Responsabilidad y seguridad

A continuación, se observarán cómo se incluyen los principios de responsabilidad y seguridad en los términos y condiciones de las aplicaciones Cuidar y Coronapp.

Empezando por el **principio de responsabilidad,** como se indicó en el apartado 4.5 de esta tesina, ambas leyes de privacidad y protección de datos personales vigentes en Argentina y Chile, definen como responsable de los datos al titular del archivo, registro o base de almacenamiento, pero tienen algunas distinciones. Por una lado, la ley argentina N° 25.326 indica que quien sea el responsable debe adoptar medidas para garantizar la seguridad y confidencialidad de los datos personales, mientras que la legislación chilena N° 19.628 no exige la adopción de medidas de protección y seguridad, solo establece que el responsable deberá indemnizar al titular en caso de tratamiento indebido.

En un primer momento en los términos y condiciones de CoronApp de Chile, no era sencillo encontrar a quien se definía específicamente como el responsable del archivo o registro de datos. En primer lugar se indicaba que la aplicación había sido desarrollada por la División de Gobierno Digital del Ministerio Secretaría General de la Presidencia de Chile (SEGPRES). Luego, se modificaron indicando 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 (...)" (Términos y Condiciones CoronApp, 2020). Frente a esto, la entrevistada para la tesina Michelle Bordachar comentaba lo siguiente:

> Se dio algo muy particular porque al principio la aplicación fue desarrollada por la División de Gobierno Digital del Ministerio Secretaría General de la Presidencia de Chile (SEGPRES) y esa era la autoridad que estaba en los términos y condiciones de la aplicación. Después, cuando empezaron a haber quejas en contra de la aplicación se dieron cuenta de que la única base habilitante que podían tener si no era el consentimiento de las personas, era en base al código sanitario que le da facultades al Ministerio de Salud (MINSAL), entonces ahí tuvieron que cambiar todo el discurso y decir que el responsable de la aplicación no era SEGPRES y Gobierno Digital, sino que era el Ministerio de Salud pero si uno le preguntaba a la gente del MINSAL acerca de las cláusulas que eran bien abusivas te decían que ellos no la habían hecho, que el responsable era la Secretaría General de la Presidencia (Entrevista a Bordachar, 2021).

Específicamente en el punto 5 de los términos y condiciones se establece que toda la información registrada es almacenada y replicada en una nube privada, propiedad de Amazon Web Services, ubicada en Virginia, Estados Unidos pero que la misma queda bajo la completa administración del Ministerio de Salud y se somete a las leyes chilenas en caso de inconvenientes. Esto es particularmente difícil de verificar ya que, como se mencionó anteriormente, Chile no cuenta con normas específicas que regulen la transferencia internacional de datos y al no contar con una autoridad que vele por la aplicación de la ley el

control y posibles denuncias ante incumplimientos o vulneración de principios y/o derechos no se encuentran fácilmente disponibles de lograr.

En cuanto al **principio de seguridad,** se detalló anteriormente que la ley chilena N° 19.628 no incorpora garantías relativas a la seguridad, es decir, no incorpora mecanismos de seguridad técnicos, administrativos, físicos o legales, sino que únicamente establece en su artículo 23° que el titular de los datos podrá ser indemnizado por el tratamiento indebido de sus datos personales. Sin embargo, en los términos y condiciones de la aplicación chilena se explicita que "la seguridad de CoronApp ha sido verificada mediante un análisis de vulnerabilidades (...). Toda la comunicación entre servidor y aplicaciones ocurre en canales de comunicación cifrados" (Términos y condiciones CoronApp, 2020) y se añade que la Subsecretaría de Redes Asistenciales ha adoptado todas las medidas necesarias para garantizar la confidencialidad y la protección de los datos personales recabados, pero en ningún lugar se especifica quien se encarga de supervisar que tales medidas se hayan tomado y cómo podrá el titular de los datos acceder y/o reportar un uso indebido de los mismos.

Pasando a observar estos dos principios en los términos y condiciones de la aplicación Cuidar, en relación al de **responsabilidad,** queda establecido en la sección 5.4 que el responsable de la base de datos es la Subsecretaría de Gobierno Abierto y se garantiza que la misma se compromete a adoptar todas las medidas necesarias para la seguridad de los datos personales de los usuarios para prevenir procesamientos ilegítimos. Al igual que en el caso de CoronApp, se establecen limitaciones a la responsabilidad en tanto que la Secretaría no se responsabiliza por el mal uso de la aplicación, ni por su mal funcionamiento, pérdida de información o interrupciones de los proveedores de servicios.

En cuanto al **principio de seguridad**, la ley argentina N° 25.326 en su artículo 9 indica que el responsable del banco o archivos de datos deberá tomar medidas técnicas que garanticen la seguridad y confidencialidad de los datos personales. En este sentido, en la sección 5.8 de los términos y condiciones de Cuidar se declara:

> La Secretaría se compromete a adoptar todos los recaudos que sean necesarios para garantizar la seguridad de los datos personales del Usuario, inclusive la prevención de procesamientos no autorizados o ilegítimos, pérdida accidental, destrucción o daños a dichos datos personales. Asimismo, la Secretaría se compromete a adoptar todas las medidas que sean necesarias para garantizar que toda persona que tenga acceso a los datos personales del Usuario les dé el tratamiento detallado en esta cláusula (p.7).

Se observa así que los términos incorporan lo indicado en la ley al establecer que la Secretaría tomará las medidas técnicas necesarias para asegurar la protección en el tratamiento que este organismo realice y además garantizará que los terceros que accedan cumplan con lo estipulado en el documento.

Otra distinción fundamental relativa a la **seguridad** de los datos personales, es que en Argentina con la reglamentación de la ley de Protección de Datos Personales se estableció la creación de un órgano de control "el cual deberá realizar todas las acciones necesarias para el cumplimiento de los objetivos y demás disposiciones de la presente ley" (Ley N° 25.326).

La autoridad se encuentra incluida en la sección 5.7 de los términos y condiciones de la aplicación Cuidar, indicando que el usuario de la aplicación podrá acudir a dicha autoridad en caso de considerar que se ha incumplido con algún principio y/o derecho garantizado en la ley.

Por su parte, la legislación chilena no incorpora la creación de un órgano de control pero en el 2008 se sancionó la ley N° 20.285 de Acceso a la Información Pública con la que se crea el Consejo para la Transparencia que según informa en su portal web tiene como principal objetivo velar por el cumplimento de dicha ley y a su vez dentro de sus facultades se incluye la realización de recomendaciones a organismos estatales y públicos relativas a la protección de datos personales.

En los términos y condiciones no se hace referencia al Consejo y, si bien se declara que el Ministerio de Salud es el responsable de la administración de la base de datos y el mismo cuenta con facultades para tratar los datos relacionados a la materia de su competencia, el problema surge en cuanto a que los datos de geolocalización solicitados y otros que sin especificar se obtendrían del teléfono móvil del usuario, exceden al ámbito del Ministerio de Salud.

