SE PRESENTAN EN CALIDAD DE *AMICUS CURIAE*.

APORTAN ARGUMENTOS.

Señores Jueces de la Sala V de la Cámara Nacional de Apelaciones en lo Contencioso Administrativo Federal:

La Fundación para la Difusión del Conocimiento y el Desarrollo Sustentable "Vía Libre" (en adelante "Vía Libre" o FVL), representado en este acto por María Beatriz Busaniche, en calidad Presidenta de la mencionada institución, con el patrocinio letrado de Margarita Trovato (T° 133 F° 719 CPACF), constituyendo domicilio legal en xxxxxxxxxx, y domicilio electrónico en el usuario xxxxxxxxxx, en el marco de la causa caratulada "Palazzi, Pablo c/ EN-Registro Nacional de las Personas S/Habeas Data", expte. 18307/2021, nos presentamos y decimos:

1. OBJETO

Por el presente venimos a presentar consideraciones jurídicas conducentes para la resolución del presente caso, donde se discute la protección y el acceso a datos personales, así como la vía idónea para reclamarlo, contemplados en los arts. 18, 19 y 43 de la Constitución Nacional, así como en diversos Instrumentos Internacionales de Derechos Humanos que gozan de jerarquía constitucional (art. 75.22 CN). Son, además, argumentos de relevancia pública que buscan alimentar y robustecer el debate en torno a la protección de datos personales y a la autodeterminación informativa que asiste a todos los ciudadanos.

En este sentido, solicitamos se nos tenga presentados en calidad de amigos del tribunal (*amicus curiae*) y que, en función de los argumentos brindados, se revise el rechazo del hábeas data interpuesto, se habilite el acceso a la totalidad de los datos personales en poder de la demandada y se informen las medidas de seguridad adoptadas sobre la base de datos en la que consta información del actor.

2. PERSONERÍA

María Beatriz Busaniche, DNI xxxxxxxxxx, conforme surge del Estatuto cuya copia simple se acompaña y la representación en actos judiciales que éste me otorga en su art. 14, me presento en calidad de Presidenta de la Fundación para la Difusión del Conocimiento y el Desarrollo Sustentable Vía Libre, de acuerdo con la constancia de inscripción ante la IPJ que se acompaña, con domicilio real en xxxxxxxxxx.

3. EL INSTITUTO DEL AMICUS CURIAE - INTERÉS DE LA FVL EN EL PRESENTE CASO

a. Sobre el instituto del *amicus curiae*

La figura del *amicus curiae,* reconocida por un gran número de tribunales nacionales e internacionales, apunta a permitir la incorporación de conocimiento, experiencia y argumentos de hecho y derecho que puedan servir al juzgador a la hora de resolver un caso. El objeto de presentaciones de este tipo consiste en que terceros ajenos a una disputa judicial —pero con un justificado interés en la resolución final del litigio—, puedan expresar sus opiniones en torno a la materia, a través de aportes de trascendencia para la sustentación del proceso judicial.

Tiene dicho la doctrina que "(...) La posibilidad de fundar decisiones judiciales en argumentos públicamente ponderados constituye un factor suplementario de legitimidad de la actuación del Poder Judicial. La presentación del *amicus curiae* apunta entonces a concretar una doble función: a) aportar al tribunal bajo cuyo examen se encuentra una disputa judicial de interés público argumentos u opiniones que puedan servir como elementos de juicio para que aquel tome una decisión ilustrada al respecto; y b) brindar carácter público a los argumentos empleados frente a una cuestión de interés general decidida por el Poder Judicial, identificando claramente la toma de posición de los grupos interesados, y sometiendo a la consideración general las razones que el tribunal tendrá en vista al adoptar y fundar su decisión"[1].

En nuestra práctica jurídica el *amicus curiae* se encuentra ampliamente aceptado de conformidad con los antecedentes existentes en el derecho comparado y en el derecho internacional de derechos humanos. Es que, si bien al día de hoy no tiene una regulación propia a nivel nacional (más allá del régimen especial que se dio la Corte Suprema, como veremos a continuación), existe un largo recorrido doctrinario y jurisprudencial, tanto nacional como internacional, sobre su procedencia y el valor de su incorporación.

De hecho, la institución del *amicus* es una figura clásica: se remonta originalmente al derecho romano y luego se incorpora a la práctica judicial de los países de tradición anglosajona, generalizándose luego en diversos países de habla inglesa hasta convertirse en un elemento característico de las causas con un marcado interés público. A lo largo de los años, esta figura se ha extendido en forma notoria en los sistemas regionales de derechos humanos, tanto el Interamericano del que somos parte como de sus análogos en Asia y Europa.

