

Reflexiones en torno a la crisis sanitaria: el fenómeno de los datos personales y sensibles

Camilo Brenett Álvarez¹

Introducción

Los datos y su respectivo tratamiento son un fenómeno que con el desarrollo de la sociedad digital ha cobrado especial relevancia, puesto que variadas acciones en Internet requieren de un flujo constante de información que proporcionan los usuarios sobre sí mismos. Frente a esta nueva interacción, han surgido también otras interrogantes que sitúan en el centro de la discusión la debida protección para la ciudadanía que emplea tecnologías y el resguardo de bienes jurídicos como la protección de los ciudadanos frente al tratamiento de datos que pueden realizar privados y el Estado. Tomando en consideración este precedente que continúa irresoluto al menos para la realidad del país, cabe problematizar lo sucedido bajo las particularidades de la emergencia sanitaria a raíz del Covid-19 y los límites en el tratamiento de datos bajo un contexto de “normalidad” como también en circunstancias excepcionales.

En el presente informe, serán examinados los términos y condiciones de funcionamiento respecto a datos personales y tratamiento de datos en la aplicación oficial del Gobierno de Chile llamada “Coronapp”² a la luz de la legislación chilena sobre datos personales y su tratamiento. El objetivo es analizar el fenómeno del tratamiento de datos enmarcado en la reciente pandemia junto a la identificación de algunas problemáticas que tal vez no hayan sido nuevas, pero definitivamente fueron profundizadas por el devenir de la situación sanitaria y se erigen hasta la actualidad como una deuda para nuestro país.

¿Qué se entiende como datos personales, datos sensibles relativos a la salud y tratamiento de datos?

La Comisión Europea³ define los datos personales como cualquier información sobre una persona natural viva previamente identificada o eventualmente identificable. Dicho de otra manera, las diversas informaciones que una vez conocidas pueden ayudarnos a individualizar una

Novedades

12/06/2023

Política

Reflexiones en torno a la crisis sanitaria: el fenómeno de los datos personales y sensibles

07/06/2023

Sociedad

Evolución(es) del concepto de Cohesión Social: ideas preliminares para su desarrollo en Chile

30/05/2023

Política

Sobre la Fragmentación del Congreso en Chile

09/05/2023

Internacional

La política exterior en el gobierno de Joe Biden

04/05/2023

Sociedad

20 años de Educación Media obligatoria: Breve historia de desafíos acumulados

12/04/2023

Política

Propuestas para una Constitución Laboral

Acerca de

Este informe ha sido revisado por el Consejo Editorial de Asuntos Públicos. El contenido no representa necesariamente la opinión del Centro de Estudios del Desarrollo, CED.

©2023 asuntospublicos.cl. Todos los derechos reservados.

Se autoriza la reproducción, total o parcial, de lo publicado en este informe con sólo indicar la fuente.

¹ Estudiante de Derecho de la Universidad Alberto Hurtado. Pasante del Centro de Estudios del Desarrollo.

² Coronapp fue la única aplicación oficial del Gobierno de Chile para el control y prevención del COVID-19. Según datos obtenidos por Ley de Transparencia hasta el día 7 de mayo de 2020, sumaba 82.355 descargas, lo que se traduce en que menos del 1% de la población tenía la aplicación en sus dispositivos móviles. Lo anterior resulta relevante dada la poca incidencia y masividad que tuvo la aplicación, pero no tiene un efecto en los aspectos legales que se discuten en el presente informe. Disponible en: <https://www.emol.com/noticias/Tecnologia/2020/05/28/987424/1-poblacion-app-Gobierno-coronavirus.html> / (Fecha de consulta: 17 de 05 2023).

