Desafíos urgentes para una protección efectiva de datos personales

Regulaciones sobre el sector público y privado en defensa de la ciudadanía

Por Fundación Vía Libre
Beatriz Busaniche y Margarita Trovato

Fundación Vía Libre
Fundación Avina
HEINRICH BÖLL STIFTUNG

En el marco de los recientes debates sobre una actualización de la legislación de protección de datos personales para Argentina, desde Fundación Vía Libre entendemos prioritarios al menos dos temas que tienen que ver con la actuación y el modelo de negocios del sector privado así como con la responsabilidad y las acciones del sector público.

Un cambio de paradigma en protección de datos supone una legislación que apunte a proteger los derechos de las personas en relación a sus datos y no el dato en sí como objeto específico. En esa línea, consideramos indispensable que cualquier actualización de la norma de protección de datos preste especial atención a dos temas: los derechos de las personas sobre los datos inferidos y la seguridad de la información en manos del Estado. A esos dos asuntos damos prioridad en el presente artículo.

> La urgente necesidad de **velar por los derechos** de las personas sobre los datos inferidos

Hoy los datos no sólo se recolectan y almacenan, también se infieren. En un mundo donde los modelos económicos de Internet se basan en la recolección, procesamiento y generación de grandes volúmenes de datos, deviene fundamental pensar en la protección de las personas en el marco de esos procesos, especialmente si consideramos que el procesamiento suele ser masivo, continuo, automatizado y cada vez más complejo y opaco.

Decisiones de actores públicos y privados que nos afectan ya no se basan exclusivamente en datos personales que brindamos sino también que se construyen mediante modelos inferenciales -aunque generalmente no lo sepamos y por lo tanto no podamos discutirlo- **y afectan un gran abanico de derechos humanos**, desde la privacidad hasta la autonomía y potencialmente la integridad física y mental.

Así, cuando hablamos de **datos inferidos, *nos referimos a aquellos que refieren a un individuo identificado o identificable pero que no son provistos por el titular*** (ni pasiva ni activamente), quien de hecho generalmente no conoce siquiera su existencia[1]. En cambio, esta información es creada por el responsable del tratamiento o por terceros a través del análisis de grandes volúmenes de datos (big data analytics): no se desprenden de la mera observación, sino que *se producen a través de alguna "operación intelectual"*, como la deducción, comparación, razonamiento -entre otras- que generalmente se implementa de forma automatizada y se utilizan luego para construir perfiles y predecir comportamientos.

En este contexto, **es indispensable brindar protección jurídica y mecanismos de salvaguarda** no sólo a los datos que cedemos sino -y especialmente- a aquellos que se construyen sobre nosotros sin nuestro consentimiento ni, en muchos casos, siquiera conocimiento.

[1] La doctrina y la jurisprudencia internacionales no brindan una definición unívoca. La que presentamos aquí es referida por Wachter, S. and Mittelstadt, B. "A right to reasonable inferences: Re-thinking data protection law in the age of big data and AI", en *Columbia Business Law Review* (2019), p. 23; y por Holder, A. E., "What We Don't Know They Know: What To Do About Inferences in European and California Data Protection Law", 2020, p. 5. Tanto para un tratamiento más extenso del concepto de "datos inferidos" como para una profundización general sobre los temas abordados en este artículo, nos remitimos al informe "Protección legal de datos personales inferidos" publicado por la Fundación Vía Libre en mayo de 2023, disponible en el siguiente link

> Algunos **problemas propios de la producción y el uso** de datos inferidos

Los datos inferidos tienen, por su propia naturaleza y forma de producción, una serie de aspectos problemáticos que deben ser tenidos en cuenta y abordados a la hora de legislar. En primer lugar, **son producidos sin consentimiento adecuado y generalmente sin conocimiento de los titulares.** A su vez, en estas mismas condiciones, son agrupados por determinadas características. En base a esa pertenencia se inferirán nuevos datos. Así, indefectiblemente por su propia naturaleza y forma de producción, los datos inferidos son información subjetiva (no observada) y no verificable (estimaciones probabilísticas), aunque las decisiones que fundamentan tienen efecto certero. La construcción suele hacerse en base a correlaciones poco intuitivas y no necesariamente causales -especialmente cuando se hace de forma automatizada sin razonamiento humano-, por lo que suele resultar sesgada, inexacta, discriminatoria. Además, se almacenan en registros persistentes que el titular no conoce ni tiene cómo discutir su veracidad.