En conclusión se observa que si bien ambos principios aquí analizados se encuentran contenidos en ambas aplicaciones existe una diferencia fundamental que es la relativa a la autoridad de control. Si bien CoronApp establece medidas de seguridad como la anonimización de los datos de los titulares, tiempo de conservación y algunas exigencias ante la cesión de datos a terceros, esto se vuelve muy difícil de verificar y controlar al no contar, ni designar un órgano de control específico que se encargue de velar por el cumplimiento de los establecido en estos términos y condiciones. A tal sentido, la Declaración conjunta de la sociedad civil (2020) indica en su punto 7 “Toda respuesta debe incorporar mecanismos de rendición de cuentas y salvaguardias contra el uso indebido”, es decir que además de expresar las garantías de protección, tienen que brindar formas claras para que los titulares de los datos

puedan verificar acceder a la información y reclamar en caso de un tratamiento o uso indebido.

Cuadro comparativo: Principios incluidos en los términos y condiciones de las aplicaciones Cuidar y CoronApp.

Principios / Aplicaciones	**Cuidar (Argentina)**	**CoronApp (Chile)**
Consentimiento	El Usuario manifiesta haber leído y aceptado en su totalidad los Términos y Condiciones; dicha aceptación es indispensable para la utilización de la Aplicación. En caso de no estar de acuerdo con los Términos y Condiciones se ruega no utilizar la aplicación.	El Usuario declara haber leído y aceptado los términos y condiciones. En caso de no estar de acuerdo con estos, el usuario deberá abstenerse de utilizar los servicios que proporciona la aplicación. Incumple con el principio de consentimiento informado al establecer que con el objetivo de mejorar el servicio la aplicación podrá recolectar "cierta información" del teléfono del usuario, sin brindar mayores especificaciones al respecto.
Finalidad	Finalidades declaradas: Brindar información con la finalidad de ayudar a prevenir la propagación del virus; dar intervención a las autoridades sanitarias o permitir el desarrollo de políticas públicas para la prevención y mitigación de la propagación de la enfermedad. Los datos personales previamente anonimizados se podrán utilizar para fines científicos o epidemiológicos.	Finalidades declaradas: Brindar información y monitoreo de síntomas; "Ayuda vecina"; "Reportar aglomeraciones"; "Conectar con la Comisaría Virtual". Se utilizarán "ciertos datos" del teléfono del usuario para realizar mejoras en la aplicación, las cuales no detalla. Los datos personales previamente anonimizados podrán usarse para fines científicos, históricos o de investigación.
Exactitud	El titular de los datos debe garantizar que todos los datos suministrados en el	El usuario se compromete a mantener la información en su cuenta de forma

	proceso de registro son verdaderos, completos y actualizados.	veraz, exacta completa y actualizada.
Minimización	Incorpora el principio al solicitar solo los datos necesarios y pertinentes para los fines previstos. Se observa como punto problemático la solicitud del número de DNI con el Número de Trámite, debido a que su posible filtración o divulgación puede causar graves daños a la privacidad del titular.	No incorpora este principio y esto se observa al indicar que se podrá recolectar "cierta información" del teléfono del usuario.
Limitación de conservación	Los datos sensibles y de geolocalización se preservarán únicamente mientras sean necesarios y dure la emergencia sanitaria.	Los datos serán almacenados y tratados durante el tiempo que dure la alerta sanitaria.
Transferencia internacional y cesión	La Subsecretaría podrá ceder información únicamente a otras **entidades estatales y/o establecimientos sanitarios nacionales, provinciales o municipales**, para que estos puedan contener y/o mitigar la propagación del virus COVID-19, ayudar a prevenir la sobreocupación del sistema sanitario argentino.	Los datos recolectados serán accedidos tanto por el Ministerio de Salud, como por otras entidades establecidas por ley y el MINSAL podrá ser requerido a entregar acceso o divulgar los datos a terceros, en virtud de una orden judicial, esto es por los tribunales de justicia, o administrativa, en el caso de sumarios sanitarios. Los datos recolectados se almacenan en una base de datos de Amazon Web Services ubicada en Virginia, Estados Unidos. Se indica que la misma se somete a la legislación y normas de Chile, aunque el país no cuenta con una norma específica que regule la transferencia internacional de datos.
Responsabilidad	Subsecretaría de Gobierno Abierto y País Digital de la Secretaría de Innovación Pública de la Jefatura de Gabinete de Ministros de la Nación.	Ministerio de Salud (MINSAL) a través de la Subsecretaría de Redes Asistenciales.
Seguridad - Autoridad de	La Secretaría se compromete a adoptar todos los recaudos que sean necesarios	La seguridad de CoronApp ha sido verificada mediante un análisis de

aplicación	para garantizar la seguridad de los datos personales del usuario, inclusive la prevención de procesamientos no autorizados o ilegítimos, pérdida accidental, destrucción o daños a dichos datos personales. Asimismo, la Secretaría se compromete a adoptar todas las medidas que sean necesarias para garantizar que toda persona que tenga acceso a los datos personales del usuario les dé el tratamiento detallado en los términos. El usuario podrá acudir a la Agencia de Acceso a la Información Pública, autoridad de control de la Ley de Protección de Datos Personales ante algún posible incumplimiento o vulneración de derecho.	vulnerabilidades. Toda la comunicación entre servidor y aplicaciones ocurre en canales de comunicación cifrados. Se establece que la Subsecretaría de Redes Asistenciales ha adoptado todas las medidas necesarias para garantizar la confidencialidad y la protección de los datos personales recabados pero no se detalla quién o qué organismo se encarga de supervisar que tales medidas se cumplan o donde podrán los usuarios reportar un uso indebido.

Fuente: Elaboración propia.

5.5 Tensiones

A partir de haber observado comparativamente cómo se incluyen los principios de protección de datos personales seleccionados en los términos y condiciones de las aplicaciones Cuidar y CoronApp, en este apartado se procede a dar cuenta de las tensiones que se han advertido en la comparación.

En primer lugar, una de las tensiones más relevantes que motivó la investigación y se observó a la largo de la tesina, es la relativa al equilibrio de derechos entre la protección de salud pública, la protección de la privacidad y los datos personales, y libertad de expresión. Así quedó expresado en la introducción de la Declaración conjunta de la sociedad civil (2020):

> La tecnología puede y debe desempeñar importantes funciones durante este esfuerzo que se está realizando para salvar vidas, como difundir mensajes de salud pública y

> aumentar el acceso a los servicios de salud. No obstante, el aumento de los poderes de vigilancia digital de los Estados –como tener acceso a los datos de localización de los teléfonos móviles– amenaza la privacidad, la libertad de expresión y la libertad de asociación de una manera que podría violar derechos y reducir la confianza en las autoridades, con el consiguiente menoscabo de la eficacia de las repuestas de salud pública.

