¿Proyecto de protección de datos personales en Chile cumple con estándar de la UE?

Expertos, parlamentarios y Gobierno difieren sobre si la autonomía de la futura Agencia de Protección de Datos se alineará a las exigencias del bloque europeo.

LUCY ARAVENA L.

—Uno de los proyectos de ley que ha sido fijado como prioritario para la última etapa del actual Gobierno ha sido el que establece la protección de los datos personales. La iniciativa se encuentra en la Comisión de Constitución del Senado y las expectativas es que sea despachado al menos de la Cámara Alta antes de la administración de Michelle Bachelet concluya.

Y si bien existe coincidencia entre los expertos en que el proyecto de ley es un avance con respecto a la legislación vigente y cumple con los estándares de la OCDE, no existe la misma concordancia en cuanto sí cumple con las exigencias de la Unión Europea (UE), bloque comercial y de intercambio de información importante para el país, lo que ha abierto un nuevo debate en torno a la iniciativa.

Europa es el continente donde la protección de datos ha alcanzado un nivel más elevado. Esto porque dentro de la UE se prohíbe la transferencia de datos a países que no cuenten con un nivel adecuado de protección y establece un procedimiento para determinar formalmente si un país ofrece o no ese nivel. En ese sentido, la independencia de la autoridad encargada de la protección de datos se considera como un rasgo indispensable y, por ende, como una exigencia clave de la UE.

La principal consecuencia de que un país sea declarado adecuado por el bloque comercial es que se podrán transferir datos desde los Estados miembros sin necesidad de ningún tipo de trámite o autorización especial (ver listado). De ahí, la importancia de que Chile cumpla con este estándar. Hoy a nivel global sólo 10 países cumplen con el estándar de la Unión Europea. (Ver tabla)

DEBATE. Por un lado, varios expertos han sostenido que el proyecto de ley aún no garantiza la plena independencia de la Agencia de Protección de Datos, autoridad creada para resguardar este derecho, de otros poderes del Estado. Y es que esta nueva institucionalidad estará situada bajo el paraguas y financiamiento del Ministerio de Hacienda, lo que le restaría independencia. Sin embargo, los para los parlamentarios que siguen de cerca este proyecto, el actual diseño de la agencia sí cumple los requisitos tanto de la OCDE como de la Unión Europea.

Por esta razón, tanto para los legisladores como para el Gobierno que están trabajando en los ajustes que tendrá la iniciativa, la autonomía se puede garantizar de otras formas en que más importante sea que la Agencia no tenga que rendir cuentas a Hacienda. Así, al interior de la Comisión se está comenzado a revisar justamente la institucionalidad de la Agencia y la idea es que sea parecida a la que tiene la Unidad de Análisis Financiero, que también depende de Teatinos 120.

Uno de los principales actores que ha cuestionado la institucionalidad ha sido el presidente del Consejo para la Transparencia, Marcelo Drago, quien ha sostenido que "no me explico por qué se insiste en un sistema que es una dependencia del Ministerio de Hacienda, sin ningún grado de autonomía jerárquica. Se habla de autonomía técnica, pero en el momento en que la jefatura de la Agencia tenga que rendirle cuentas a algún superior de la cartera, no es autónoma" Mientras, el presidente del Instituto Chileno de Derecho y Tecnologías, Raúl Arrieta, también ha expresado que "en el articulado que está propuesto se debe excluir lo que tiene que ver con la supervigilancia del Ministerio de Hacienda". Para la presidenta de la Fundación Datos Protegidos, Romina Garrido, la Agencia debería tener un mayor grado de autonomía, lo cual también haría que esta institucionalidad pueda sancionar la infracción relacionada con la protección de datos tanto de los privados como de los organismos públicos, lo cual no ocurre en el proyecto de ley.

Presentación El Ejecutivo definió el tipo de institucionalidad al ingresar el proyecto.

Preguntas clave

¿A qué se le llama un dato personal?

Es cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo que identifique o puede hacer indentificable a una persona. En ese sentido, el espectro es amplio. El dato personal puede ser relativa a la identidad propiamente tal, como los nombres, domicilio, e-mail, una fotografía o video de un individuo, como también puede ser respecto de sus preferencias u ocupaciones, como sus estudios, trabajo o aficiones.

¿A qué se le llama un dato sensible?