Este escenario empeora cuando consideramos que hoy en día los procesos de construcción de estos datos no están regulados de forma clara: no hay obligaciones para los responsables del tratamiento de justificar el análisis que se hace ni de transparentar las técnicas que se aplican para obtener información que será luego la base de decisiones esenciales para la vida de las personas, con impacto directo en términos de derechos humanos.

Los datos inferidos son datos personales, en tanto tratan a sujetos identificados o identificables y se usan para tomar decisiones sobre ellos.

> Sobre la **urgente necesidad de regularlos**. Algunos puntos mínimos para una nueva legislación.

Así, en función de los riesgos que presenta su construcción y su uso en términos de derechos humanos, se vuelve indispensable dotarlos de un conjunto de derechos y garantías suficientes- que hoy no existen.

En nuestro país, la ley actual está desactualizada y resulta incompleta frente al avance de las tecnologías, en particular teniendo en cuenta la reciente ratificación del Convenio 108+, cuya entrada en vigor implica la obligación para Argentina de adecuar su normativa interna.

Para garantizar una protección suficiente y adecuada, es fundamental recordar que los datos inferidos son un tipo de datos personales, y por lo tanto **deben ser contemplados jurídicamente como tales: refieren directamente a individuos identificados/identificables** y las decisiones basadas en ellos pueden afectar gravemente sus derechos básicos. Suelen ser escuchados en contra de esta categorización algunos argumentos tales como que no son cedidos por su titular o que no refieren a información confirmada. Sin embargo, estas condiciones no hacen más que reafirmar la urgencia de protegerlos jurídicamente. También es frecuente la afirmación de que una regulación de este tipo sería contraria al secreto comercial que reviste al algoritmo que se utiliza para producirlos. En este punto vale aclarar, por un lado, que proteger los datos y establecer mecanismos de rendición de cuentas **no implica exponer secretos industriales**, y, por otro, que en cualquier caso **los derechos personalísimos** (ej. privacidad, autodeterminación) priman sobre los patrimoniales

(propiedad intelectual), por lo que de ninguna forma debería ser óbice para su protección.

De hecho, los marcos regulatorios de otras regiones avanzan en ese sentido: a modo de ejemplo, California y Australia los contemplan como datos personales expresamente, mientras que China y la Unión Europea no los excluyen. De hecho, son cada vez más las interpretaciones protectorias en este sentido[2].

De esta manera, sobre la base de la necesidad urgente de brindarles un marco de protección jurídica con perspectiva de derechos humanos, proponemos tres puntos básicos que deben ser tenidos en cuenta a la hora de legislar.

1. Explicitar que **los datos inferidos son datos personales, es decir que les cabe el mismo paraguas de protección jurídica**. Esto incluye, de mínima, los derechos clásicos conocidos como ARCO (acceso, rectificación, cancelación, oposición) y las condiciones para su ejercicio, como por ejemplo establecer mecanismos de rendición de cuentas, clarificar las reglas del consentimiento y la carga de la prueba, entre otras.

2. En función de esta protección, **limitar el proceso de construcción y el uso de los datos inferidos**, más allá del resultado inmediato en términos de perjuicios o daño que generen. Esto incluye, por ejemplo, prohibir aquellas producidas mediante procesos que no puedan ser explicados acabada y suficientemente,

3. **Contemplar y promover una autoridad de aplicación fuerte**, con autonomía funcional y presupuesto suficiente. Este punto es particularmente relevante por dos cuestiones: por un lado, en tanto la producción y uso de estos datos es la base de un modelo de negocios y de políticas estatales; por otro, por la dimensión colectiva de la privacidad que implica la masividad con la que se producen y el hecho de que muchas veces se deriven de la supuesta pertenencia a grupos con características determinadas. En esos casos los derechos individuales se vuelven más difusos y la acumulación de demandas individuales no tiene el mismo efecto.