³ A través del Reglamento 2016/679 del Parlamento Europeo con fecha 27 de abril del año 2016. Disponible en: <https://www.boe.es/doue/2016/119/L00001-00088.pdf>.

persona en el marco del constante tráfico de datos que circula a través del Internet y sus diversas plataformas, bases de almacenamiento de datos, programas, software y aplicaciones. Por otra parte, el mismo Reglamento define el tratamiento de datos personales en su artículo 4.2 como “cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción”. En una clasificación aún más precisa se regulan los datos relativos a salud, esta subclasificación hace referencia a cualquier información que pueda contribuir a revelar mayor conocimiento sobre diagnósticos y estado de salud en general⁴.

En cuanto la legislación chilena, contrario al contexto europeo, la Ley N° 19.628 se encarga de abordar estas temáticas y resulta notoriamente obsoleta, ya que data del año 1999. Sin embargo en su artículo 2 podemos encontrar una definición respecto a los datos personales, en donde el Legislador los caracteriza como “los relativos a cualquier información concerniente a personas naturales, identificadas o identificables”; En el mismo apartado, literal “O” es definido el concepto de tratamiento de datos para nuestra legislación, estableciendo que este consiste en cualquier operación, procedimiento o conjunto de operaciones que permitan la recolección, almacenamiento, extracción, selección, comunicación de datos de carácter personal.

¿Que establece la Constitución al respecto?

En lo que respecta a nuestro ordenamiento constitucional, los datos personales principalmente pueden ser vinculados a garantías relativas a la privacidad que se encuentran en el artículo 19 numeral 4, donde en principio, el Estado contrae obligaciones en el marco de garantizar el respeto y el deber de proteger la vida privada y la honra de toda persona junto a la familia. Lo anteriormente descrito, es fruto de una reforma constitucional que entró en vigencia en el año 2018, mediante una moción parlamentaria del año 2014⁵. En dicha moción, se buscó enriquecer lo establecido a raíz del bien jurídico de la vida privada, agregando al catálogo de garantías constitucionales la protección de datos personales como un derecho fundamental autónomo de toda persona. En el mismo sentido, con el fin de otorgar mayor certeza jurídica a la acción de proteger tales datos, se incorpora al texto constitucional el siguiente precepto: “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”. Como resultado de esta modificación, se busca en primer término concretar una aproximación al concepto de autodeterminación informativa lo que se traduce en el control de los datos personales por parte de su titular, y en segundo término, se otorga una remisión expresa para que el Legislador actualice la normativa del año 1999 sobre protección y tratamiento de datos.

¿Cuál es el problema de la legislación vigente sobre datos personales en Chile?

La principal característica de la legislación sobre datos personales consiste en su obsolescencia y lo inconexo que resulta en relación con los preceptos constitucionales recientemente promulgados. Esto se debe a que previo a la reforma constitucional del año 2018, fue promulgada la Ley de protección de la vida

⁴ A través del Reglamento 2016/679 del Parlamento Europeo con fecha 27 de abril del año 2016. Disponible en: <https://www.boe.es/doi/2016/119/L00001-00088.pdf>.

⁵ La moción de reforma constitucional fue ingresada por los Senadores Hernán Larraín Fernández, Felipe Harboe Bascuñán, Eugenio Tuma Zedán, Pedro Araya Guerrero y Ricardo Lagos Weber.

privada N° 19.628 en 1999 que establece una serie de requisitos en base al consentimiento para el posterior tratamiento de datos personales. Sin embargo, el paradigma jurídico y el avance tecnológico en 1999 era muy distinto al debate y las ideas que en la actualidad se desarrollan respecto a la protección y tratamiento de datos. Por esta razón, la reforma constitucional puede haber sido un notable avance para la legislación chilena sin embargo la Ley que está llamada a materializar los esfuerzos y avances constitucionales no guarda coherencia debido a la desconexión entre dos cuerpos normativos de distintas épocas y a las nuevas tendencias regulatorias.

