

Ciudad Autónoma de Buenos Aires, 20 de mayo de 2024

A la Comisión de Legislación Penal,

Presidenta, Dip. Laura Rodríguez Machado

Vicepresidente 1º, Dip. Mariano Campero

A la Comisión de Seguridad Interior,

Presidente, Dip. José Nuñez

Vicepresidente 1º, Dip. José Glinski

De la Honorable Cámara de Diputados del Congreso de la Nación

S _____ / _____ D

**Ref.: Mensaje PEN 17/2024 - Proyecto de Ley tendiente a modificar la Ley
Nº 26.879 “Registro de Datos Genéticos”**

Por medio de la presente nos dirigimos desde la **Fundación Vía Libre** para acercar a los Diputados y las Diputadas argumentos técnicos y de derecho sobre las cuestiones que se discuten en el proyecto de referencia.

La Fundación Vía Libre es una organización que trabaja hace más de veinte años en la intersección entre tecnología y derechos humanos: promueve y defiende derechos fundamentales en entornos mediados por tecnologías de información y comunicación. En relación con los temas que aquí interesan, tiene una amplia trayectoria en **protección de datos personales y autodeterminación informacional, privacidad, seguridad de la información y vigilancia**, tal como lo demuestran sus publicaciones, intervenciones en procesos judiciales y debates legislativos¹. Es en este marco que Beatriz Busaniche, presidenta de la Fundación, fue invitada como expositora experta a la sesión conjunta de ambas comisiones el día 15/05/2024, oportunidad que volvemos a agradecer.

A través de esta presentación retomaremos varios de los puntos allí expuestos e introduciremos otros que, por cuestiones de tiempo, no fue posible abordar en aquel

¹ Para más información visitar <https://www.vialibre.org.ar/>

momento pero que consideramos indispensables a la hora de debatir y legislar sobre temas tan sensibles para los y las ciudadanas. Consideramos que se complementan de forma virtuosa con varias de las exposiciones de las personas expertas que fueron invitadas.

I. El tipo de datos que se pretende recolectar

En primer lugar, y atento la confusión que suelen conllevar en estas cuestiones, es importante caracterizar el tipo de datos que se recolectan para la base en cuestión. A diferencia de otros datos personales (por ejemplo, el número de DNI), se trata en este caso de **datos sensibles** y por lo tanto implican una obligación reforzada de protección por parte del Estado. Se trata de la información más íntima de las personas, que permite individualizarlas y revelar muchas de las cuestiones que merecen especial cuidado según la Ley 25.326 de Protección de Datos Personales (por ejemplo, origen racial y étnico, información referente a la salud). Además, en el proyecto en cuestión, esta información queda asociada a otros datos: nombre, apellido, DNI, fotografía actualizada, domicilio, etc. (art. 3.b del proyecto). Si bien menciona que se almacenarán “en forma independiente a su información genética” no brinda mayores precisiones ni explica cómo se mantendrá esta disociación para quienes tienen acceso al Registro, incluyendo aquí a quienes brindan el software para las búsquedas y el cotejo allí.

En este punto es importante mencionar el Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (“Convenio 108”), vinculante en nuestro ordenamiento jurídico, y su versión actualizada (“Convenio 108+”) que entrará en vigor próximamente², al que esta misma Cámara aprobó la adhesión y ratificación por parte del Estado Argentino hace muy poco tiempo. El proyecto de referencia en su formulación actual colisiona con estas previsiones por el tratamiento que propone para datos tan sensibles como los genéticos, como veremos a continuación.

El Convenio 108+, complementario a la ley 25.326 de Protección de Datos Personales, establece una serie de garantías sobre los datos personales, especialmente en cuanto a los datos sensibles (cuestión esencial en lo que aquí nos ocupa). Entre otras cuestiones:

a. Incluye explícitamente a los datos genéticos y biométricos en la categoría de “datos sensibles”. Esta cuestión es fundamental teniendo en cuenta que la ley 25.326

² Este Protocolo Modificatorio fue ratificado por la Argentina a fines de 2022, a través de la ley 27.699, y entrará en vigencia al alcanzarse el número mínimo requerido de ratificaciones de otros Estados. Sin embargo, la ratificación de nuestro país indica sin lugar a dudas la voluntad del legislador de regirse por sus disposiciones y forma parte del *soft law* en la materia.