> La **seguridad de la información** como deber inalienable del Estado

El Estado no es una entidad unívoca. No sólo existen diversos poderes del Estado, sino Estados de distinto nivel, desde la Nación hasta el último de los municipios. Todos estos diversos rostros del Estado dialogan con la ciudadanía de formas propias y cada uno recolecta y administra datos de la ciudadanía a todo nivel.

Desde el sistema de registro nacional de las personas representado por el RENAPER hasta la Justicia que se ocupa de dirimir conflictos en todos los ámbitos, desde civil a penal, pasando por una disputa familiar por alimentos hasta la persecución penal por un delito. Pero también el municipio cuenta con datos catastrales y registros de nuestra vida cotidiana, cámaras de vigilancia del espacio público o registros escolares. **La cantidad y calidad de los datos que recopila el Estado es notable**, y en muchos casos incluye datos filiatorios, familiares, de salud, patrimoniales, datos de nuestra

[2] Para más información sobre los marcos normativos de otras regiones o países y sus respectivas interpretaciones judiciales, ver el cap. 4 del informe antes citado.

intimidad, y una larguísima sumatoria de momentos en los cuales el Estado captura y almacena información. Vale una mención especial al hecho de que no tenemos opciones frente a la entrega de datos al Estado. En la mayoría de los casos, está lejos de ser opcional, libre o planificada.

Aún así, **deberían regir fuertes límites en la legalidad de la recolección y tratamiento de esa información**, partiendo del consentimiento informado e incluyendo las reglas para ser compartidos entre dependencias del mismo Estado. Sin embargo, la legislación vigente es endeble y presenta lagunas en estos puntos, como iremos viendo.

Llegados a este punto y sabiendo que muchos de los temas vinculados al consentimiento y la cesión de datos al interior del Estado no son temas resueltos ni pacíficos, elegimos aquí dedicar unas palabras a uno de los deberes fundamentales en torno a la garantía del derecho a la privacidad de las personas: nos referimos a la seguridad de la información que el Estado legítimamente puede poseer y tratar.

A la fecha, la ley 25.326 plantea una obligación al respecto: por un lado, su art. 9 obliga al responsable o usuario del archivo de datos a "adoptar las medidas técnicas y organizativas que resulten necesarias para garantizar la seguridad y confidencialidad de los datos personales, de modo de evitar su adulteración, pérdida, consulta o tratamiento no autorizado, 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", a la vez que prohíbe registrar datos personales en registros que no reúnan las condiciones técnicas mínimas de integridad y seguridad.

Seguidamente **establece el secreto profesional de quienes intervengan** en cualquier fase del tratamiento de datos personales sobre éstos -incluso una vez terminada su relación laboral-, que sólo podrá ser relevado por resolución judicial o cuando existan razones fundadas vinculadas con "la seguridad pública, la defensa nacional o la salud pública" (art. 10).

La cuestión de las medidas adoptadas para la seguridad es tan importante que incluso es parte de la información que se debe aportar al inscribir un registro, archivo, base o banco de datos, sea público o privado (art. 21). Sin embargo, la ley en su formulación actual no contempla los incidentes de seguridad de los datos ni cómo proceder ante ellos, cuestión sumamente relevante en contexto de avance tecnológico permanente en el que vivimos[3].

Es fundamental entender el escenario: los incidentes de seguridad, tales como "data breaches" (fugas de información) crecieron en los últimos años, en parte como respuesta a "múltiples factores propios de la industria de procesamiento de datos: la capacidad técnica para procesar datos de manera ilegítima evoluciona con la misma potencia de la capacidad de procesamiento legítimo"[4].

