**Instituto de Investigaciones Gino Germani**26, 27 y 28 de octubre de 2022

**María Florencia Antueno** (Facultad de Ciencias Sociales - UBA)

**Correo electrónico:** antuenoff@gmail.com

**Formación académica:** Lic. en Ciencias de la Comunicación (tesis pendiente)

**Eje problemático propuesto:** 11. Estado, instituciones y políticas públicas

**Eje problemático alternativo:** 4.Medios y tecnologías digitales

**Título de la ponencia:** Políticas públicas, datos personales e iniciativas digitales gubernamentales de monitoreo y gestión sanitaria durante la pandemia por la Covid-19: el caso de la aplicación CoronApp en Chile (2020).

**Palabras clave:** Chile; COVID-19; Aplicaciones;Políticas públicas.

## **1.Introducción**

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 misma 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 y la pandemia irrumpe en el marco de un fuerte estallido social, caracterizado por una ola de protestas que nucleaban reclamos de carácter heterogéneo como el acceso a la salud, la precarización laboral, el fin del sistema privado de pensiones, entre otros. Y decantaron en la necesidad de la reforma de la Constitución, la cual fue redactada durante la dictadura de Augusto Pinochet (Heiss, 18/2020)[[1]](#footnote-0). Desde el 2011 en Chile se fueron registrando cada vez más manifestaciones estudiantiles, hasta llegar a octubre del 2019 donde se produce lo que se conoce como la revuelta o el estallido donde miles de estudiantes se negaron a pagar el aumento del metro, bajo la consigna “*No son treinta pesos, son treinta años.*” La pandemia vino a evidenciar aún más la crítica situación de desigualdad y precarización de las clases medias y bajas. Esta revuelta fue la manifestación más grande de la historia del país. A pocos meses del hecho, se produjo la pandemia la cual la administración de Sebastián Piñera tuvo que enfrentarla con un 6% de imagen positiva, según la encuesta N° 84 del Centro de Estudios Públicos (2019). Por supuesto que la pandemia trajo consigo una serie de desafíos para el gobierno, defensor del modelo neoliberal consagrado en la Constitución de 1980, el cual se encontró en la paradoja frente a desplegar un nivel de coordinación social e intervención estatal contrario a su proyecto ideológico. Fue así que en un primer momento el gobierno de Piñera se mostró reticente a tomar medidas de aislamiento social y pareció sugerir que seguiría el modelo británico de inmunidad “de rebaño”, es decir, buscar que la exposición de la población al virus generase inmunidad. Sin embargo, a dos semanas desde la llegada de la COVID-19 el país se encontró ante la necesidad de contener la rápida expansión del virus con medidas asociadas a los objetivos de lograr el aislamiento y el distanciamiento físico de sus poblaciones. Así, el 16 de marzo, ante el aumento de casos y la imposibilidad de rastrear el origen de la infección se decretó el cierre de fronteras, la suspensión de las clases, la cuarentena obligatoria para personas contagiadas, la reducción del número de personas en actos públicos y la sanitización del transporte. Se decretó el Estado de Excepción Constitucional de Catástrofe, contemplado en la Constitución Política de la República para situaciones de calamidad pública. Este permite restringir las libertades de locomoción y reunión, requisar bienes, limitar el ejercicio del derecho de propiedad y adoptar todas las medidas extraordinarias de carácter administrativo que sean necesarias para el pronto restablecimiento de la normalidad (art. 43). Junto con esto, se declaró toque de queda nocturno. El mismo había sido impuesto en distintas ciudades durante los días de protestas de octubre, se volvió a decretar durante marzo del 2020 y estuvo en vigencia durante más de un año, dato no menor para nuestro análisis.

