**Boletín N° 13.497-07**

**Proyecto de ley, iniciado en moción del Honorable Senador señor Harboe, que refuerza la protección de los datos sensibles de salud, durante cuarentena sanitaria o estado de excepción de catástrofe declarada por la autoridad.**

Para Byung- Chul Han uno de los rasgos más distintivo de la revolución digital consiste la supresión de toda distancia[1]. En efecto, comúnmente solemos escuchar que las redes sociales nos acercan a la información, que ésta circula a una velocidad sin precedentes, que se han derribado las distancias y las fronteras informativas. Sin embargo, lo anterior, no implica que estemos mas cerca o más lejos de la información, sino que simplemente ella "esta ahí", "disponible", "desnuda", frente a todos. Pero, más allá de estas reflexiones de este gran autor Surcoreano, lo cierto que la "ausencia de distancia" afecta, desde luego en nuestra vidas y en especial en nuestra privacidad, más aún en tiempos de crisis, como el que actualmente vivimos.

Pensemos un momento, que la propagación del COVID-19, ha significado, no sólo que se haya intensificado el uso de redes sociales o vías remotas como forma de comunicación, sino que la lucha contra el virus no sea exclusivamente biológica, sino que también sea informática, a través del tratamiento de miles de datos personales sensibles; de salud, hábitos, de localización, etc. China, Hungría, Turquía, Argentina, Italia, entre otras técnicas, están usando cámaras térmicas, de reconocimiento facial, drones que entregan medicamentos y el uso de IA para reconocer el avance de la pandemia caracterizando que grupos humanos son más o menos sensibles a contraer el virus, donde además, la "colaboración" internacional y el "uso" compartido de información es clave frente a esta enemigo planetario.

Pero, ¿que pasa con nuestra información?, ¿están nuestro datos realmente protegidos?, y más aún, en época donde se habla de personas infectadas, fichas clínicas, diagnósticos, ¿están nuestros datos de salud realmente protegido frente abusos indebidos?, ¿se tiene realmente conciencia sobre de la importancia que tiene esta información para los estados, empresas y para nosotros mismos?. La verdad es que no.

De hecho un reciente estudio de Tren Digital UC arrojó que el 60% de los encuestados estaría de acuerdo con que se rastreen los celulares de persona

[1] Chul –Han, Byun. (2017). La expulsión de lo distinto. Ed. Herder p. 16.

contagiadas[2]. En este contexto, la indubitada influencia de la tecnología sobre el derecho a la protección de datos personales, impone, por una parte, desafíos de cara a cómo enfrentar los nuevos fenómenos digitales, y por otra, que la autodeterminación informativa y los poderes de control sobre la información, deban estar en permanente revisión. El derecho a la protección de datos se halla bajo la amenaza de quedar rezagado frente a nuevas técnicas de tratamiento[3], en especial ante crisis con alcances globales, donde ya no existe distancia.

En este orden de cosas surge, y se reflota una vez más la discusión sobre la necesidad de reforzar el estatuto normativo protector de la privacidad y en especial de los datos denominados “sensibles”. En efecto, durante la actual crisis sanitaria por la que atraviesa el país, el uso, tratamiento y comunicación de datos sensibles, como datos clínicos, de salud, hábitos, geolocalización, datos de NNA, son absolutamente necesario no sólo para control de la pandemia, sino que encontrar como evitar futuras crisis sanitarias en el futuro. Es por ello, que resulta absolutamente necesario que tanto, los órganos de la administración del estado, como los responsables del tratamiento de datos de carácter privado, implemente los más altos estándares para protección de los datos sensibles, puesto que, mientras que por un lado, la actual ley 19.628 no posee mecanismos modernos de protección, por otro, ya está vigente en nuestro país la ley 21.096 que consagra el derecho a la protección de datos a nivel constitucional que al menos abre la puerta para un resguardo del derecho a través de la acción de protección.

Ahora bien, la actual ley 19.628 – en vigor- contempla alguna normas sobre la protección de los datos sensibles, que si bien revisten una importante utilidad, son absolutamente insuficientes para poder decir que en nuestro país estamos a la altura de los cuerpos normativos mas desarrollados.