Es decir, la tecnología puede ser de gran ayuda en contextos de emergencias extremas como estos pero que no vulneren otros derechos humanos fundamentales dependerá de que los Estados en su desarrollo decidan asegurar que eso no suceda. Frente a una emergencia como la pandemia quedó demostrado una vez más aquello que expresó Castells (2006) en cuanto a que los Estados tienen un rol central impulsando y dirigiendo la innovación tecnológica. A su vez, es necesario que sean los Estados los que desarrollen estas tecnologías bajo el respeto por los derechos humanos, evitando que estas herramientas se conviertan en instrumentos de vigilancia y control, marcadas únicamente por la necesidad de seguir ahondando en la extracción del excedente conductual, en donde los servicios ofrecidos sirven únicamente como excusa para seguir profundizando en la obtención de datos de los usuarios dentro de un ciclo más amplio de generación de ingresos (Zuboff, 2020). En relación a esto, Natalia Zuazo indicaba en la entrevista realizada para este trabajo que "La pandemia en muchos sentidos dejó a la vista como los derechos humanos en el ámbito digital tienen absolutamente que ver con la realidad de las personas" (Entrevistas a Zuazo, 2021); en el sentido de que se puso en evidencia que no era menor que los países cuenten con una actualizada legislación sobre protección de datos personales ante la necesidad de recolectar datos para brindar información y generar políticas públicas que respondan a la emergencia. De hecho, durante todo el

apartado donde se analizó cómo se incluyen los principios se evidenció que estos se cumplen en los términos y condiciones, de forma muy similar a como aparecen expresados en las leyes vigentes. Hecho que demuestra que no es menor contar con normativas actualizadas y robustas de protección de datos personales que permitan el desarrollo de herramientas tecnológicas que respeten los derechos humanos.

Específicamente en los términos y condiciones de Cuidar y CoronApp se observaron algunas tensiones a tener en cuenta. Para empezar, en CoronApp de Chile, algunas de las funciones problemáticas en relación a la protección de la privacidad eran las de "Ayuda vecina", "Reportar aglomeraciones", "Denuncias por incumplimiento de cuarenta" y declaraciones del lugar donde se pasaría el aislamiento en caso de ser confirmado como caso positivo. Todas estas funciones requerían que el usuario otorgue acceso a su geolocalización y "una fotografía para identificarlo entre los vecinos cuando solicita y entrega ayuda" (Términos y condiciones CoronApp, 2020). Frente a esto se consultó con la entrevistada Michelle Bordachar quien expresó lo siguiente:

> Esta app solicitaba acceso a geolocalización y eso es muy delicado porque suceden situaciones como que aparte de mi nadie va y viene de mi casa a mi trabajo, ni hace el mismo recorrido, entonces es súper fácil cruzar esa información y saber a quién pertenece. Lo que pasó con esa tecnología es que no se piensa en el contexto político de Chile en donde estábamos justo con el estallido social en un contexto de protesta y entonces qué libertad de ejercicio de protesta o sindical uno puede tener. Si este tipo de aplicaciones no viene con una perspectiva de derechos humanos significan una restricción y una amenaza para un montón de otros derechos (Entrevista a Bordachar, 2021).

Se observa así que incluir ciertas funciones que promuevan la vigilancia sin tener en cuenta el contexto, o lo que es peor, teniéndolo en cuenta pero así y todo decidir incluirlas igual, puede causar más daño a la privacidad de las personas que un beneficio a la protección de su salud. De hecho esta dicotomía que se planteó en torno a la protección de datos personales versus la protección de la salud pública quedó expresada por ambas entrevistadas y por la Declaración conjunta de la sociedad civil (2020) como falsa; Michelle Bordachar declaró al respecto:

> De partida el derecho a la privacidad no es absoluto (...) Esto no significa que nadie nunca pueda acceder a nuestros datos, sino que esto tiene que hacerse conforme a la ley. La crítica no era el acceso a los datos, sino a qué datos y bajo qué condiciones (Entrevista a Bordachar, 2021).

Entonces, los Estados no tenían que elegir entre proteger uno u otro derecho, sino más bien tomar decisiones para lograr alcanzar un equilibrio y asegurar que toda limitación, tal como lo indica el test tripartito desarrollado por la Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos (CIDH), sea necesaria, pertinente y legítima.

Por otro lado, otras de las tensiones que se identificó es la referida a la autoridad de aplicación o fiscalizadora de lo establecido en los términos y condiciones. En lo que respecta a la aplicación Cuidar de Argentina, esto quedó claramente expresado al indicar que el responsable de la base de datos es la Subsecretaría de Gobierno Abierto y País Digital de la Secretaría de Innovación Pública de la Jefatura de Gabinete de Ministros de la Nación, y al incluir que el usuario podrá acudir a la Agencia de Acceso a la Información Pública, autoridad de control de la ley de Protección de Datos Personales, si considera que se ha incumplido algún principio y/o derecho. Esto permite que todas las medidas de seguridad

incorporadas en la aplicación como la anonimización de los datos de geolocalización o la eliminación de los datos sensibles una vez finalizada la emergencia sanitaria, puedan ser controladas por un órgano competente que asegure que efectivamente eso se cumplirá. Sin embargo, hay algunos vacíos en los términos y condiciones de la aplicación en cuanto a que no especifica qué pasará con los datos personales que no son sensibles una vez finalizada la emergencia sanitaria.

En la Declaración conjunta de la sociedad civil (2020) en su punto 4 se indica que "cuando se afirme que los datos son anónimos, ha de poder demostrarse y respaldarse con información suficiente sobre cómo se han anonimizado" y si bien esto no se encuentra detallado en los términos y condiciones de Cuidar, al contar con una autoridad responsable, los titulares de los datos pueden exigir a la misma que rinda cuentas al respecto.

En lo que respecta a CoronApp, como se indicó anteriormente, en todos los casos en los que en los términos y condiciones se desarrolla una medida de protección, como que los datos serán anonimizados para que terceros puedan acceder con fines históricos y/científicos, no se indica cómo se hará, ni se detallan mecanismos externos que permitan comprobarlo. Esto se dificulta aún más al no contar con una autoridad de aplicación específica de la ley sobre Protección de la Vida Privada. Viollier (2017) explica que:

> La ausencia de dicha autoridad de control implica que los individuos afectados deben recurrir ante los tribunales ordinarios de justicia, sea a través de la acción constitucional de protección (...) Los costos asociados a la tramitación judicial, sumado al relativo desconocimiento que sufren los individuos del tratamiento que terceras personas realizan de sus datos personales, hacen que la carencia de una autoridad de control afecte directamente la aplicabilidad de la Ley 19.628 para los ciudadanos comunes (p.26-27).

Se advierte así que además de desarrollar e incluir salvaguardas al tratamiento de los datos personales y sensibles es necesario implementar o crear una autoridad externa que permita asegurar que todo lo indicado se aplica en la práctica.

Para concluir, la última tensión que se observa es la relativa a la complejidad a la que se enfrentaron los Estados para poder recolectar y almacenar la cantidad de datos solicitados. Como se precisó, los casos aquí analizados fueron desarrollados mediante la articulación del Estado con el sector público, científico y privado. En ambos casos tuvo participación Amazon Web Services pero con la particularidad de que en la aplicación chilena se indicaba que los datos eran almacenados en una nube bajo total administración de dicha plataforma en Estados Unidos. Se consultó al respecto a la especialista en tecnología, Natalia Zuazo quien expresó:

> Por supuesto que siempre es mejor tener infraestructura propia para almacenar pero a veces cuando estás desarrollando tecnología en el momento no tenés esa infraestructura disponible (...) la infraestructura tiene que ser una misión a largo plazo de los Estados porque nunca sabes cuando la vas a necesitar (Entrevista a Zuazo, 2021).

Retomando a Srnicek (2018) para comprender esto se advierte que estas plataformas nube permiten la terciarización de gran parte de procesos y ahorrar en grandes inversiones relativas a desarrollos tecnológicos e infraestructuras, esto a su vez es altamente beneficioso para estas empresas ya que este modelo de alquiler "le permite recolectar datos constantemente (...) Empresas como Amazon ganan acceso directo a nuevos conjuntos de datos completos" (p.62). Esto se convierte así en un reto para la soberanía digital de los Estados, en el sentido

de que los mismos deberían poder planificar a largo plazo para poder desarrollar herramientas tecnológicas que no dependan de estas plataformas.