A este aumento objetivo se le suma **la frecuente subestimación** a nivel general. Es que socialmente suele ser difícil la comprensión de lo que pueden significar estos incidentes en términos de derechos y vulneración a la privacidad. Explica la doctrina que "el foco de dicha actividad son por lo general datos calificados como críticos o sensibles e información calificada para la organización víctima del incidente. La pérdida de esos datos por lo general conduce a su utilización para llevar

[3] Si bien no ahondaremos en este informe en las vulnerabilidades en sí mismas, remitimos en este punto al informe específico elaborado en 2022 por la Fundación Vía Libre junto con Democracia en Red y O.D.I.A., "Panorama general sobre la seguridad de la información, las vulnerabilidades y los incidentes en Argentina" donde nos referimos los distintos tipos de vulnerabilidades, cómo y qué derechos afectan, y la situación de los reportes. Está disponible para su descarga en https://datosenfuga.org.
[4] Faliero, J. C., *La protección de datos personales*, Ed. Ad-Hoc, Buenos Aires, 2019, p. 171

adelante actividades delictivas, tales como fraude financiero, robo de identidad, afectaciones a la propiedad intelectual, espionaje e inteligencia, extorsión, etcétera. Dada la cotidianidad de la ocurrencia de este fenómeno, los individuos se han vuelto progresivamente indiferentes a su existencia (...) Esta progresiva indiferencia a la severidad y trascendencia que poseen los incidentes de seguridad se debe en parte a la pérdida progresiva y relajamiento en la noción y percepción de la privacidad e intimidad personal"[5].

La responsabilidad del Estado debe ir mucho más allá de esta incomprensión en la que no puede amparar ningún acto negligente. Si contemplamos que además la ley no prevé cursos de acción frente a los incidentes, el escenario es aún más complejo.

La legislación comparada (el RGPD, por ejemplo) obliga, en caso de vulneración, a un informe que dé cuenta del hecho a la autoridad de control y, en algunos supuestos, a los titulares de los datos. En este sentido, en parte subsanando las lagunas legales, la Dirección Nacional de Protección de Datos Personales y la Agencia de Acceso a la Información Pública emitieron diversas disposiciones sobre el tratamiento y conservación de datos personales y las respectivas medidas de seguridad. En particular, la AAIP estableció mediante su resolución 471 del 2019 las "Medidas de seguridad recomendadas para el tratamiento y conservación de los datos personales en medios informatizados". Si bien se trata únicamente de disposiciones enunciativas ("recomendaciones"), establece pautas para a) la recolección de datos, b) el control de acceso, c) el control de cambios, d) el respaldo y la recuperación, e) la gestión de vulnerabilidades, f) la destrucción de la información, g) los incidentes de seguridad -donde corresponde elaborar un informe y enviar la notificación correspondiente a la autoridad de aplicación-, y h) para la definición de los entornos de desarrollo de los sistemas de información. Aún así, en estas acciones meramente declarativas no existen los recursos apropiados para la mitigación de esos incidentes.

Las filtraciones de datos personales de la ciudadanía que sufrieron diversas reparticiones del Estado en el último tiempo nos permiten asegurar que **sus sistemas son vulnerables.** Dado el uso abusivo de las excepciones que permite la ley en estos asuntos hasta el punto de desnaturalizarla, y la pobreza de las respuestas estatales -incluyendo las judiciales, hasta el momento- a los incidentes graves reportados en los últimos años, se torna urgente integrar un capítulo riguroso que exija medidas de seguridad efectivas y actualizadas, así como mecanismos apropiados de reparación de potenciales daños. Para ello debe dotar a la autoridad de aplicación de capacidades técnicas y legales para hacer cumplir a todos los estamentos del Estado su obligación de respeto y protección a ultranza de los derechos fundamentales de la ciudadanía.

[5] Faliero, J. C., Op. Cit. p. 168.