Por lo pronto el artículo 2 letra g) nos da una definición, que enumera una categoría de datos que son considerados sensibles. A su turno, el artículo 7 del mismo cuerpo legal, indica que las “personas que trabajan en el tratamiento de datos personales en organismo públicos como privados están obligados a guardar

---

[2] El Mercurio, edición viernes 27 de marzo 2020. Cuerpo C7. Disponible en https://digital.elmercurio.com/2020/03/27/C/U33P57LU#zoom=page-width

[3] Abarca, S. (2018). *El tratamiento automatizado de datos como elemento definitorio del derecho a la protección de datos personales en el contexto europeo*. Seminario de titulación para obtener el grado de Magíster en Derecho PUCV.

secreto” , o si se quiere existe un deber de “resguardo” sobre ellos.  Con todo, el atávico problema de impractibilidad del ejercicio de los derechos consagrados en dicha ley, abre un manto de dudas, de cómo en la práctica los datos sensibles son tratados por órganos del estado y por responsables privados y cuales son realmente los estándares usados.

A mayor abundamiento, en virtud de la desanimada atribución que posee el CPLT en el artículo 33 letra m) de la ley 209.285, ha logrado sentar alguna jurisprudencia administrativa y dictar algunas norma infralegales como por ejemplo las “recomendaciones del Consejo para la Transparencia sobre protección de datos personales por parte de los Organismos de la Administración del Estado”, que sin duda han contribuido a la instalar dentro de la administración publica una incipiente cultura de cumplimiento normativo en materia de privacidad, pero aún lejos de un sistema de protección y tratamiento de datos robusto.

Por otra parte, los artículo 12, 13 y 21 de la ley 20.584 que regula los derecho y deberes que tienen las personas en relación con acciones vinculadas a su atención de salud, no provee la suficiente protección en lo referido al tratamiento de los datos sensibles de salud, puesto que por una parte reconduce la protección de la información contenida en la ficha clínica a la ley 19.628, que como hemos visto no posee mecanismo de protección, y por otra, el mecanismo de cumplimiento de la ley 20.584 consiste en un procedimiento reclamo, según el artículo 37, ante el propio prestador institucional lo que a todas luces es insuficiente como mecanismo de resguardo de la información sensibles concerniente a sus titulares.

Así las cosas, en nuestro país aún  está en trámite en el Senado de la República, el proyecto de ley 11.092-07 11.144-07[4] ( en adelante “el proyecto”) que moderniza  el ordenamiento jurídico en materia de protección de datos, estableciendo catálogo de definiciones, principios, procedimientos sancionatorio, sanciones, entre otras cosas, y enviste al CPLT como máxima autoridad administrativa en materia de protección de datos con facultades normativas, interpretativas y fiscalizadoras. Lo anterior, sin duda constituye un avance sustantivo y transformador. Sin embargo, conforme la crisis sanitaria avanza, el tratamiento y procesamiento de datos sensibles (sobre todo de salud) se torna

[4] Disponible en: http://www.senado.cl/appsenado/templates/tramitacion/index.php?boletin_ini=11092-07

absolutamente necesario, siendo incluso un tema, literalmente de vida o muerte. Es por esta razón que urge, como un imperativo democrático, reforzar los mecanismos de protección de la información concerniente a las personas, sobre todo cuando corresponden a ámbitos sensibles como la salud circunscrito en una momento tan sensible como el que hoy vivimos

El proyecto al cual hemos hecho referencia contempla normas muy avanzadas y en total sintonía con le RGPD (Reglamento General de Protección de Datos europeo). En este orden de cosas, el proyecto logra establecer que dato sensible es una categoría especial de datos personales y que está referido a toda aquella información que permita revelar el origen étnico o racial; filiación política, sindical o gremial; convicciones ideológicas o filosóficas; creencias religiosas; datos relativos a la salud; al perfil biológico humano; datos biométricos, e información concerniente a la vida sexual, orientación sexual, a la identidad de género y a los hábitos personales, información que por su especial naturaleza, merece una protección más intensa por el ordenamiento jurídico toda vez que su tratamiento desleal, malicioso, o mal uso puede "dañar" de manera más intensa la dignidad de la persona.