no hace referencia explícita a ellos (en parte por su antigüedad), aunque de su definición sobre datos sensibles (art. 2) es posible derivar que los genéticos y biométricos se incluyan en esta categoría y por lo tanto merecen una especial protección.

b. Prevé que el tratamiento de los datos genéticos sólo puede permitirse cuando la ley establezca mecanismos o garantías adecuados para la protección contra los riesgos que su tratamiento pueda generar en los intereses, derechos y libertades de los titulares de los datos.

c. Establece que para su tratamiento es necesario tanto el consentimiento del titular como la existencia de un interés legítimo.

d. Determina la obligación de notificar a la autoridad de control los incidentes de seguridad que puedan afectar los derechos de los titulares de los datos (cuestión que también resulta endeble en la ley 25.326). Sobre esta cuestión ahondaremos en el punto III sobre seguridad de la información.

Sobre este punto traemos a colación la Resolución 255/22 de la Agencia de Acceso a la Información Pública relativa a las mejores prácticas en la aplicación de la Ley de Protección de Datos Personales No. 25326 (LPDP) respecto a los datos genéticos, especialmente luego de la ratificación de este convenio.

No es incorrecto que el Estado recolecte datos de sus ciudadanos, pero siempre que sea en cumplimiento de su función registral y no como parte de una política criminal, que terminaría por instalar un estado de vigilancia generalizado, invertir el principio de inocencia y criminalizar aún más a sectores ya vulnerabilizados. En este sentido, de ninguna forma el Estado requiere para su función esencial datos tan íntimos como los genéticos, que además el proceso de extracción puede ser mucho más intrusivo que, por ejemplo, la obtención de la huella digital. **El tipo de facultades que otorga este proyecto excede por lejos aquellas indispensables para la función registral y de administración del Estado³**, habilitando actuaciones contrarias a la protección que debería brindar a los ciudadanos y a sus datos personales, de los cuales es garante y custodio, más no titular.

Así, sentada la especial protección que merecen los datos genéticos según nuestro ordenamiento jurídico, es que consideramos que este proyecto es de dudosa constitucionalidad y convencionalidad.

³ Al respecto invitamos a consultar el informe de la Fundación Vía Libre “Gestión de datos personales por parte del Estado”, de abril de 2024. Disponible en https://www.vialibre.org.ar/wp-content/uploads/2024/04/FVL2024_Informe_GestionDeDatosPersonalesPorParteDelEstado-comprimido.pdf.

II. La ampliación a todos los delitos y no sólo para personas condenadas

Como mencionaron otros expositores expertos en las sesiones conjuntas de los días 8 y 15/05, consideramos indispensable poner de manifiesto **la falta de proporcionalidad** entre la afectación de derechos y la finalidad que este proyecto plantea.

En primer lugar, el proyecto amplía la recolección de datos a **todos los delitos del Código Penal**, sin discriminar en función del nivel de gravedad. La información genética del (potencial) autor de un delito sexual o un homicidio agravado quedaría almacenada igual que la de una persona que rayó un auto accidentalmente.

Por otro lado, la inclusión en el Registro se extiende a un **universo enorme y desproporcionado de personas**, que incluye desde trabajadores judiciales hasta personas inocentes simplemente sospechadas de haber cometido un delito, en tanto incorpora la información de personas imputadas en procesos penales. Recordemos que la presunción de inocencia rige durante todo el proceso y únicamente se revierte con una sentencia firme condenatoria -requisito que rige la inclusión en el Registro según la ley actual-. La inclusión de personas imputadas no sólo invierte el principio de inocencia sino que, además, vuelve el Registro un espacio donde se van a integrar inocentes (cuyos procesos pueden llevar años hasta el sobreseimiento) y condenados, tanto por delitos graves como por menores, incluso personas que fueron imputadas y cuyos procesos pueden llevar años en terminar en un sobreseimiento. Recordemos que, salvo una decisión firme de sobreseimiento o absolución, los datos permanecen 100 años en el Registro.