Esta problemática sobre normas más actualizadas también ha sido expresada por la OCDE, por intermedio de una carta de advertencia en el mes de julio del año 2015⁶. De acuerdo a este documento, países como Chile y Turquía persisten en el incumplimiento de estándares aceptables en materia de la protección de datos personales. Esto se debe en primer término al enfoque normativo sobre el tratamiento de los datos personales por sobre la potestad del titular de estos datos, en razón de que no resulta del todo preciso el reconocimiento de derechos por parte del usuario en cuanto a los datos compartidos. Por otra parte, no existen mecanismos ni una Institucionalidad especializada en resguardar el interés de quien pueda verse afectado con el tratamiento de datos que lesione la privacidad por lo que en la práctica, el resguardo de lo que se establece en la Ley N° 19.628 termina siendo responsabilidad del particular.

¿Qué pasó en contexto de crisis sanitaria con el tratamiento y el resguardo de datos personales en Chile?

Así llegamos al 2020 con una legislación prácticamente obsoleta que tuvo que hacer frente a grandes desafíos digitales en materia de tratamiento de datos en el marco de la pandemia.

A nivel global, la Organización Mundial de la Salud catalogó al COVID-19 como “pandemia” un 11 de marzo del año 2020. En Chile, la detección del primer contagio se produjo el 3 de marzo del año 2020 y en un primer momento los contagios fueron provocados por residentes que contraen el virus en viajes fuera del país. A partir de ese momento el Poder Ejecutivo comunicó una serie de medidas para atender la emergencia sanitaria como la suspensión de clases en primera instancia por dos semanas para después oficializar la medida en forma indefinida, la creación de aduanas sanitarias, el cierre de fronteras y los toques de queda junto a la creación de salvoconductos sanitarios.

El 13 de marzo del año 2020, por intermedio de un anuncio presidencial, el gobierno de Chile comunicó entre otras medidas, que se estarían realizando esfuerzos conjuntos con Corea del Sur para la producción de una aplicación que agilizaría la comunicación entre las autoridades sanitarias y la ciudadanía. Un mes después, el 16 de abril se realizó el lanzamiento de “Coronapp” una aplicación de descarga gratuita para dispositivos móviles inteligentes. Esta aplicación tenía 4 funciones: reporte y control de síntomas, medio de información oficial, monitoreo de cuarentenas y reportes de aglomeraciones e incumplimientos de la norma sanitaria.

Para el cumplimiento de los objetivos señalados, la aplicación debía solicitar una autorización para el tratamiento de los datos de sus usuarios. Esta autorización junto con los términos y condiciones de la

⁶ Así se constata en medios de prensa de la época. Artículo disponible en: <https://www.latercera.com/pulso/ocde-envia-carta-de-advertencia-a-chile-por-retraso-en-proteccion-de-datos-personales/> (Fecha de consulta: 19 de abril de 2023).

aplicación son parte del tratamiento de los datos a obtener, información especialmente sensible⁷ que reviste un nivel aún más delicado que los datos de carácter personal debido a su relevancia y la peligrosidad de su tratamiento y conocimiento. En lo que respecta a términos y condiciones, junto a la política de privacidad, existen una serie de puntos polémicos que generan fricciones entre bienes jurídicos como la privacidad, la intimidad y la salud pública. A continuación, voy a explicar los principales aspectos que resultan discutibles de los “términos y condiciones” de esta aplicación.

a) Poder de decisión respecto a los datos

La aplicación en primer término ofrece el poder discrecional del usuario para aceptar o denegar el conocimiento de los datos solicitados por la aplicación. Sin embargo, no se le confiere al usuario la posibilidad de limitar la autorización reconociendo, por ejemplo, el derecho a querer eliminar sus datos de la base de datos de la aplicación. El no reconocimiento de estos Derechos o atribuciones de los usuarios se traduce en un debilitamiento de la noción de titularidad sobre los datos personales y sensibles al limitar las facultades del usuario respecto a los datos compartidos. Esto condiciona la capacidad por parte de los usuarios de poder limitar el conocimiento de información sensible por parte de autoridades y entidades públicas o privadas.