6. Conclusiones

El objetivo de esta tesina consistió en analizar desde un estudio comparativo los términos y condiciones de las aplicaciones Cuidar y CoronApp, a fin de conocer en qué medida incorporan los principios de protección de datos personales de: consentimiento, finalidad, exactitud, minimización, limitación a la conservación, transferencia internacional, cesión, responsabilidad y seguridad. Para ello se inició observando si los mismos se encuentran incorporados y cómo en las leyes vigentes en ambos países, para así poder avanzar en el análisis comparado de los términos y condiciones e identificar las tensiones que emergieron en la comparación.

En un principio se observó que si bien ambas legislaciones datan de años de promulgación similares (1999 y 2000), la legislación vigente en Argentina sobre protección de datos personales tiene incorporados más principios de protección de datos personales que la legislación chilena. Entre sus diferencias sustanciales se encuentra el hecho de que Argentina con la sanción de la ley N° 25.326 fijó la creación de un órgano de control descentralizado, el cual debe velar por la adecuada protección, monitoreando el cumplimiento de las normas previstas y garantizando que los titulares de los datos puedan ejercer sus derechos. En tanto que Chile no cuenta con una autoridad de control y si bien reconoce estándares internacionales de protección, su ley se muestra más ineficiente que la argentina para garantizar una correcta protección de datos personales.

A su vez, se advirtió que los términos y condiciones de ambas aplicaciones incorporan los principios establecidos en las leyes de protección de datos personales vigentes, al mismo tiempo que reflejan los vacíos presentes en las mismas. De los principios de protección de datos personales seleccionados se vio que en la ley argentina N° 25.326 se encuentran todos

incluidos pero no así en la ley chilena N° 19.628, la cual no incluye los de minimización, transferencia internacional de datos, seguridad y limitación a la conservación. Esto mismo se encuentra en los términos y condiciones de CoronApp donde si bien se observan algunos puntos relativos a estos principios, asegurar el cumplimiento de los mismos se dificulta enormemente al no contar con una autoridad de aplicación que lo garantice. Por ejemplo, el caso en el que se indica en que los datos serán almacenados durante el tiempo que dure la alerta sanitaria pero no se indica cómo y ante qué autoridad los titulares de los datos podrán corroborar que se cumpla con ello.

Michelle Bordachar (2021), entrevistada para este trabajo, afirmó que la legislación vigente en Chile no garantiza una adecuada protección de datos personales y que, por lo tanto, la aplicación CoronApp tampoco lo hace. Mientras que la entrevistada argentina Natalia Zuazo (2021), consultora política y especialista en tecnología, afirmó que Argentina sí cuenta con una buena ley de Protección de Datos Personales y que la aplicación Cuidar cumple correctamente con la misma. También agregó que para el desarrollo de los términos y condiciones se tuvieron en cuenta diversas recomendaciones de distintas organizaciones de la sociedad civil, las cuales retomaron principios de protección que deben incluir estas aplicaciones para el respeto de los derechos humanos.

De todas formas, existen consensos entre las y los especialistas sobre la desactualización de los marcos regulatorios de ambos países, sobre todo de la falta de especificidad sobre las medidas de seguridad necesarias a adoptar para una correcta protección, de las ambigüedades y vacíos que presentan, y de la falta de controles eficientes a los organismos y empresas que gestionan datos personales. Esto hace, en el caso de Chile, que la seguridad de los datos

personales quede en manos de empresas o del organismo estatal que los gestiona, sin otro responsable que garantice su seguridad.

En este sentido, la principal conclusión a la que se ha llegado con este estudio comparativo es que los términos y condiciones de la aplicación Cuidar son más robustos con respecto a las garantías de protección que brindan, en comparación a lo que sucede con los de CoronApp, situación que coincide con que la ley argentina incorpora mayor cantidad de principios de protección que los que incluye la ley chilena.

Por otro lado, en lo que respecta a si los datos personales recolectados y almacenados por estas aplicaciones son adecuados, relevantes y pertinentes a las finalidades declaradas en cada caso, se concluye que en los términos y condiciones de la aplicación CoronApp se encuentran mayores ambigüedades al respecto. En particular el punto 2 donde indica que "puede resultar necesario recopilar y procesar cierta información, la cual se obtendrá del dispositivo móvil en donde se ha instalado la aplicación", con el fin de realizar mejoras en la aplicación. Es decir, no se especifica ni cuáles serán esos datos a tratar ni a qué mejoras o actualizaciones refiere. En cuanto a la aplicación Cuidar, con respecto a todos los datos que recolecta se observó como excesiva la solicitud de ingresar el número de DNI y el Número de Trámite, debido a que su posible divulgación pueden provocar graves daños a la privacidad del titular.

Asimismo otra de las tensiones observadas en el caso de CoronApp de Chile fue la relativa a que la misma incluía funciones de denuncias por aglomeraciones e incumplimiento de cuarentena mediante rastreo por geolocalización, en un contexto en el que el país se encontraba a pocos meses de haber vivido la marcha más grande de su historia. La misma se conoció como *revuelta social* o el *estallido de octubre* y fue llevada a cabo el 18 de octubre de 2019. Dicha protesta, tuvo como tema central la gran desigualdad y la precarización de las

clases medias y medias-bajas que existe en Chile, y el pedido de reformar la Constitución Nacional impuesta en 1980 durante la dictadura de Augusto Pinochet. Incluir estas funcionalidades de denuncia y control entre ciudadanos, en dicho contexto no hizo más que aumentar la desconfianza y el descontento de la población frente a una herramienta que se presentaba como necesaria y útil en el contexto de la emergencia sanitaria. Así, la dicotomía planteada en torno a la protección de la privacidad y los datos personales vs. la protección de la salud pública, se evidenció como falsa, tal como expresaron las entrevistadas para la tesina y la Declaración conjunta de las organizaciones de la sociedad civil; en el sentido de que si bien los Estados debían priorizar la protección de la salud pública, desarrollar herramientas que promuevan la vigilancia y control social del Estado a los ciudadanos, y de los ciudadanos entre sí, no hace más que profundizar los daños e incurrir en la vulneración de otros derechos.

En un contexto donde, según Castells (1995), el modo de desarrollo está orientado "hacia la acumulación de conocimiento", y el nuevo modelo de negocio de las plataformas se basa en la información y gestión de los datos (Srnicek, 2018), los grises pero también los aciertos en las normativas vigentes sobre protección de los datos personales demuestran la necesidad de actualización y desarrollo de marcos regulatorios fuertes para que las tecnologías destinadas a servir al bien común estén basadas en el respeto a los derechos humanos. Tal como se indica en la Declaración conjunta de la sociedad civil (2020), el cumplimiento de los estándares internacionales y la incorporación de la mayor cantidad de principios de protección de datos personales, permite a la población confiar la entrega de sus datos personales a las autoridades sanitarias y que las mismas puedan trabajar y colaborar en diseñar y planificar las políticas públicas necesarias para afrontar esta y futuras emergencias.