Es aquella información personal que revela el origen racial o étnico, opiniones políticas, convicciones religiosas o morales, afiliación sindical, información referente a la salud y vida sexual o cualquier otro dato que pueda producir, por su naturaleza y su contexto, algún trato discriminatorio al titular de los datos personales. Por ejemplo, los antecedentes clínicos que se traspasan a las isapres y a las farmacias es un tráfico no apropiado de este tipo de dato.

¿De que se encargará la Agencia de Protección de Datos?

Tal como su nombre lo dice, esta institucionalidad estará encargada de fiscalizar que los privados respeten el derecho de protección de datos personales y no hagan mal tratamiento o traspaso de esta información de las personas. Asimismo, esta Agencia deberá sancionar a las empresas que infrinjan esta legislación con multas y otros castigos. La Agencia será una institucionalidad situada bajo el paraguas del Ministerio de Hacienda.

CONTENIDO MULTIPLATAFORMA
www.pulso.cl
Vea más información en www.pulso.cl y/o en aplicaciones móviles.

PAÍSES CON AUTORIDAD DE PROTECCIÓN DE DATOS

EUROPA	
Albania	
Alemania	
Andorra	●
Austria	
Bélgica	
Bosnia y Herzegovina	
Bulgaria	
Chipre	
Croacia	
Dinamarca	
Eslovaquia	
Eslovenia	
España	●●
Estonia	
Finlandia	
Francia	●●
Grecia	
Guernsey	●
Hungría	
Irlanda	
Islandia	
Italia	
Islas Feroe	●
Letonia	
Liechtenstein	
Lituania	
Luxemburgo	
Malta	
Moldavia	
Mónaco	
Noruega	
Países Bajos	
Polonia	
Portugal	● / ●●
Reino Unido	● / ●●●
República Checa	
Rumanía	
Serbia	
Suecia	●
Suiza	
ÁFRICA	
Burkina Faso	
Marruecos	
Mauricio	
Senegal	
Túnez	
Israel	●
AMÉRICA	
Argentina	●●
Colombia	●●
Costa Rica	●●
E.E.U.U.	
México	●●●
Perú	
Uruguay	● /●●
Canada	● /●●●
ASIA	
Hong Kong	
Israel	
Korea del Sur	
OCEANÍA	
Australia	
Nueva Zelanda	● /●●

● Países que pueden comercializar directamente con Unión Europea
●● Países con agencia autónoma de datos personales
●●● Países con agencia de protección de datos y transparencia
Fuente: Datos Protegidos

Propuestas de la ONG Datos Protegidos

1 Amplitud de acción de protección de datos

La ley de datos debe ser general y aplicarse de manera supletoria a otros tratamientos regulados por leyes especiales. Ejemplo: datos en salud, telecomunicaciones, tránsito, entre otras materias.
La definición de datos sensibles debe ser amplia y no cerrada a determinada categoría de datos, dado que un dato puede llegar a ser sensible si su tratamiento da origen a una discriminación arbitraria o ilegal o conlleve un grave riesgo para su titular.

2 Principio de temporalidad y de responsabilidad

El principio de proporcionalidad debe perfeccionarse con una "minización de datos", es decir, establecer que se soliciten sólo los datos pertinentes al objetivo que se busca. Se debe contemplar el principio de temporalidad, el cual significa que el tratamiento de los datos no puede ser indefinido en el tiempo.
Debe imponerse al responsable del tratamiento de los datos el deber de comprobar que ha cumplido con las obligaciones legales y no sobre el titular.

3 El deber de reportar posibles riesgos y de confidencialidad

El deber de secreto o confidencialidad debe mantenerse aún después de cesar las actividades de tratamiento por parte del responsable o sus dependientes de manera indefinida.
En cuanto al deber de reportar las vulneraciones a las medidas de seguridad que pesa sobre los responsables, el proyecto debiera contemplar que esta notificación a los titulares se lleve a cabo siempre que exista un riesgo y no acotarlo a la vulneración de un dato sensible.

4 Casos sobre la salud

Una de las excepciones que contempla el proyecto para requerir el consentimiento por parte del titular de los datos, tiene lugar "cuando resulte indispensable para el cumplimiento de un contrato cuya finalidad exija tratar datos relativos a la salud del titular." La norma debe referirse específicamente al tratamiento de una prestación de salud y no en otros contratos. Lo anterior puede dar lugar, por ejemplo, a que un contrato bancario exija el tratamiento de datos de salud.