b) Almacenamiento de los datos

En cuanto el almacenamiento de los datos recepcionados en el funcionamiento de la aplicación surgen nuevos conflictos relacionados al carácter transnacional que muchas veces tiene la problemática del tratamiento de datos personales. La entidad que se encarga del almacenamiento es “Amazon Web Services” a través de una nube de carácter privado bajo la administración exclusiva del Ministerio de Salud. Sin embargo y pese a la exclusividad del Minsal, la compañía privada cuenta con sede en Virginia, Estados Unidos, lo que genera preocupación al haber posibles conflictos entre los marcos jurídicos aplicables para dicha compañía en materias como el resguardo de los datos almacenados por otras entidades y las eventuales responsabilidades civiles que correspondan. Por otra parte, el almacenamiento se configura en dos hipótesis que generan confusión por lo difuso de su explicación. Según consta en los alcances del Consejo para la Transparencia⁸ y un informe elaborado por la Biblioteca del Congreso Nacional⁹, la aplicación estaría facultada para conservar los datos recolectados por un plazo de 15 años o hasta el término de la emergencia sanitaria, sin embargo los factores que determinan la decisión no son del todo claros ni tampoco se explica qué es lo que se entiende como “término de la emergencia sanitaria” relegando estas indicaciones a una peligrosa dimensión discrecional por parte de la autoridad sanitaria y no por criterios objetivos previamente definidos. Sin embargo, las legislaciones más avanzadas en la materia, como la regulación europea¹⁰, coinciden en que el tratamiento de datos debe llevarse a cabo fundamentado en directrices claras y específicas.

⁷ Es importante entender que cuando hablamos de dato personal y dato sensible, estamos describiendo una relación de género-especie ya que por dato personal se entiende todo elemento que ayude a identificar a una persona natural, mientras que los datos sensibles corresponden a elementos que revelen origen racial/étnico, opiniones y convicciones personales, datos genéticos y biomédicos, antecedentes y diagnósticos médicos, datos respecto la vida sexual.

⁸ Oficio disponible en: <https://www.consejotransparencia.cl/wp-content/uploads/2020/05/Oficio-CPLT-675-SEGPRES-SALUD-CORONAPP-07.05.2020.pdf> (Fecha de consulta: 19 de 04 de 2023).

⁹ Boletín N°10 disponible en: https://obtienearchivo.bcn.cl/obtienearchivo?id=documentos/10221.1/79593/1/boletin_coronavirus_10.1_FINAL.pdf (Fecha de consulta: 19 de 04 de 2023).

¹⁰ A través del Reglamento 2016/679 del Parlamento Europeo con fecha 27 de abril del año 2016. Disponible en: <https://www.boe.es/boe/2016/119/L00001-00088.pdf>.

c) Multiplicidad de fines con los que se recolectan y almacenan los datos

La aplicación define el alcance de sus funciones en 4 segmentos como ya fue señalado anteriormente (reporte y control de síntomas, medio de información oficial, monitoreo de cuarentenas y reportes de aglomeraciones e incumplimientos de la norma sanitaria). Para su correcto funcionamiento requiere una multiplicidad de datos en donde se vuelve complejo evaluar la estricta necesidad¹¹ de su recolección para el cumplimiento de los fines que la misma aplicación define. Sin embargo, es importante considerar que la recolección de datos debe enmarcarse en atención a criterios de legalidad, explicitud y especificidad. La característica genérica de ciertos datos solicitados como por ejemplo, la geolocalización de los usuarios para la supervisión de los eventuales contagios o la posibilidad de denunciar inobservancias a la norma sanitaria basándose exclusivamente en el criterio de ciudadanos, son elementos que no pueden ser desconocidos por las consecuencias en materia de privacidad y de fragmentación social¹², pudiendo prestarse para otro tipo de fines alejados de la prevención y el control de una crisis sanitaria.