Es por esta razón que el mencionado proyecto señala que los datos sensibles de salud de datos se hará siempre con el consentimiento expreso del titular, salvo, -entre otras hipótesis-", cuando el tratamiento de los datos personales del titular resulte indispensable para salvaguardar la vida, salud o integridad física o psíquica del titular o de otra persona o, cuando el titular se encuentre física o jurídicamente impedido de otorgar su consentimiento". La diferencia de esta norma del proyecto con el ordenamiento en vigor hoy, dice relación con que se refuerza el rol del consentimiento del titular como fuente de licitud, pero a su vez, permite el tratamiento sin consentimiento en hipótesis bien definidas y graves con absoluto apego a los principios de legalidad, finalidad, buena fe, licitud, cuya infracción que trae aparejada fuertes sanciones de multas. Lo mismo, ocurrirá con el tratamiento de datos biométricos, donde además se elevan lo niveles de información que deben darse al titular del dato.

El tratamiento de información sensible es clave para el resguardo y protección de la salud, más aún, "la protección de datos no debería utilizarse para obstaculizar o limitar la efectividad de las medidas que adopten las autoridades"[5], pero debe

[5] Disponible en: https://www.aepd.es/es/prensa-y-comunicacion/notas-de-prensa/la-aepd-publica-un-informe-sobre-los-tratamientos-de-datos-en

hacerse respetando la dignidad de las personas, pues, ni aún bajo un estado de catástrofe o cuarentena sanitaria, se podría afectar el derecho a la protección de datos (incluidos de salud), idea que ha sido reafirmada por la AEPD (Agencia Española de Protección de Datos) al señalar "*para el tratamiento de datos de salud no basta con que exista una base jurídica del art. 6 RGPD, sino que de acuerdo con el art. 9.1 y 9.2 RGPD exista una circunstancia que levante la prohibición de tratamiento de dicha categoría especial de datos (entre ellos, datos de salud*)"[6]. En este mismo sentido el CPLT en su Recomendación contenida en el Oficio 211 de fecha 17 de marzo de 2020, ha sido enfático al señalar que "*los planes, políticas, programas y acciones que la autoridad competente adopte, en respuesta a la pandemia del COVID-19, y que implican el tratamiento de datos personales, inclusos los datos sensibles de salud, deben ser necesarias y proporcionales*"[7].

En efecto, en nuestro país de acuerdo a la CPR, por la declaración de estado de catástrofe el Presidente sólo podrá restringir las libertades de locomoción, de reunión y establecer limitaciones al derecho de propiedad, pero bajo ningún respecto podría establecer restricciones que afectaran el derecho a la protección de datos personales.

Conforme a los anterior, existe una clara asimetría entre las técnicas usadas para combatir la pandemia y el estatuto protector de los ciudadanos. Protección que no puede ser entendida como un óbice para las acciones sanitarias que despliegue la autoridad, por el contrario, las medidas tecnológicas que supongan tratamiento de datos están autorizadas por el ordenamiento y la pandemia constituye base jurídica suficiente para el tratamiento de datos sensibles, puesto que configuran una amenaza y afectación clara de la vida y salud humana, pero éstas acciones deben; estar diseñadas desde la privacidad (es lo que se conoce como Privacy by design), considerar las mayores medidas de seguridad posibles para evitar "fugas" de información, contener información clara y precisa acerca de los fines para los cuales se ha recogido los información, entre otras.

Debemos tener conciencia de que el tratamiento de datos de salud para el combate de la pandemia mundial del COVID-19, puede y debe estar en sintonía

---

[6] Informe jurídico 0017/2020 AEPD. Disponible en: https://www.aepd.es/es/documento/2020-0017.pdf

[7] Recomendación Oficio nº 211. CPLT. Disponible https://www.consejotransparencia.cl/wp-content/uploads/2020/03/recomendaciones-COVID19.pdf

con el ejercicio de nuestros garantías fundamentales, en especial con el derecho que nos asiste a tener control sobre la información que nos concierne. No es posible y constituye una muy mala señal, que bajo la consigna “la emergencia lo requiere,” los datos de salud se recojan, traten, vayan y vengan de un tratador a otro, sin un control flujo, sin conocer el nivel de adecuación de los receptores de información en un esquema de cooperación internacional, etc.