A partir de lo analizado, se evidencia que no es menor contar con normativas más fuertes y abarcativas al momento de llevar a cabo el desarrollo de herramientas tecnológicas que ayuden a gestionar situaciones de emergencia como la pandemia y protejan, al mismo tiempo, los derechos de los usuarios. Por supuesto que la emergencia sanitaria conlleva que los Estados y gobiernos prioricen la protección de la salud pública y establezcan algunas limitaciones en cuanto a la protección de la privacidad y libertad de expresión, pero esto siempre se debe realizar mediante el establecimiento de medidas que sean lo menos dañinas posibles y garantizando que las mismas sean legales, pertinentes y necesarias, a fin de no incurrir en prácticas de vigilancia o control social que puedan causar mayores daños que los que ya estaba enfrentando la sociedad con la pandemia.

A su vez, se muestra como favorable la celeridad en la respuesta y preparaciones de ambos países a nivel digital. Sin embargo, en la comparación se destaca la experiencia argentina por sobre la chilena en cuanto a la constitución de una base de datos propia, por la existencia de normativas e instituciones más fuertes de protección de datos y por el trabajo de articulación entre diferentes actores para lograr que la herramienta contemple la mayor cantidad de medidas de protección. Sin embargo, se deberán tener en cuenta los progresos de ambas herramientas en cuanto a las posibles nuevas funcionalidades que mencionan a fin incorporar evaluaciones de impacto en tales desarrollos y que asegurar que los titulares cuenten con la información correspondiente.

7. Bibliografía

Aguerre, C (2020). La delgada y móvil frontera de las corona-apps en América Latina en Análisis Carolina. Recuperado de https://www.fundacioncarolina.es/la-delgada-y-movil-frontera-de-las-corona-apps-en-america-latina/

Argentina se suma al Convenio 108+. (2019, 20 de febrero). Agencia de Acceso a la Información Pública. Recuperado de https://www.argentina.gob.ar/noticias/argentina-se-suma-al-convenio-108#:~:text=Argentina%20es%20Estado%20parte%20del,firmar%20el%20Convenio%20108%20modernizado

Argentina, Estado Parte del Convenio 108 (28 de febrero, 2019). Portal Oficial del Estado Argentino. https://www.argentina.gob.ar/noticias/argentina-estado-parte-del-convenio-108#:~:text=Nuestro%20pa%C3%ADs%20se%20convirti%C3%B3%20en,personal%20y%20su%20Protocolo%20Adicional

Castells, M. (1995). *La ciudad informacional: tecnologías de la información, reestructuración económica y el proceso urbano regional*. Alianza Editorial.

Castells, M. (2006). *La era de la información*. Edición de Hipersociología.

Cerda Silva A. (2012). Protección de datos personales y prestación de servicios en línea en América Latina. En E. Bertoni (ed.), *Hacia una internet libre de censura* (pp. 165-180). Universidad de Palermo.

Chocarro, S. (2017). Estándares internacionales de libertad de expresión: Guía básica para operadores de justicia de América Latina. Recuperado de https://www.corteidh.or.cr/tablas/r37048.pdf

Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (N° 108). (1981). Consejo de Europa. Recuperado de https://rm.coe.int/16806c1abd

Cuarenta y dos países adoptan los Principios de la OCDE sobre Inteligencia Artificial. (2019, 22 de mayo). OCDE Centro de México. Recuperado de https://www.oecd.org/centrodemexico/medios/cuarentaydospaisesadoptanlosprincipiosdelaocdesobreinteligenciaartificial.htm

Declaración conjunta de la sociedad civil. (2020, 2 de abril). Los Estados deben respetar los derechos humanos al emplear tecnologías de vigilancia estatal para combatir la pandemia. Recuperado de https://www.hrw.org/es/news/2020/04/02/declaracion-conjunta-de-la-sociedad-civil-los-estados-deben-respetar-los-derechos

Deleuze, G. (1995) “Post-scriptum sobre las sociedades de control”, en *Conversaciones*. Editorial Pre-Textos. Recuperado de http://www.oei.org.ar/edumedia/pdfs/T10_Docu1_Conversaciones_Deleuze.pdf

El Gobierno relanzar CUIDAR, la nueva versión de la app coronavirus argentina. (2020, 27 de abril). Secretaría de Innovación Pública. Recuperado de

https://www.argentina.gob.ar/noticias/el-gobierno-relanza-cuidar-la-nueva-version-de-la-app-coronavirus-argentina

El uso de las aplicaciones para contener el avance del Coronavirus en China, Corea y Singapur. (2020, 9 de abril). Observatorio Parlamentario. Biblioteca del Congreso Nacional de Chile. Recuperado de https://www.bcn.cl/observatorio/asiapacifico/noticias/vigilancia-sanitaria-coronavirus-china-corea-singapur

Elecciones 2019: Los resultados de las elecciones en todo el país. (2019, 18 de diciembre) *Diario Clarín*. Recuperado en https://www.clarin.com/politica/resultados-elecciones-2019-quien-gano-argentina_0_fAmHiiJe.html

Foucault, Michel. (1975). *Vigilar y castigar*. Editorial Siglo veintiuno.

Gauna, Celeste. (2020). En caso de emergencia: descargue un app - Parte II. *Asociación por los Derechos Civiles.* Recuperado en https://adc.org.ar/2020/12/22/en-caso-de-emergencia-descargue-una-app-parte-ii/

Guía Legislativa sobre la Privacidad y la Protección de Datos Personales. (2015). Organización de los Estados Americanos. Recuperado de https://www.oas.org/es/sla/ddi/docs/proteccion_datos_personales_Guia_Legilsativa_CJI.pdf

Hacia una nueva Ley de Protección de Datos Personales. (2022). Agencia de Acceso a la Información Pública. Recuperado en

https://www.argentina.gob.ar/sites/default/files/hacia_una_nueva_ley_de_proteccion_de_datos_personales.pdf

Heiss, C. (2020). Chile, entre el estallido y la pandemia. Análisis Carolina. Fundación Carolina. https://www.fundacioncarolina.es/wp-content/uploads/2020/04/AC-18.2020.pdf

Nájera, J., y Ricaurte, P. (2020). Tecnologías de interés públicos: el caso de las coronapps en América Latina. Recuperado de https://centrolatam.digital/wp-content/uploads/2021/04/Policy-report_Tecnologi%CC%81as-de-intere%CC%81s-pu%CC%81blico-el-caso-de-las-coronaapps-en-Ame%CC%81rica-Latina.pdf

Molina Quiroga, E. (2003). Protección de datos personales como derecho autónomo. Principios rectores. Informes de solvencia crediticia. Uso arbitrario. Daño moral y material. Recuperado de http://www.saij.gob.ar/eduardo-molina-quiroga-proteccion-datos-personales-como-derecho-autonomo-principios-rectores-informes-solvencia-crediticia-uso-arbitrario-dano-moral-material-dacc030027-2003/123456789-0abc-defg7200-30ccanirtcod

O'Donnell, G. (1977). Apuntes para una Teoría del Estado. Centro de estudios de Estado y Sociedad (CEDES).

Oszlak, O. y O´Donnell, G. (1984). Estado y políticas estatales en América Latina: hacia una estrategia de investigación. En Flores, G. & Nef, J. (eds.). *Administración pública: perspectivas críticas*. Instituto Centroamericano de Administración Pública (ICAP).