d) Posesión de los datos recolectados

Finalmente, los datos recolectados y almacenados por la aplicación según los términos y condiciones de la misma estarían bajo el control del Ministerio de Salud. Aun así, existe la posibilidad - y así es declarado abiertamente por su política de privacidad - que cuando así lo exija la Ley o alguna orientación administrativa, los datos sean compartidos con entidades privadas u otra institución pública. En qué medida, qué tipo y cantidad de datos podrían ser eventualmente compartidos no se indica con claridad, así como tampoco queda claro quién puede ser este receptor. En este sentido, se vulneran garantías en materia de tratamiento de datos al no existir certeza de quién será finalmente la entidad que manipulará la información recolectada.

¿Cuál es la actual discusión legislativa respecto a protección y tratamiento de datos?

Frente al estado actual del marco jurídico aplicable a la protección y tratamiento de datos, persiste la discusión en torno al proyecto de Ley que moderniza la legislación vigente y crea la Agencia Nacional de protección de datos. El proyecto de Ley sobre Protección de datos personales en discusión es el resultado de la refundición de dos iniciativas legislativas contenidas en los boletines 11.092-07 y 11.144-07¹³ en una sola iniciativa que regula la protección y el tratamiento de los datos personales junto a la creación de la Agencia de Protección de Datos Personales.

¿Cuáles son las motivaciones y objetivos del proyecto de ley?

Los antecedentes directos que fundamentan la relevancia de la iniciativa se vinculan a dos ejes principales. En primer término, se evidencian los cambios en las dinámicas sociales, avanzando rápidamente a la configuración de una sociedad digital en donde el tráfico de datos a través de internet se vuelve

¹¹ Para profundizar en la calidad de datos recopilados durante la crisis sanitaria y la postura de la "Mesa de datos" del Ministerio de Ciencias, revisar: <https://www.latercera.com/la-tercera-pm/noticia/a-la-mesa-de-datos-del-ministerio-de-ciencias-le-faltan-datos/PXKY76HAE5FWZKNHBXJ657QW2Y/> (Fecha de consulta: 19 de 04 de 2023).

¹² Reiterados hechos de discriminación para funcionarios de la salud por parte de vecinos en sus domicilios hacen pensar que el conocimiento de diagnósticos podría traer similares consecuencias. <https://www.24horas.cl/coronavirus/personal-medico-es-amedrentado-y-discriminado-por-vecinos-que-temen-contagio-de-coronavirus-4099296> (Fecha de consulta: 16 de 05 de 2023).

¹³ Trámite legislativo disponible en: <https://www.camara.cl/legislacion/ProyectosDeLey/tramitacion.aspx?prmID=11661&prmBoletin=11144-07> (Fecha de consulta: 19 de 04 de 2023).

sumamente importante. Por otra parte, las exigencias impuestas por organismos internacionales como la OCDE que invitan al país a modernizar y actualizar nuestro marco normativo con el fin de conectarnos con la economía globalizada siguiendo los estándares del primer mundo y explorando nuevos problemas en cuanto ciudadanos sujetos de derecho, así como el empleo y utilización de tecnologías para la realización de cuestiones cotidianas hasta acciones comerciales más complejas.

Los principios que sustentan la iniciativa, consisten en una novedad normativa puesto que otorgan mayor sustento a la normativa y reconocen dimensiones novedosas que la legislación actual no considera. Detalladamente son los siguientes:

- (a) **Licitud:** necesidad de consentimiento expreso o mandato legal para su tratamiento;
- (b) **Finalidad:** establece una exigencia triple de especificidad, licitud y explicitud para la recolección de datos;
- (c) **Proporcionalidad:** para limitar la recolección y el tratamiento a la información estrictamente necesaria para el cumplimiento de los determinados fines;
- (d) **Calidad:** datos deben ser actuales y precisos en relación a los fines del tratamiento;
- (e) **Responsabilidad:** para todos los que ejecuten el tratamiento de datos en conformidad con lo establecido en la presente Ley;
- (f) **Seguridad:** con el fin de garantizar niveles protección contra filtraciones, pérdidas, destrucción o daño accidental, tomando determinaciones técnicas preventivas;
- (g) **Información:** garantizando el accesible y rápido conocimiento sobre políticas y prácticas en el tratamiento de datos.