La suma de estas dos cuestiones -la ampliación a todos los delitos y un universo desproporcionado de personas- trae como consecuencia otra preocupación sobre la que debemos alertar: ¿quiénes tienen más posibilidades, de acuerdo a la selectividad del sistema penal, de ser siquiera *imputadas*? Si se toman además los datos genéticos de personas que ya han sido condenadas (tal como prevé el nuevo art. 3), ¿qué personas conformarán esa base? ¿Se hace porque se presume que reincidirán o que tienen más posibilidades que otras de cometer un delito? Este enfoque no hace más que reforzar la criminalización sobre sectores ya vulnerabilizados, y crear una base de datos sesgada en este sentido, violando los principios de igualdad y no discriminación que deben regir.

En este sentido, la jurisprudencia interamericana y universal es clara en **los parámetros para evaluar la legitimidad de la restricción de derechos**, sistematizados en el llamado “test tripartito”⁴: 1) la limitación debe estar prevista por ley de manera previa expresa (para lo cual se debate esta ley); 2) debe estar orientada al logro de objetivos legítimos (ampliamente discutible en este caso); y 3) debe ser necesaria, proporcional e

⁴ Este análisis es retomado por la CSJN en el caso Halabi (Fallos: 332:11) y en su acordada 17/2019.

idónea en una sociedad democrática para el logro de los fines imperiosos que se persiguen. Dicho de otro modo, este último punto implica que no haya una solución menos lesiva y que el medio empleado guarde correspondencia con el nivel de afectación a derechos.

Y este es justamente uno de los graves problemas del proyecto en cuestión: en función de colaborar con la identificación de autores de delitos, se permiten enormes avasallamientos de los derechos de toda la población e incluso la alteración de garantías básicas del proceso penal.

En concreto, nos referimos al derecho a la autodeterminación informacional, entendido como la potestad de cada persona a decidir por sí misma sobre la publicidad, divulgación y uso de sus datos personales, que a su vez es condición para el ejercicio de otros derechos y por lo tanto debe ser estrictamente garantizado⁵. En el mismo sentido, a la protección de la privacidad e intimidad de las personas, pilares centrales de un Estado democrático y republicano.

En el mismo sentido, afecta también las garantías penales⁶: invierte el principio de inocencia en tanto confecciona una base de “potenciales autores de delitos” que incluye a cualquiera sobre quien se posea una mera sospecha (personas imputadas en una causa) y nos coloca a todos los ciudadanos en un estado de indefensión frente a la vigilancia estatal que implica.

Sobre el balance entre protección de derechos e injerencia/intromisión estatal en pos de la persecución de delitos se refirió recientemente la Corte Suprema de Justicia de la Nación a través de su acordada 17/2019. En su acápite VI. recordó “que el balance entre el derecho de toda persona a no sufrir invasiones a su privacidad y el interés estatal en la persecución penal de un posible delito, debe incluir una necesaria ponderación de los instrumentos escogidos y los fines hacia los que se dirige la específica herramienta investigativa dispuesta en la causa, en cuyo marco corresponde tamizar la medida elegida por los filtros de la necesidad, la adecuación y la proporcionalidad.”.

Sin duda estos derechos se ven vulnerados por la confección de un Registro como el que propone este proyecto, por el tipo de información que contiene y a quiénes involucra.

⁵ De hecho, fue reconocido recientemente como derecho autónomo por la Corte Interamericana de Derechos Humanos en el caso “CAJAR” (Miembros de la Corporación Colectivo de Abogados “José Alvear Restrepo” vs. Colombia), sentencia del 18 de octubre de 2023, a partir de los arts. 11 y 13 de la CADH.

⁶ En este punto nos remitimos a los especialistas en derecho penal y representantes de organizaciones que trabajan específicamente en esta materia, tales como Innocence Project o el Centro de Estudios Legales y sociales.

Los objetivos planteados en el proyecto de ley podrían llevarse adelante con una recolección mucho más ajustada de datos, atribuida exclusivamente a delitos graves definidos taxativamente en la norma, bajo condiciones mucho más estrictas, y sobre un universo reducido de personas. Es un exceso, por ejemplo, la recolección de datos de empleados judiciales, así como una vulneración a distintas garantías -como veremos a continuación- la que se plantea sobre personas imputadas.

En un supuesto similar se pronunció el Tribunal Europeo de Derechos Humanos (cuyas decisiones no resultan vinculantes para la Argentina pero sí fijan un estándar internacional de peso), donde entendió que la conservación sistemática e indiscriminada por parte de autoridades públicas de huellas dactilares, muestras celulares y perfiles de ADN de personas no condenadas **no cumple el requisito de necesidad en una sociedad democrática** (TEDH, Caso Marper v. UK, 2008)⁷.