Pacto Internacional de Deberes Civiles y Políticos. (1966). Secretaría de Derechos Humanos y Pluralismo Cultural. 21. Recuperado de https://www.argentina.gob.ar/sites/default/files/derechoshumanos_publicaciones_coleccciondebolsillo_06_derechos_civiles_politicos.pdf

Resultado de las elecciones. (2017) *Diario Emol*. Recuperado de https://www.emol.com/especiales/2017/actualidad/nacional/elecciones/resultados.asp#v19001

Resultados definitivos Elecciones Presidencial, Parlamentarias y de Core 2017. (2017). Servicio Electoral de Chile. Recuperado de https://www.servel.cl/resultados-definitivos-elecciones-presidencial-parlamentaria-cores-2017/

Sautu, R. (2003). El diseño de una investigación: teoría, objetivos y métodos. *Todo es teoría*. Objetivos y métodos de investigación (pp. 21-51). Lumiere.

Singapur lanzará a nivel mundial una aplicación contra la propagación del COVID-19. (2020, 8 de marzo). *Wild Entrepreneur*. Recuperado de https://wildentrepreneur.org/singapur-lanzara-a-nivel-mundial-una-aplicacion-contra-la-propagacion-del-covid-19/

Sistema y aplicación Cuidar. (2020). Secretaría de Innovación Pública. Recuperado de https://www.argentina.gob.ar/jefatura/innovacion-publica/acciones-realizadas-en-el-marco-del-coronavirus-covid-19/sistema-y#:~:text=Como%20parte%20integral%20de%20las,Decisi%C3%B3n%20Administrativa%20432%2F2020

Srnicek, N. (2018). *Capitalismo de Plataformas*. Editorial Caja Negra.

Villegas Carrasquilla, L. (2012). Protección de datos personales en América Latina: retención y tratamiento de datos personales en el mundo de Internet. En E. Bertoni (ed.), *Hacia una internet libre de censura* (pp. 125-164). Universidad de Palermo

Viollier, P. (2017). El estado de la Protección de Datos Personales en Chile. Recuperado de https://www.derechosdigitales.org/wp-content/uploads/PVB-datos-int.pdf

Zuboff, S. (2020). *La era del capitalismo de la vigilancia*. Editorial Paidós.

7.1 Legislación

Decreto N° 104. Diario Oficial de la República de Chile. Santiago, Chile. 18 de marzo de 2020.

Decreto N° 867. Boletín Oficial de la República Argentina. Buenos Aires, Argentina. 23 de diciembre de 2021.

Decreto N°1.558. Boletín Oficial de la República Argentina. Buenos Aires, Argentina. 29 de noviembre de 2001.

Decreto N°297. Boletín Oficial de la República Argentina. Buenos Aires, Argentina. 19 de marzo de 2020.

Disposición N° 3. Boletín Oficial de la República Argentina. Buenos Aires, Argentina. 5 de mayo de 2020.

Ley N° 21.096. Diario Oficial de la República de Chile. Santiago, Chile. 16 de junio de 2018.

Ley N°25.326. Boletín Oficial de la República Argentina. Buenos Aires, Argentina. 2 de noviembre de 2020.

N° 19.628 sobre Protección de la Vida Privada. Diario Oficial de la República de Chile. Santiago, Chile. 28 de agosto de 1999.

Resolución N° 1339. Diario Oficial de la República de Chile. 15 de septiembre de 2022.

Términos y condiciones CoronApp. (2020). Ministerio de Salud de Chile. Recuperado de https://web.archive.org/web/20220331022515/https://coronapp.gob.cl/terminos.html

Términos y condiciones Cuidar. (2020). Jefatura de Gabinete de Ministerios. Recuperado de https://www.argentina.gob.ar/sites/default/files/terminos_y_condiciones_aplicacion_cuidar_-_covid_19_-_v5.pdf

8. Anexos

8.1 Entrevista a Natalia Zuazo, consultora política y tecnología para Access Now, UNESCO y otros. Autora de Guerras de internet (2015) y Los dueños de internet (2018).

-¿Considerás que Argentina cuenta con la normativa necesaria para garantizar una adecuada protección de datos personales frente al despliegue de estas tecnologías digitales?

Si, yo creo que tenemos una buena ley de Protección de Datos Personales. En términos de estándares internacionales es una buena ley. Esto no quita que haya una necesidad desde hace algunos años de reforma de la ley en virtud de que se sancionó en el año 2000. Recién en ese año se estaban desplegando, por ejemplo, las infraestructuras de cables submarinos. Nuestro uso y despliegue de las tecnologías recién se estaba dando a nivel de infraestructuras; no existían plataformas, ni Facebook, ni Google. Todo el ecosistema Internet que tenemos hoy que es intensivamente demandante de datos personales, no existía; entonces por más que sea una ley buena necesita definitivamente una actualización. Y además en términos de estándares internacionales ha habido otros avances. Por ejemplo, nuestra ley es una ley que si queremos pensar de donde abreva está más en consonancia con la tradición europea, y Europa hace algunos años actualizó su Reglamento General de Protección de Datos (RGPD), en el año 2018, con algunas cuestiones bastante interesantes. No significa eso que nosotros tengamos que copiar todo lo que dice Europa pero según nuestra tradición hay cosas que

deberíamos volver a repasar. En conclusión, creo que tenemos una buena ley pero creo que tenemos que actualizarla.

-¿Creés que la pandemia evidenció la necesidad de actualizar la ley sobre protección de datos personales?

Si. Yo creo que lo que pasa también es otra cosa, hay una visión respecto de que la cuestión de los datos personales y en general muchos de los temas que tienen que ver con los derechos humanos en el ámbito digital, cuando hay otras cuestiones urgentes y otras crisis, sean de salud, económicas o más urgentes, estas cuestiones pueden quedar en un segundo plano. En un punto esto puede ser lógico, puede ser entendible pero si nos ponemos a pensar estas cuestiones nos afectan en lo cotidiano y tienen directamente que ver con la desigualdad económica y social del mundo. Una empresa que obtiene sus ganancias mediante la explotación de datos y lo hace no respetando los derechos de las personas porque un país no adecua su ley, por lo que no tienen límites en cuanto a protección de datos, y por lo tanto los dueños de esa empresa pueden obtener riquezas mediante esos datos, eso de una manera directa afecta a la desigualdad de un país. Esas operaciones que nos parecen un poco indirectas al pensamiento hace que no veamos la importancia de tener leyes actualizadas en este sentido. Los que asesoramos en estas cuestiones y presentamos proyectos, tenemos ahí una dificultad en lograr un entendimiento mayor de la importancia que tienen estas cosas. La pandemia en muchos sentidos dejó a la vista como los derechos humanos en el ámbito digital tienen absolutamente que ver con la realidad de las personas. Todo el despliegue de las mal llamadas Inteligencia Artificial, todo el despliegue que se hace con el reconocimiento facial, aplicaciones médicas con funciones desde turnos médicos, estudios, base de datos de

personas vacunadas; ante todo esto no es menor tener una ley de Protección de Datos Personales actualizada.

-¿Considerás que es necesario ceder en el derecho a la privacidad y protección de datos personales para un combate efectivo de la pandemia? En este sentido, ¿podríamos considerar excluyentes la protección a la salud pública y el derecho a la protección de nuestros datos?