Los principios señalados con anterioridad no están reconocidos en los términos descritos por la legislación vigente por lo que esta iniciativa robustece no sólo en términos administrativos o declarativos la protección y el tratamiento de datos, sino que profundiza en el entendimiento de la materia a través de principios precisos, correctamente aplicados y con alcances debidamente definidos.

En función de los principios detallados, los principales títulos de la iniciativa parlamentaria pueden ser resumidos en el reconocimiento de derechos en favor de los titulares de los datos, la creación de una serie de procedimientos de reclamación a favor de los titulares de los datos, una regulación en el tratamiento de datos vinculados a obligaciones económicas, financieras, bancarias o comerciales, la estipulación de responsabilidades y encargados a la hora de la manipulación de datos, la seguridad de los datos personales, la reglamentación del tratamiento de datos por parte de organismos públicos y por último, las infracciones y sanciones por la inobservancia de lo establecido en la Ley sobre protección de datos personales. Las contribuciones de mayor notoriedad y que se relacionan con las materias analizadas a lo largo de este informe consisten en:

El reconocimiento de la titularidad sobre los datos personales por parte de su titular, junto a una elaboración mucho más acabada del concepto de "requisito" en materia de consentimiento. La creación de una categorización respecto a los datos personales y de una protección mucho más robusta sobre la información relativa a menores de edad. También son reconocidos los Derechos de Acceso, Rectificación, Cancelación, Oposición y Portabilidad, conocidos internacionalmente como derechos ARCO, nombre originado por las iniciales de cada una de estas garantías asociadas a la materia.

En cuanto la obligación del Estado de garantizar los Derechos previamente mencionados, la iniciativa crea la Agencia de Protección de Datos Personales con el fin de fiscalizar y sancionar las inobservancias a la legislación mediante penas pecuniarias por un máximo de 5.000 UTM, la creación junto a la agencia de protección, de un registro nacional de cumplimiento y sanciones junto a innovadores procedimientos para perseguir a responsables de infringir la Ley.

Finalmente, son establecidas obligaciones para los organismos responsables del procesamiento de datos, sean organismos públicos o privados, con el fin de adoptar medidas de seguridad y obligaciones de reporte frente a eventuales vulneraciones a las medidas de seguridad de los sitios, software, aplicaciones y bases de datos.

En anexo se adjunta un cuadro comparativo en donde serán graficados los cambios del proyecto en el transcurso de su tramitación constitucional en lo relativo al tratamiento de datos respecto a criterios como la creación de la categoría de dato personal sensible, tratamiento, datos relativos a la salud, comunicación o cesión de datos.

Conclusiones

Tal como lo ha manifestado la OCDE, resulta indiscutible que el paradigma jurídico chileno sobre protección y tratamiento de datos no sólo es obsoleto, sino que también es ineficaz. No deja de llamar la atención que, pese al vertiginoso desarrollo de la sociedad digital actual, la única Ley que se hace cargo de la protección y el tratamiento de datos sea del año 1999, como tampoco es intrascendente que la protección de datos personales como garantía constitucional haya sido posible recién en el año 2018. La necesidad de un marco normativo actualizado y mucho mejor diseñado podría eventualmente ser resuelto mediante la iniciativa legislativa tramitada desde el año 2017. Sin embargo, han transcurrido 6 años y sigue siendo discutida, por lo que pareciera ser que los compromisos internacionales asumidos por el Estado de Chile o una crisis sanitaria no son factores relevantes y suficientes para la modernización oportuna del régimen jurídico aplicable;

Y es que con lo descrito en el transcurso del año 2020 surgieron nuevas interrogantes respecto a la protección y tratamiento de datos en escenarios de excepción y la potestad de los organismos públicos para la ponderación de diversos bienes jurídicos como por ejemplo la salud o el orden público en contraste con la privacidad y la intimidad de la ciudadanía. En este nuevo contexto podemos evidenciar dos problemas fundamentales, la ausencia del reconocimiento de titularidad respecto a los datos personales y sensibles, como también, la carencia de normas que exigieran a nuestra institucionalidad una mayor prolijidad respecto a la información requerida y los procedimientos para tratarla.