De esta manera, si hablamos de datos sensibles, la protección frente a la vulneración de estos derechos debe ser todavía mayor, por lo que la evaluación de la legitimidad de las restricciones es aún más estricta. Un avance de las facultades estatales en el sentido que prevé el proyecto debería tener una justificación mucho más profunda; implicar un objetivo legítimo que realmente no se pueda alcanzar de otra forma y que amerite tal intromisión. En su redacción actual es absolutamente desproporcionado el costo en términos de derechos de todos los ciudadanos en función de los objetivos que incorpora en su art. 2. **La intromisión y vigilancia sobre la vida privada, así como la confección de una base de datos de tal sensibilidad en poder del Estado (y con acceso por parte de las fuerzas de seguridad, como veremos más adelante), sin justificación sobre la inexistencia de otro medio más idóneo y menos lesivo, carece de toda proporcionalidad con el objetivo perseguido.**

III. Seguridad de la información

La sensibilidad y masividad de los datos que este proyecto propone recolectar es inversamente proporcional a la capacidad de protegerlos que tiene el Estado hoy en día. Por todo lo expuesto hasta aquí, es claro que la propia ley debería establecer **cómo garantizar la cadena de custodia de la información recolectada, asegurando de forma apropiada la trazabilidad**. Son cuestiones que no sólo el texto no contempla, sino que el Estado argentino ha demostrado numerosas veces su negligencia para cumplirlas.

⁷ Para más información recomendamos consultar <https://www.cepc.gob.es/publicaciones/revistas/revista-de-derecho-comunitario-europeo/numero-33-mayoagosto-2009/tedh-sentencia-de-04122008-s-y-marper-c-reino-unido-3056204-y-3056604-articulo-8-cedh-vida-privada-1>.

La legislación existente prevé ciertos deberes: la ley 25.326 establece una obligación general para el responsable o usuario del archivo de datos sobre la adopción de “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 (art. 9). Sin embargo, la ley y su reglamentación son poco precisas en cuanto al contenido de esta obligación de seguridad en la custodia de los datos, y es una de las cuestiones por las que insistimos hace tiempo en la actualización de la norma. Por ejemplo, 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 vivimos⁸.

Este panorama legislativo se complementa con las disposiciones del Convenio 108+ citadas en el punto I de esta presentación, donde se establece, por ejemplo, la obligación de notificar a la autoridad de control los incidentes de seguridad que puedan afectar los derechos de los titulares de los datos (art. 7 y concordantes). También recordamos la resolución 47/2018 de la AAIP sobre medidas de seguridad y su aplicación a los datos genéticos, de acuerdo con la resolución 47/2018 de la misma agencia.

Aún así, no se instrumentaron los recursos apropiados para implementarlas. Vemos día a día las consecuencias tanto de la falta de medidas efectivas para asegurar la información como para mitigar los riesgos y daños. En este punto 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 al aumento de la capacidad técnica para procesar datos, tanto de manera legítima como ilegítima.

Basta recordar algunos episodios recientes, como el caso de la filtración de las bases de datos de las propias fuerzas federales -en aquel momento conducidas por la misma Ministra que hoy propone este proyecto de ley- conocidas como “La gorra leaks 1 y 2” en 2019⁹ en la cual los atacantes usaron técnicas pueriles de ingeniería social para obtener permisos de acceso y contraseñas. Se trató de un caso de alta negligencia en torno a la preservación de información que incluía, entre otras cosas, cuestiones de la

⁸ 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>.

⁹ Ver, por ejemplo, <https://www.infobae.com/sociedad/policiales/2019/10/31/la-gorra-leaks-como-es-el-insolito-y-sencillo-truco-que-uso-un-hacker-para-robar-los-datos-privados-de-la-policia-federal/>

propia fuerza policial que no debían ser públicas por razones de seguridad y datos de testigos y denunciantes en causas penales.

También fue de público conocimiento la negligencia en la custodia de bases de datos sensibles del Ministerio de Salud y del Registro Nacional de las Personas (2021)¹⁰, y la falta de medidas de mitigación que deberían haber sido tomadas en consecuencia.

Las filtraciones de datos personales que sufrieron diversas reparticiones del Estado en el último tiempo nos permiten asegurar que sus sistemas son vulnerables. Es evidente 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.