Creo que no tenemos porqué quedarnos con esta opción de proteger una cosa u otra. Definitivamente no creo que tengamos que pensar así y tenemos que trabajar por eso. El Estado tiene que ponerse en un lugar de mediación que siempre es más difícil, más costoso, lleva más tiempo y trabajo. Tiene que probar que puede ser eficiente en resguardar esos intereses porque si después no hace lo que tiene que hacer, es decir, nosotros decimos "ok Estado, te cedo estos datos para que los cuides porque creemos más en vos que en el mercado para que hagas esto", pero después el Estado lo hace mal, entonces va a haber alguna razón para que eso no suceda. Igual no es que el Estado hace solo esto. El Estado puede hacerlo con sus propias capacidades estatales desarrollando sus propios softwares, sus propios servidores, su propia infraestructura o puede hacerlo con otras empresas. De hecho, gran parte de la aplicación Cuidar se hizo así, desde organismos estatales y con otros externos.

-Chile: ¿cuáles serían las consecuencias de almacenar datos en un banco de Amazon WS ubicado en Virginia, USA?

Esas decisiones son muy complejas. En principio no me parece lo mejor. No sé por qué se habrá tomado esa decisión pero el principio que debe aplicar siempre es de minimización de tiempo, el mínimo tiempo posible para los fines recomendados por el Ministerios de Salud y autoridades sanitarias. Tal vez tienen alguna razón sanitaria. Eso nos pasó a nosotros también. Había cosas que yo recomendaba no hacer pero después el Ministerio de Salud o CONICET nos decía que hay que hacerlo así porque el virus muta y no es tan sencillo. En cuanto al almacenamiento por supuesto que siempre es mejor tener infraestructura propia para almacenar pero a veces cuando estás desarrollando tecnología en el momento no tenés esa infraestructura disponible. Por eso, siempre la infraestructura tiene que ser una misión a largo plazo de los Estados porque nunca sabes cuando la vas a necesitar.

-Al inicio de la pandemia las organizaciones de la sociedad civil desarrollaron una serie de orientaciones para garantizar una efectiva protección de datos personales frente a las apps, ¿crees que los términos y condiciones de Cuidar/ConorApp se ajustan a estas?

Si, se tuvieron en cuenta. Se tuvieron en cuenta las de la Unión Estadounidense por las Libertades Civiles, las de Electronic Frontier Foundation, entre otras.

-¿Qué consecuencias puede tener la implementación de tecnologías digitales como estas sin lineamientos de derechos humanos?

Si ves las aplicaciones de las provincias hay una afectación muy grave de los estándares internacionales de derechos humanos. Hay aplicaciones que son muy inseguras y que están expuestos datos sensibles de las personas. Si se deja expuesta una base de datos de una persona que tuvo Covid y esa persona el día de mañana quiere conseguir un trabajo y el

empleador se fija en esa base de datos y elige no contratarlo se están afectando directamente sus derechos. Claramente cuando un desarrollo local o provincial no toma en cuenta las medidas de protección y seguridad adecuadas está exponiendo a su población a estas violaciones de derechos.

-La app de Chile tenía la opción de reportar aglomeraciones…

Eso es bastante peligroso porque tengamos en cuenta el proceso político de Chile. Puede gustarte o no el gobierno de turno del país pero por eso se llaman estándares internacionales de derechos humanos y por eso es importante respetarlos siempre para el desarrollo de tecnología. Porque de repente cambia el gobierno y viene uno que es peor, porque siempre puede haber algo peor, agarra esa app y la usa para detectar juntadas donde hay muchas personas haciendo algo y eso se usa para destrabar manifestaciones, juntadas o lo que sea. Puede ser leído como personas tomando algo en la esquina o conspiraciones políticas. Por eso también fue todo un tema decidir implementar apps con contact tracing porque son otros los riesgos.

-¿Cuáles son los puntos de los términos y condiciones que considerás conflictivos de la app?

Creo que fueron desarrollados bastante bien, sobre todo teniendo en cuenta el contexto. Considero que hubieron cosas que podrían haberse hecho mejor, sobre todo la parte del uso del número de trámite que me parece que eso es un problema que se sigue acarreando desde la app MiArgentina y en algún momento hay que rever.

8.2 Entrevista a Michelle Bordachar, abogada, especialista en ciberseguridad. Analista de políticas públicas en la organización Derechos Digitales e investigadora del Centro de Estudios en Derecho Informático en la Facultad de Derecho de la Universidad de Chile.

-¿Considerás que Chile cuenta con la normativa necesaria para garantizar una adecuada protección de datos personales frente al despliegue de estas tecnologías digitales?

La respuesta definitiva es no. No contamos con una ley de protección de datos personales necesaria. La ley que tenemos es de 1999, no fue pensada para la época en la que vivimos y en la vivíamos hace 10 años tampoco.

-¿Creés que la pandemia evidenció la necesidad de actualizar la ley sobre protección de datos personales?

Si, de todas maneras. Vino a poner en evidencia la cantidad de datos personales que implican las aplicaciones y en el fondo la cantidad de información que se puede dar a conocer mediante medios tecnológicos. Al mismo tiempo siento que no tenemos ley y el mundo sigue, entonces puede que el sentido de urgencia se haya quitado y las personas se terminan acostumbrando. De hecho nuestra ley de Protección de Datos Personales iba avanzando bastante bien, o sea llevábamos cuatro años tramitandola, pero en el último año la tramitación había sido bastante efectiva. En marzo de 2020, en plena pandemia cuando uno hubiera pensado que era cuando más se tenían que poner las pilas con el tema de los datos personales, se paralizó la discusión del proyecto de ley hasta ahora. Lo que se ve es que de repente se

digitalizó todo y seguimos sin protección de datos. Es decir, vino a evidenciar la necesidad pero también vino a quitarle la urgencia.

-En relación a esto y a que Chile actualmente no cuenta con una autoridad específica de Protección de Datos Personales, en este caso de la CoronApp ¿qué implica no contar con esto?

En eso se dio algo muy particular porque al principio la aplicación fue desarrollada por División de Gobierno Digital del Ministerio Secretaría General de la Presidencia de Chile (SEGPRES) y esa era la autoridad que estaba en las políticas y términos de la aplicación. Después cuando empezaron a haber quejas en contra de la aplicación se dieron cuenta de que la única base habilitante que podían tener si no era el consentimiento de las personas, era en base al código sanitario que le da facultades al Ministerio de Salud (MINSAL). Entonces ahí tuvieron que cambiar todo el discurso y decir que el responsable de la aplicación no era SEGPRES y Gobierno Digital, sino que era el Ministerio de Salud pero si uno le preguntaba a la gente del MINSAL acerca de las cláusulas que eran bien abusivas te decían que ellos no la habían hecho, que el responsable era la Secretaría General de la Presidencia. El tema es que si uno leía los términos y condiciones de partida no te pedían solo los datos que necesitaban sino que además podrían pedirte otros, la lista no era taxativa sino más bien abierta "vamos a pedirte datos tales como…" y en derecho cuando sale un "tales como" eso significa cualquier cosa. Es decir, de partida, no cumplía con el principio de la ley de que el consentimiento debe ser informado porque uno no estaba consintiendo con algo que uno estuviera informado porque no te informaban que datos exactamente iban a recabar. Después no tenía un límite de tiempo para tener los datos y había datos que no eran de salud, por lo que la defensa del

Ministerio de Salud era que ellos tienen derecho a tener datos de salud, lo cual es cierto pero todos los otros que no corresponden no tienen derecho a tenerlos a no ser que se especifique el plazo en el que van a conservar dichos datos. Después además uno autorizaba a entregar los datos a otras entidades, incluidas entidades privadas en donde no te decían si esos datos iban a ser anonimizados, no se comprometían a nada. En síntesis la defensa del MINSAL era que esta aplicación venían a tratar datos que ellos ya tienen la facultad de tratarlos, cuando uno le respondía que la base habilitante para el tratamiento de datos no es la ley porque están pidiendo consentimiento para un montón de otras cosas que van más allá de lo que está estrictamente autorizado por la ley, y al momento de solicitar consentimiento las cláusulas que ustedes ponen son super abusivas porque son amplias, están en términos vagos, no se comprometen a medidas de seguridad suficiente, se reservan el derecho a entregar los datos a instituciones privadas, etc.