Cuando nos referimos a la titularidad de datos, debemos entender que las y los ciudadanos poseen Derechos vinculados a los datos y en tal sentido, los organismos públicos deben promover y garantizar su reconocimiento, permitiendo superar la obsoleta noción de permisibilidad o denegación al momento de compartir nuestros datos. Esto es posible lograrlo con el reconocimiento de los derechos ARCO que precisamente son incluidos en el proyecto de ley que fue examinado con anterioridad. En el mismo sentido, también nos parece de extrema relevancia determinar correctamente los márgenes del debate, puesto que la acción de promover derechos respecto a la protección de datos personales y su tratamiento no implica que los datos sean una manifestación de propiedad y que el mercado pueda ingresar al debate mercantilizando las lógicas de los datos personales y sensibles.

En relación con el tratamiento de datos, se observa de la revisión de esta herramienta tecnológica del gobierno (Coronapp) y de la normativa vigente, la ausencia de directrices normativas que limiten y sirvan de guía a criterios de instituciones. Esto se vuelve problemático en razón de la eventual lesión a bienes jurídicos debidamente protegidos a nivel constitucional en el capítulo de garantías del artículo 19 numerales 4 y 5 al carecer de límites que determinen correctamente los alcances de la actividad Estatal.

En último caso y vinculado tanto a la titularidad como a la limitación de las facultades gubernamentales, la carencia de una institucionalidad que esté llamada a resolver problemáticas propias de la protección y el tratamiento de datos genera un vicio en la eficacia de cualquier atisbo de reconocimiento a la problemática de los datos sensibles puesto que, en caso de incumplimiento en materia de protección de datos, la ciudadanía no cuenta con procedimientos ni organismos a quien recurrir.

Es por lo anteriormente expuesto, que la promulgación de la iniciativa legislativa para la Protección y la creación de la Agencia de tratamiento de datos no sólo moderniza el orden jurídico aplicable, sino que también reconoce nuevos derechos que son respaldados por una institucionalidad fortalecida, y colabora en la determinación de fronteras y alcances para la ponderación de bienes jurídicos de relevancia en situaciones de normalidad y de excepcionalidad.

Anexo: Cuadro comparativo acerca de los cambios del proyecto en el transcurso de su tramitación constitucional (2017-2023).

Criterio	Mensaje Presidencial	Primer Trámite Constitucional	Segundo Trámite Constitucional
Categoría dato sensible	Son definidos los datos sensibles como los referidos a características físicas o morales como por ejemplo la afiliación política, identidad genética o estado de salud. (artículo 2, literal g)	Se modifica el artículo 2, literal alterando su tenor ejemplificador a taxativo.	Se modifica el carácter taxativo del artículo en comentario.
Tratamiento	Caracteriza el tratamiento de datos mencionando los posibles métodos para realizar la actividad.	Contempla el tratamiento para la totalidad de datos personales de cualquier tipo y agrega el conjunto de datos como objeto válido de tratamiento.	
Datos de salud	Se determina la exigencia normativa para su correcto tratamiento.	Incluye la misma exigencia para el perfil biológico humano.	
Comunicación de datos	Se estipula la exigencia para la cesión de datos condicionada a la autorización del titular.	Se establece una excepción a la exigencia, en el caso de que la comunicación de datos sea necesaria para el cumplimiento de funciones de la institución pública que fiscalice o inspeccione.	

Fuente: Elaboración propia