A nivel mundial se venía desarrollando una tendencia con China, Corea del Sur y Singapur siendo los primeros en utilizar sistemas de vigilancia para garantizar la eficacia de las medidas y frenar la propagación del virus. El gobierno singapurense fue pionero en desarrollar, bajo iniciativa gubernamental, una aplicación denominada TraceTogether, la cual fue liberada a código abierto (open source) para que los desarrolladores de todo el mundo puedan utilizarla de forma gratuita, modificar y redistribuirla (Wild Entrepreneu, 2020). La misma utiliza un sistema de rastreo de contactos por tecnología Bluetooth y ha sido retomada por Asia, Europa y América Latina, mediante modificaciones y adecuaciones a cada contexto.

Latinoamérica no fue la excepción, Bolivia fue el primer país en lanzar una “coron-app” en diciembre del 2019, seguido de Colombia y Uruguay (Aguerre, 30/2020). Chile lanzó en abril CoronApp, desarrollada por la división Gobierno Digital[[2]](#footnote-1). La misma fue promocionada como una herramienta para poder realizar autoevaluación de síntomas, alertar a las autoridades, informar y/o denunciar conductas de alto riesgo y brindar o solicitar ayuda a los vecinos.

Dado este rápido avance en el desarrollo de estas aplicaciones móviles, diversas organizaciones civiles manifestaron públicamente sus preocupaciones. Amnistía Internacional, Human Rights Watch Org, Access Now, Center for Digital Democracy y Privacy International, entre otras, expusieron, el 2 de abril de 2019, una Declaración conjunta de la sociedad civil[[3]](#footnote-2) en la que alertaron sobre la posible vulneración de derechos humanos relativos a la privacidad y protección de datos personales. En ese documento presentado por Human Rights Watch, Vía libre Org., etc., (2020) 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 la necesidad 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 toda medida de protección necesaria a 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.

Frente al almacenamiento y tratamiento de datos personales y sensibles como son lo de salud, y la habilitación de acciones de denuncia por aglomeraciones e inclumplimiento de cuarentena en contextos tan delicados como el estallido social que tenía lugar en Chile y el proceso de reforma de su Constitución; nos preguntamos si esta tecnología ha sido desarrolladas siguiendo un correcto lineamiento con los derechos humanos, promoviendo, efectivamente, el cuidado de la salud y la protección de la privacidad. Es así que surgen preguntas como: ¿Cumplen los Términos y Condiciones con los principios de protección de datos personales? ¿Las políticas, términos y condiciones de las aplicaciones se ajustan a las legislaciones vigentes, aún en un marco de excepcionalidad por la pandemia? ¿Los datos recolectados y almacenados son adecuados, relevantes y limitados a las finalidades declaradas? ¿Son los datos personales y sensibles recogidos proporcionales a los objetivos planteados? ¿Qué implicaciones pueden tener los objetivos de denuncia a las autoridades en un contexto de revuelta social?

**Herramientas teóricas para pensar el desarrollo de tecnologías por parte de los Estados nacionales**

En primer lugar, partimos por comprender que ninguna opción tecnológica es neutra y ninguna tecnología lo es. Por ello nos parece relevante situar el desarrollo de la Coronapp para comprender el contexto y el Estado que desarrolla esta política pública. Para esto, partimos por entender con O'donnell (1977) al Estado capitalista como un organizador de las relaciones sociales, en el sentido de que tiende a ser mediador de dichas relaciones y aportar elementos para su reproducción. Y a las políticas estatales 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)

A su vez, para analizar esto nos parece pertinente retomar a Manuel Castells (1995) en su texto *La ciudad informacional: tecnologías de la información, reestructuración económica y el proceso urbano regional*, donde afirma que hacia finales del siglo XX el capitalismo ha sufrido un proceso de reestructuración profunda. Se ha dado el paso de una economía de escala a una economía global, caracterizada por una descentralización y flexibilización de la gestión de las empresas y una integración e interconexión global de los mercados financieros. Los actores económicos se mueven por una red global que elimina las fronteras nacionales, dando 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” (Castells, 1995, 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.

El autor define a los modos de desarrollo como fórmulas tecnológicas definidas por el elemento que determina la productividad en el proceso de producción. Entiende que el conocimiento interviene en todos los modelos de desarrollo “(...) ya que el proceso de producción está basado siempre en algún nivel de conocimiento.” (2006, p. 18) En particular en este modo de desarrollo actual, la información constituye tanto la materia como el producto.