El Consejo de la Transparencia dentro de sus facultades, atribuciones y funciones está la de fiscalizar que los organismos del Estado hagan un tratamiento adecuado de los datos personales. Cada cierto tiempo el Consejo para la Transparencia saca una circular, donde advierte sobre posibles abusos en el tratamiento de datos y envía una recomendación al respecto pero la misma no tiene ninguna validez porque no tiene facultad de sanción, ni nada. Es decir, solo puede hacer recomendaciones, entonces desde el Gobierno hacen cualquier cosa con los datos. Tampoco cuenta con personal capacitado en materia de protección de datos, con una autoridad de aplicación específica eso no pasaría.

-¿Qué consecuencias puede tener la implementación de tecnologías digitales como estas sin lineamientos de derechos humanos?

Yo creo que la privacidad es la condición necesaria para el ejercicio de un montón de otros derechos, como la libertad de expresión, libertad sindical, libertad de protesta. Hay un montón de derechos humanos que si uno no tiene privacidad no pueden ser ejercidos. Entonces al final el problema con este tipo de aplicaciones es que si no existe un enfoque con derechos humanos es que podemos usar la aplicación para esto pero también para un montón de cosas más, es decir, no existe un compromiso en el fondo. Exigen poner de tu parte entregando tus datos para ayudar a controlar la pandemia y te exigen confiar en la autoridad pero por otra parte no están dispuestos a responder a esa confianza mediante un compromiso de resguardar esa información. Al no existir ese compromiso puede terminar siendo usado para otros fines, para mi eso solo pasa cuando uno desarrolla estas políticas sin un enfoque de derechos humanos. Por ejemplo, esta app solicitaba acceso a geolocalización y eso es muy delicado porque suceden situaciones como que aparte de mi nadie va y viene de mi casa a mi trabajo, ni hace el mismo recorrido entonces es súper fácil cruzar esa información y saber a quién pertenece. Lo que pasó con esa tecnología es que no se piensa en el contexto político de Chile en donde estábamos justo con el estallido social en un contexto de protesta y entonces qué libertad de ejercicio de protesta o sindical uno puede tener. Si este tipo de aplicaciones no viene con una perspectiva de derechos humanos significan una restricción y una amenaza para un montón de otros derechos.

-Si, de hecho la app permitía la denuncia de aglomeraciones por parte de vecinos

Si, estaban las dos opciones la denuncia a aglomeraciones y la denuncia a un vecino para alertar que tenía Covid. Ese era justamente el problema que estaba totalmente al margen de la ley. No solo la ley 19. 628 es clara en que el titular es quien presta el consentimiento, sino

que la ley 20.584 sobre Derechos y Obligaciones del Paciente es super clara al decir que la ficha clínica sólo pueden acceder de partida personas que tengan relación con las prestaciones de salud del paciente o aquellos a los que el paciente haya autorizado, pero en ninguna parte sale que un tercero puede autorizar nada. Es una aplicación del Estado en donde se estaba poniendo directa vulneración a derechos fundamentales. Lo que si en Chile, si bien no tenemos ley de Protección de Datos Personales actual, desde julio del 2018 si es un derecho fundamental, está reconocido en la Constitución. Y eso te cambia porque ya no se trata de un Estado vulnerando un derecho mal regulado, sino un Estado vulnerando un derecho constitucional.

-¿Considerás que es necesario ceder en el derecho a la privacidad y protección de datos personales para un combate efectivo de la pandemia? En este sentido, ¿podríamos considerar excluyentes la protección a la salud pública y el derecho a la protección de nuestros datos?

De partida el derecho a la privacidad no es absoluto, en el sentido que por lo menos acá en Chile es la misma Constitución la que dice que la protección va a estar asegurada conforme a la ley. Esto no significa que nadie nunca pueda acceder a nuestris datos, sino que tiene que hacerse conforme a la ley. La crítica no era el acceso a los datos, sino a qué datos y bajo qué condiciones. El problema era que no se cumplía ninguna de las condiciones legales para que ese tratamiento fuera legítimo, entonces el problema es que la dicotomía que se generaba no estaba en torno a la privacidad y la protección de la salud, la dicotomía era entre el tratamiento de datos de forma ilícita versus la protección de la salud. Se pretendió hacer un tratamiento ilícito de datos bajo la bandera de la protección de la salud. Lo que se propone

desde la aplicación es un tratamiento completamente abusivo de los datos, en el sentido de que la medida debía presentarse como idónea, necesaria y proporcional en cuanto a los datos, los tiempos y usos para los cuales se solicitaban los datos y nada de eso se cumple. Lo que se propone desde la aplicación es un tratamiento ilegal porque no es que la ley prohíba tratar datos personales, el Estado puede tratar datos personales y sensibles porque nuestro derecho a la privacidad no es absoluto pero su discurso es falso y muy abusivo.

-Chile: ¿cuáles serían las consecuencias de almacenar datos en un banco de Amazon WS ubicado en Virginia, USA?

Probablemente esa decisión haya sido tomada por cuestiones económicas, pensando en que esos servidores seguramente son más seguros que los nuestros. De todas maneras, me parece una decisión práctica, no era problemática en el sentido de que en Chile no existe prohibición de transferencia internacional de datos porque no tenemos las reglas que existen en Europa. Más que nada existe un silencio absoluto sobre la transferencia internacional de datos personales. Siempre es complejo enviar los datos a otro lugar porque van a quedar en otra jurisdicción por lo que se van a regir por otras reglas, por lo general las grandes potencias imponen eliminar todas las restricciones de localización porque consideran que son medidas proteccionistas. Obvio, porque la mayoría de los servidores está en Estados Unidos, y ponen las reglas de juego. Es un tema súper complejo en el sentido de que todos saben los riesgos que implica, en cuanto a que terceros terminen teniendo acceso a la información pero también es la tendencia porque Estados Unidos golpea la mesa y te puede terminar llevando a un tribunal de la OMS (aunque ya no sirva para nada). En conclusión, de todas las cláusulas abusivas que existían con la app Amazon Web Services era la que menos importaba porque

en definitiva se estaba haciendo en base al consentimiento y todo el mundo manda sus datos fuera porque en Chile no hay reglas al respecto. Es un tema muy complicado porque cuando mandamos nuestros datos afuera es un acto de fe confiar en que esa información no va a ser accedida por terceros, pero la tendencia mundial es que se está empezando a obligar a los países a eliminar las barreras de localización de servidores.