Este proyecto pretende seguir construyendo bases de datos de información sensible sin que el Estado haya ofrecido evidencia alguna de su capacidad de custodiar de manera apropiada la información que recolecta y manipula. Tampoco demostró invertir o tener siquiera un plan en torno a las cuestiones de seguridad de la información. Así las cosas, no puede seguir demandando a los ciudadanos la entrega de información sensible que puede dañar de forma irreparable la integridad, la libertad y la privacidad de las personas.

Un proyecto como el que se discute ahora no puede desconocer lo endeble de este escenario normativo y, a la vez, las obligaciones internacionales contraídas por la Argentina en materia de seguridad de la información.

III.i. Sobre el acceso por parte de las fuerzas de seguridad:

Otro punto del proyecto que suscita grave preocupación es la disponibilidad del Registro para los auxiliares de la justicia a nivel federal, es decir **las fuerzas de seguridad federales**. Mientras que la ley actual lo habilita para autoridades judiciales y del Ministerio Público Fiscal, el proyecto elimina a este último (lo cual es llamativo y de dudosa técnica legislativa en tanto le encomienda a la Procuración General la firma de convenios con registros de otras jurisdicciones y organismos internacionales, y habilita a los fiscales a ordenar la toma de muestras) y suma a las mencionadas fuerzas.

Entramos aquí en un terreno muy complicado: las normas de transparencia, acceso a la información y protección de datos cuentan con supuestos vagos de excepción bajo el argumento de la “seguridad nacional”, en los que las autoridades suelen ampararse de manera arbitraria y las autoridades judiciales tienden a convalidar.

¹⁰ Ver, por ejemplo, https://www.clarin.com/tecnologia/filtracion-renaper-difunden-datos-sensibles-60-000-argentinos-piden-cerca-17-mil-dolares-dni_0_2eE_kXXBo.html.

En otras palabras, se trata de un entramado muy opaco en el que el control ciudadano se vuelve aún más complejo, inadmisibile para una base de datos con el nivel de sensibilidad que se pretende construir a través de este proyecto. En este sentido, el articulado debería incluir expresamente las previsiones de las leyes 25.326 (art. 17 y concordantes), 27.275 (art. 8 y concordantes) y 25.520 (art. 16bis y concordantes) en cuanto al acceso a datos personales, a medidas de seguridad sobre la información y al alcance limitado del régimen de excepciones. Recordemos que el derecho de acceso a datos personales y a información pública tiene carácter legal, constitucional y convencional, y requiere de prerrogativas expresas para poder asegurar su operatividad. Esto es indispensable sobre todo teniendo en cuenta que, de aprobarse esta ley, se aplicaría a personas imputadas: es decir, inocentes.

A su vez, en tanto esta norma permite -y promueve- la adhesión de otras jurisdicciones, se habilitaría también el acceso a las fuerzas provinciales, lo cual torna aún más difícil la protección y el ejercicio de derechos en torno a los datos personales y la privacidad. ¿Quiénes, de qué rango, bajo qué autorizaciones, bajo qué protocolo de seguridad de acceso a la información tendrán las fuerzas de seguridad capacidad de acceder a esa base de datos? Volvemos a traer a colación en este punto la necesidad de garantizar la trazabilidad del tratamiento de los datos y su cadena de custodia, cuestiones que se vuelven casi imposibles de garantizar bajo el manto de opacidad que suele regir estas actuaciones.

Esta prerrogativa se vuelve aún más grave en el escenario de falencias normativas y evidente falta de estructura estatal para cumplir adecuadamente el deber de proteger los datos de la ciudadanía.

IV. Cesiones y transferencias

Otro de los aspectos preocupantes es la política de **cesión y transferencia** de datos, tanto con Registros de otras jurisdicciones del país como con organismos internacionales a través de convenios que la Procuración deberá impulsar (nuevo art. 7).

Esto implica problemas de distintos niveles. Por un lado, la legislación y la jurisprudencia nacionales como internacionales son claras en las condiciones para que la transferencia internacional o la cesión de datos dentro de dependencias del Estado sea legítima: debe contar con el consentimiento del titular y hacerse con la misma finalidad para la que fueron recolectados (cfr. arts. 4, 5, 6 y 11 de la ley 23.526). Si bien el régimen de excepciones que introduce la norma es amplio y ambiguo, la doctrina y la jurisprudencia han siempre enfatizado en la necesidad de interpretarlas de manera

restrictiva, siempre en pos de la más amplia protección de los derechos de los titulares¹¹. Esto parece contrario a las potestades que otorga el proyecto.