Dos décadas después 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, en donde su capital se explica por la creación de ecosistemas, basados en la información y el procesamiento de datos. Para el autor, en esta etapa del capitalismo la materia prima son los datos, en donde el propio procesamiento produce nuevos datos, en un proceso que se retroalimenta. Los datos en el capitalismo informacional pasan a tener un rol fundamental como recurso. Su recolección, almacenamiento y análisis pasan a tener un rol central para mantener el crecimiento de la producción y de la economía. El autor establece como uno de sus argumentos principales que en el siglo XXI el capitalismo se centra en la extracción de esta nueva materia prima.

Frente a este escenario, la académica Zuboff, Shoshana (2020) explica que hoy nos adentramos en una nueva era de la economía política, denominado por la autora como “capitalismo de la vigilancia”. Esta era, para la autora, “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” (Zuboff 2020, p, 23). Lo particular de este capitalismo de la vigilancia como una variante del capitalismo informacional es que los actores de mercados están “atrapados en una dinámica de intensificación continua de los medios de modificación de la conducta y creciente fortalecimiento del poder instrumentario.” (Zuboff, 2020, p. 22)

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 objetivos comerciales buscados.

**Contexto regulatorio**

Bajo estos conceptos nace la propuesta de indagar sobre la protección de datos personales en la aplicación CoronApp; en un contexto en donde las tecnologías informacionales han cambiado las lógicas de la economía, haciendo que la generación, procesamiento y transmisión de información hayan pasado a ser, 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 la 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 pandemia, encontramos pertinente problematizar la protección de los datos personales de los individuos y revisar las pautas de seguridad, términos y condiciones de privacidad de esta aplicación móvil. El acceso a ciertos datos como los de geolocalización, su recolección y tratamiento, las posibilidades de denunciar aglomeraciones o al vecino, corren el riesgo de constituirse en nuevas fuentes de control social y amenazas contra la privacidad e impedir el efectivo ejercicio de otros derechos por parte de los ciudadanos.

A fin de conocer brevemente el marco regulatorio en materia de protección de datos personales en Chile, haremos un repaso por la adhesión a tratados internacionales y su actual legislación sobre Protección de la Vida Privada. Los sistemas latinoamericanos de protección de datos tienen la particularidad de que en la mayoría de los países de la región se encuentran amparados en sus constituciones nacionales. En Chile en el 2010 se 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. Ese años se sancionó la Ley que consagra el Derecho a la Protección de Datos Personales  N° 21.096, modificando el artículo 19 N° 4 de su Constitución. El mismo otorga carácter constitucional al derecho a la protección de datos personales y lo reconoce como un derecho fundamental que tienen todos sus ciudadanos por el simple hecho de ser personas.

Le ley que actualmente regula el tratamiento de datos personales en el país es la N° 19.629, sancionada en el año 1999 a pocos años de que el Parlamento Europeo promulgara la Directiva 95 N° 95/46/CE, la cual permitía la transferencia internacional de datos, únicamente, con aquellos países que presentaron un adecuado nivel de protección. Eso hizo que la legislación chilena incorpore los principios de protección establecidos en la Directiva: consentimiento, lealtad, legalidad, transparencia, exactitud, minimización, seguridad y responsabilidad. Esta Directiva, fue derogada en el 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 la libre circulación de estos, en donde recupera y actualiza los principios contenidos.

A su vez, la Organización de Estados Americanos (OEA), de la que Chile forma parte, ha trabajado desde el año 1996 diferentes resoluciones relativas a la protección de datos personales instando a los estados miembros a tomar determinadas acciones en la materia. En particular, en la “Guía Legislativa sobre la Privacidad y la Protección de Datos Personales en las Américas” (2015) se establecen doce principios[[4]](#footnote-3) que deben regir en el ámbito público y privado para una adecuada protección de los datos personales.