Es por esta razón que resulta absolutamente indispensable la existencia de medidas legislativas urgentes que permitan un uso correcto y adecuado de los datos personales sensibles de salud, y evitar que ellos terminen en manos de compañías aseguradas, laboratorios farmacéuticos o empresas de publicidad, y por el contrario, jueguen un rol fundamental para la superación de la crisis sanitaria. Tal y como se ha señalado en el RGPD “este tratamiento de datos relativos a la salud por razones de interés público no debe dar lugar a que terceros, como empresarios, compañías de seguros o entidades bancarias, traten los datos personales con otros fines.” (Cº 54)[8]

Conforme a lo anterior, la presente moción busca fijar normas y estándares altos en materia de tratamiento de datos sensibles, sobre todo los de salud, en época de crisis sanitaria.

**Proyecto de ley**

Artículo único

“Declarada una cuarentena sanitaria o un estado de excepción constitucional por calamidad pública que signifique grave riesgo para la salud o vida de las personas, el tratamiento de datos personales sensibles, en especial datos sensibles de salud, incluidos el perfil biológico, datos genéticos, protéomicos o metabólicos y datos biométricos, está sujeto a las siguientes reglas:

a) El tratamiento de los datos personales sensibles de salud sólo puede realizarse cuando el titular a quien conciernen estos datos manifiesta su consentimiento en forma expresa, otorgado a través de una declaración escrita, verbal o por un medio tecnológico equivalente**.**

[8] Disponible en https://www.boe.es/doue/2016/119/L00001-00088.pdf

b) No se requerirá consentimiento del titular del tratamiento, en casos de urgencia sanitaria legalmente decretada o cuando éste resulte indispensable para salvaguardar la salud, vida o integridad física o psíquica del titular o de otra persona o, cuando el titular se encuentre física o jurídicamente impedido de otorgar su consentimiento. En este último caso, una vez que cese el impedimento, el responsable debe informar detalladamente al titular los datos que fueron tratados y las operaciones específicas de tratamiento que fueron realizadas.

c) El tratamiento de los datos sensibles de salud, deberá estar limitado por finalidad sanitaria prevista en la declaración de cuarentena sanitaria o declaración de estado de catástrofe, ajustándose a aquellos datos estrictamente necesarios para la consecución de dichos fines, debiendo los datos ser exactos completos y actuales y proporcionando toda la información sobre el tratamiento de manera oportuna, clara y transparente.

d) En el tratamiento de los datos personales sensibles de salud, el responsable debe garantizar estándares adecuados de seguridad, protegiéndolos contra el tratamiento no autorizado o ilícito, y contra su pérdida, filtración, daño accidental o destrucción.

e) El que, durante una cuarentena sanitaria o un estado de excepción constitucional por calamidad pública que signifique grave riesgo para la salud o vida de las personas trate , comunique o ceda, a sabiendas, datos personales sensibles de salud sin tener base jurídica para dicho tratamiento, o que teniéndola no se ajuste a la finalidad del tratamiento, o no adopte las máximas medidas de seguridad para evitar el tratamiento ilícito, pérdida, filtración o daño, será sancionado con multa de 5.001 a 10.000 unidades tributarias mensuales, sin perjuicio de la responsabilidad prevista en el artículo 23 de la ley nº 19.628.

f) En las transferencia internacionales de datos sensibles de salud que sea realicen en el marco de la protección o cooperación sanitaria internacional para el combate de la pandemia del covid-19, la autoridad sanitaria deber cerciorarse que se realice a una persona, entidad u organización pública o privada, sujeta al ordenamiento jurídico de un país que proporcione niveles adecuados de protección de datos personales o que la transferencia está

amparada en un tratado, convención, u otro instrumento internacional ratificado por Chile y que se encuentren vigente, o amparada por cláusulas contractuales u otros instrumentos que contenga normas sobre derechos y garantías deberes de los titulares y obligaciones de los responsables, o cuando el responsable que reciba la transferencia haya adoptado modelos de cumplimiento o autorregulación, debidamente certificados y que garanticen la seguridad de los datos, o cuando la transferencia haya sido autorizada por el titular del dato.

g) Los titulares de datos sensibles de salud siempre podrán ejercer los derechos previstos en el título II de la ley nº 19.628 sobre protección de la vida privada.

h) En lo no previsto en esta ley se estará a lo dispuesto en la ley nº 19.628 sobre protección de la vida privada y nº 20.584 sobre derecho y deberes que tienen las personas en relación con acciones vinculadas a su atención de salud, en lo que corresponda.”