A la vez, en cuanto a la transferencia internacional, tanto el Convenio 108 y el marco normativo de protección de datos de la Unión Europea al que Argentina adhirió, como las directrices de la OCDE sobre privacidad¹² ofrecen más precisiones: exigen, por ejemplo, reglamentaciones específicas para determinadas categorías de datos cuando se transfieran a jurisdicciones no equivalentes en materia de protección adecuada de datos, de manera tal que suponga una burla a la legislación vigente en el estado de origen. Nada de esto está contemplado en el proyecto en cuestión. Es indispensable prever en la norma en qué términos puede acceder una agencia extranjera -si es que puede hacerlo- a una base argentina de datos sensibles.

En particular, preocupa además que dentro de los fundamentos que acompañan al proyecto de ley en el mensaje enviado por el PEN se cita como caso virtuoso y ejemplo a seguir la utilización del programa CODIS creado y mantenido por el FBI -tal como surge de diversas notas de prensa- para la gestión de estas bases de datos. Se trata de un software cerrado bajo condiciones de administración que quedan en manos de una agencia federal extranjera, que se otorga en formato “caja negra” y bajo propiedad intelectual de un Estado extranjero: esto implica que las autoridades argentinas no tienen forma de saber cómo está funcionando (por ejemplo a través de conocer su código fuente). Como mencionamos, la integración de datos sensibles y su transferencia a jurisdicciones con menores protecciones legales **colisiona con los principios legales, constitucionales y convencionales de nuestro ordenamiento, además de implicar una pérdida de soberanía sobre la información recolectada y el allanamiento sobre la incapacidad de garantizar las condiciones mínimas necesarias para el cumplimiento de los derechos de la ciudadanía sobre sus propios datos.**

V. Otras cuestiones preocupantes

A continuación enumeramos algunas cuestiones que observamos con suma preocupación y que, si bien exceden la agenda de trabajo habitual de la Fundación Vía Libre, consideramos importante traer a su atención:

- a. El régimen de obtención de huellas se aplicaría también sobre menores de edad y personas inimputables. Debería contemplarse, de mínima, un procedimiento

¹¹ Sobre este punto invitamos a consultar el informe de la Fundación Vía Libre “Gestión de datos personales por parte del Estado” antes citado.

¹² Organización para la Cooperación y el Desarrollo Económicos, “Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data”, 1980, actualizado en 2013. Se trata de estándares internacionales no vinculantes para la Argentina pero sí relevantes para el derecho internacional de los derechos humanos sobre la temática.

específico teniendo en cuenta el régimen penal juvenil en un caso y la eventual declaración de inimputabilidad en el otro, de forma tal que esos datos no queden registrados indebidamente.

- b. El proyecto prevé sanciones para quien utilice indebidamente el Registro; sin embargo, no existe al día de hoy delito alguno en el Código Penal que tipifique esta conducta, por lo cual se vuelve virtualmente inaplicable.
- c. Parece haber un problema de legalidad en la obtención de datos genéticos de personas que ya fueron condenadas previo a la entrada en vigencia de esta ley. Este punto se condice con el desarrollado previamente sobre la discriminación y criminalización que implica el registro de sus datos de manera “preventiva”, como si se asumiera que volverán a cometer un delito.
- d. De acuerdo con el nuevo art. 8, los laboratorios a cargo de los exámenes genéticos ya no deberán ser aquellos acreditados por el Ministerio de Ciencia y Tecnología sino cualquiera que cumpla con normas internacionales. Esto implica reducir los controles estatales sobre una cuestión sumamente sensible.

En función de todos los puntos expuestos es que volvemos a insistir en el grave riesgo que implica para los derechos de toda la ciudadanía la aprobación de un texto como el que propone el proyecto. Quedamos a disposición por cualquier información que fuera necesaria ampliar o que resultara de interés discutir con mayor profundidad.

Con la expectativa de que estas consideraciones sean tenidas en cuenta a la hora del debate, saludamos a Uds. atentamente,

Fundación Vía Libre

info@vialibre.org.ar