En cuanto a los principios de protección de datos contenidos en la legislación chilena sobre Protección de la Vida Privada, la misma incluye los de licitud y consentimiento, los cuales refieren a que el tratamiento de datos personales será lícito siempre que el titular haya prestado su consentimiento; el mismo debe haber sido informado de forma clara y por escrito. Pero establece una particularidad respecto a que los organismos públicos podrán utilizar datos personales, sin consentimiento del titular mientras que estén referidos a la materia de su competencia. El principio incluído en la ley es el de finalidad, el cual que refiere a que los datos personales deben usarse sólo para los fines recolectados; el de exactitud se encuentra incluído expresando que “los datos deben ser exactos, actualizados y responder con veracidad a la situación actual del titular.” El de responsabilidad se incluye en la ley indicando que el responsable de los datos personales recolectados es la base o registro donde se almacenan dichos datos; el o los mismos deberán cuidar de ellos haciéndose responsable de los daños y en caso de daño deberán indemnizar por los daños ocasionados. Una particularidad es que en ningún momento indica que los mismos deberán adoptar las medidas de seguridad necesarias para garantizar la protección. Simplemente establece medidas de sanción posterior. Por último, se encuentra incluida la protección especial a datos sensibles indicando que: “No pueden ser objeto de tratamiento los datos sensibles los cuales 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.”

En cuanto a los principios que la ley no incorpora son los de transparencia que refiere a la necesidad de que el titular cuente con información detallada acerca de donde se almacenarán los datos, la identidad y domicilio de el/los responsables, las posibles consecuencias de entregar sus datos y las de no hacerlo. Tampoco se encuentran incluidos los principios de necesidad y proporcionalidad referidos a que más allá de que los datos personales recolectados respondan a los fines declarados, los mismos deberían ser ciertos, adecuados, pertinentes y no excesivos en relación al ámbito y finalidad para los que se hubieren obtenido. Y por último, no incorpora una autoridad de aplicación de lo indicado en la ley, lo cual dificulta muchísimo su aplicación y el control de los principios, derechos y obligaciones amparados en ella. Actualmente el único órgano con facultades para realizar revisiones a través de las cuales luego podrá formular recomendaciones no vinculantes es el Consejo para la Transparencia.

**Los principios de protección de datos personales en CoronApp**

A partir de estos principios seleccionados, donde vemos que algunos se encuentran en la ley vigente y otros no, observamos cómo se expresa esto en los términos y condiciones de la aplicación. Para empezar, la aplicación fue llevada a cabo por la División de Gobierno Digital del Ministerio Secretaría General de la Presidencia (SEGAPRES) y ofrecida por la Subsecretaría de Redes Asistenciales del Ministerio de Salud (MINSAL). Es decir, fue mediante la iniciativa del Estado que esta aplicación pudo ser desarrollada y administrada 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.

Al ingresar la misma ofrece dos formas de ingreso: una opción es el ingreso con clave única[[5]](#footnote-4), la otra ingresando RUN o pasaporte, esta última exige que el usuario se registre proporcionando los siguientes datos: cédula de identidad, RUN o pasaporte, número del documento, nombre completo, número de teléfono, edad, comuna, correo electrónico (opcional), y una contraseña.

Junto con estos datos de acceso, para utilizar la función de autodiagnóstico requiere 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 había tenido contacto, vivía o trabajaba con una persona caso confirmado COVID-19; si tuvo contacto estrecho en los últimos diez días; que indique la temperatura corporal; si la persona ha estado embarazada, y si posee enfermedades preexistentes como: cáncer, diabetes, enfermedad hepática, renal crónica y/o respiratoria.

Y por último, otorga la opción de proveer información de donde realizaría la persona que haya dado resultado positivo o fuera contacto estrecho la cuarentena. Para eso solicitaba el ingreso de la dirección a través de la ubicación en el mapa y declaraba que el registro no podía ser modificado. La segunda opción que brinda es denominada como “colabora para prevenir el contagio” dentro de la cual se encuentran tres opciones que para ser utilizadas requieren del acceso a la geolocalización: la primera, es la de reportar aglomeraciones, la segunda denunciar incumplimiento de cuarentena, y la tercera para denunciar fila para acceder a servicios. Es decir, quien se descargue la aplicación podría denunciar a sus vecinos frente a las autoridades. En un contexto donde Chile todavía estaba transitando social y políticamente lo que había sido la revuelta vivida en octubre del 2019.

A partir de esto, pasamos a observar los principios contenidos en los términos y condiciones donde vimos que el de consentimiento es primordial para garantizar la licitud del tratamiento. Pero que los organismos públicos pueden no requerir cuando traten información referida a la materia de su competencia. En la aplicación esto se observa aplicado, ya que la misma no permite avanzar a no ser que uno declare que acepta los términos y condiciones pero, a su vez, permite que quien ingresa los datos pueda cargar los datos personales de hasta 8 personas más. Es decir, si bien CoronApp declara que el uso de la aplicación es a título personal al mismo tiempo cuenta con la posibilidad de agregar datos de salud de terceros que convivan o hayan estado en contacto con el titular sin garantizar que los mismos hayan prestado el consentimiento de ello; con la gravedad de que los datos solicitados por la aplicación al ser datos de salud son datos sensibles, por lo que, según establece la ley, merecen una protección aún mayor.

Se observa que la aplicación cumple con el principio de finalidad al indicar los servicios que la misma garantiza, de forma clara y precisa: i) monitoreo de síntomas; ii) información sobre la pandemia. Conecta con sitios oficiales del Gobierno de Chile (...); iii) servicios públicos. Conecta con Comisaría virtual y Chileatiende; iv) accede al chatbot informativo del Ministerio de Salud. La aplicación permite interactuar y colaborar con tu comunidad: reportando incidentes y aglomeraciones; ayuda vecina. Pero al no cumplir con el principio de consentimiento y licitud, tampoco se incluye el principio de exactitud el cual define que los datos deben ser exactos, correctos, actualizados y completos, y que el recopilador debe adoptar todas las medidas necesarias para asegurarse de que eso sea así. CoronApp, al brindar la posibilidad de ingresar datos de terceros suma otra complejidad ya que por una lado la aplicación es de uso personal y por el otro decreta que el usuario es “responsable de garantizar el buen uso de la aplicación, la completitud, veracidad, exactitud y precisión de sus datos y los de los tercero que ingresa.” (p.2) O sea que el titular no sólo es responsable de sus datos sino que pasa a tener responsabilidad por la exactitud de los datos de terceros que ingresa que no prestaron su consentimiento para que sean recolectados y almacenados.

Como se indicó anteriormente la ley N° 19.628 no incorpora los principios de necesidad y complementariedad. que refieren a que los datos personales recolectados deben ser solamente los necesarios para cumplir con los fines declarados y deben tratarse en base a ellos. Esta ausencia se ve reflejada en los términos y condiciones en donde se indica que los mismos pueden ser modificados en cualquier momento, sin aviso ni autorización previa por parte del usuario y que con el objetivo de proporcionar a los usuarios un mejor servicio, puede resultar necesario recopilar y procesar cierta información, que se obtendrá del dispositivo móvil en donde se ha instalado la aplicación. Es decir que el titular de los datos al aceptar estos términos y condiciones, está aceptando que los mismos puedan cambiar en cualquier momento y que la mera utilización posterior de la aplicación supondría la aceptación de dichos cambios.

Por último, en cuanto a los principios de responsabilidad y seguridad. La ley vigente indica que el responsable de datos personales y de indemnizar por los daños que se ocasionen es el titular del registro o base de datos. Que en este caso los términos declaran que el propietario de la base de datos, es una nube perteneciente a Amazon Web Services ubicada en Virginia, Estados Unidos; aclarando que la misma respeta la confidencialidad y se somete a la legislación chilena en caso de que surjan conflictos aunque la legislación vigente no contempla ningún punto referido al flujo transfronterizo de datos.

Por último y uno de los puntos más importante para la aplicación y funcionamiento de toda ley de protección de datos personales es la autoridad encargada de velar por su cumplimiento y del acceso a los derechos y obligaciones allí contenidos. Vimos que la legislación chilena no incorpora la creación de un órgano de control pero en el 2008 sancionaron la ley N° 20.285 de Acceso a la Información Pública con la que se crea el Consejo para la Transparencia. El mismo dentro de sus facultades, atribuciones y funciones está fiscalizar que los organismos del Estado hagan un tratamiento adecuado de los datos personales, pero sus informes y conclusiones sólo tienen carácter de recomendación, por lo cual no posee facultad de sanción. En los términos y condiciones no se hace mención al Consejo, solo se declara que el responsable de velar por la protección de los datos personales es el Ministerio de Salud aunque la aplicación fue desarrollada por la División de Gobierno Digital del Ministerio Secretaría General de la Presidencia. En este caso, como vimos, el Ministerio de Salud tiene facultades para tratar los datos relacionados a las materias de su competencia sin autorización por parte del usuario. Pero el problema aquí surge porque los datos solicitados ( Clave Fiscal, geolocalización, datos de terceros) exceden el ámbito del Ministerio. Y al mismo tiempo, la ausencia de una autoridad de aplicación dificulta enormemente que los titulares puedan ejercer su derecho a indemnización y reclamo ante incumplimientos porque tienen que recurrir directamente a un Tribunal de Justicia.

**Conclusiones**

Lo expuesto, nos lleva a la conclusión de que los términos y condiciones de la aplicación reflejan los grises y vacíos que presenta la normativa. 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 la normativa vigente sobre protección de los datos personales demuestra la necesidad de desarrollar marcos regulatorios fuertes para que la tecnología orientada al bien común, esté basada en el respeto a los derechos humanos. A fin de evitar que las herramientas se conviertan en instrumentos de vigilancia y control, marcadas únicamente por la necesidad de seguir profundizando en la extracción del excedente conductual, en los términos en que es entendido por Zuboff (2020).

Otro punto que observamos es que Chile ha sido uno de los pocos países de latinoamérica en incluir la opción de reportar aglomeraciones. Como dijimos anteriormente si pensamos en el contexto en que la misma fue desarrollada, bajo el gobierno de Sebastián Piñera y a pocos meses del *Estallido social* del cual él mismo declaró que estaban en estado de guerra, resulta todavía más imprescindible que la tecnología desarrollada con el fin de protección de la salud pública, sea diseñada desde el principio evitando la vigilancia y control, y con una correcta protección de los datos personales y sensibles que no obstaculice el ejercicio de otros derechos.

**Bibliografía**

* 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.
* 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>
* O’Donnell, G. (1977). Apuntes para una Teoría del Estado. Centro de estudios de Estado y Sociedad (CEDES).
* Organización de los Estados Americanos (s.f.). Protección de Datos Personales. Portal OEA.<https://www.oas.org/es/sla/ddi/proteccion_datos_personales.asp>
* 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).
* Srnicek, N. (2019). Capitalismo de Plataformas. Editorial Caja Negra.
* Zuboff, S. (2020). La era del capitalismo de la vigilancia. Editorial Paidós.

Legislación:

* Ley N° 19.628. Biblioteca del Congreso Nacional de Chile, Chile, 28 de agosto 1999.
* Términos y condiciones Coronapp, Ministerio Secretaría General de Gobierno, 16 de abril de 2020.
1. <https://www.fundacioncarolina.es/wp-content/uploads/2020/04/AC-18.2020.pdf> consultado 2/01/2022 [↑](#footnote-ref-0)
2. 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. [↑](#footnote-ref-1)
3. <https://www.hrw.org/es/news/2020/04/02/declaracion-conjunta-de-la-sociedad-civil-los-estados-deben-respetar-los-derechos> consultado 2/01/2022 [↑](#footnote-ref-2)
4. 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. [↑](#footnote-ref-3)
5. La Clave Única sirve para obtener en línea diversos servicios y beneficios que ofrece el Estado. [↑](#footnote-ref-4)