En Argentina, los antecedentes judiciales de reconocimiento de esta figura datan de largo tiempo, incluso antes de la reforma constitucional de 1994, en tanto el art. 33 de la Constitución Nacional establece la forma republicana de gobierno y la soberanía popular, principios que justamente el instituto del *amicus* busca asegurar: vehiculiza la participación ciudadana, el ejercicio del derecho a peticionar a las autoridades, la

[1] Cfr. Alexy, R., *Teoría de la argumentación*, CEC, Madrid, 1989, trad. de M. Atienza e I. Espejo, pág. 317.

libertad de expresión ciudadana y el debido proceso. La transparencia del debate público y el acercamiento del poder judicial a los ciudadanos contribuye al fortalecimiento de las instituciones republicanas y a la calidad del sistema democrático[2]. Así, el *amicus curiae* no es más que una materialización de los preceptos del art. 33, más aún cuando se trata de procesos judiciales que versan sobre cuestiones de derechos humanos.

Por ejemplo, ya en 1995, la Sala II de la Cámara Federal en lo Criminal y Correccional de la Capital Federal en la causa "Hechos ocurridos en el ámbito de la Escuela de Mecánica de la Armada (ESMA)", hizo lugar a la presentación de *amicus curiae* de parte de dos organizaciones internacionales de derechos humanos. Esta posición se mantuvo a lo largo de los años y, más recientemente, la Cámara Federal de Casación Penal resolvió en el mismo sentido recordando que **"la actuación como amigos del Tribunal encuentra apoyatura en el sistema interamericano y encuentra jerarquía constitucional en nuestro sistema normativo"** (CFCP, sala I, registro 1554/16.1, 25/08/2016). Asimismo, la Cámara advirtió que la falta de una reglamentación para este tipo de presentaciones ante dicho tribunal, no constituía un obstáculo para su procedencia y que, en todo caso, el reglamento de la Corte Suprema "podría servir de guía para resolver presentaciones ante esta instancia".

En similar sentido se fueron pronunciando los tribunales de distintas provincias en causas de interés general o colectivo. Así, por ejemplo, en la provincia de Tucumán, la Cámara Contencioso Administrativo hizo lugar a la solicitud de ser tenido como *amicus curiae* realizada por la organización de derechos humanos local ANDHES[3] y el Tribunal Superior de Justicia provincial hizo lo propio con relación a Amnistía Internacional Argentina[4]. Por su parte, la justicia de Mendoza también reconoció la admisibilidad de este instituto en una presentación de la Asamblea Permanente de Derechos Humanos, sosteniendo que "(…) se trata de un medio procesal adecuado para suministrar a los jueces la mayor cantidad posible de elementos de juicio para dictar una sentencia justa. (…) Ya no se trata de ilustrar al juez como amigo del tribunal sino de auspiciar, apoyar o promover la causa de uno de los litigantes. En la actualidad no se le exige neutralidad. Sí se espera, en cambio, una inteligente contribución sobre los problemas planteados por el caso, sobre su repercusión respecto de terceros y demás integrantes de la comunidad"[5].

---

[2] Informe de la Relatora Especial sobre una vivienda adecuada como elemento integrante del derecho a un nivel de vida adecuado y sobre el derecho de no discriminación a este respecto. UN Doc A/HRC/37/53, 15 de enero de 2018, párr. 33.

[3] Cámara Contencioso Administrativa de Tucumán, causa "Colegio de abogados de Tucumán vs. Honorable Convención Constituyente s/ acción de nulidad e inconstitucionalidad"

[4] Tribunal Superior de Justicia de Tucumán, causa "Iñigo David Gustavo y Otros s/privación ilegítima de la libertad y corrupción (María de los Ángeles Verón)"

[5] Suprema Corte de Justicia de la Provincia de Mendoza, causa "Curel, Gastón Oscar y otros". Voto Jueza Kemmelmajer de Carlucci.

Luego, la Corte Suprema de Justicia de la Nación echó luz sobre la necesidad de una regulación y, en el ejercicio de sus funciones administrativas, dictó las acordadas 28/2004 y 7/2013, reconociendo la importancia de la intervención como *amicus curiae* y reglamentando su presentación en trámites ante ella. Para esto se basó no sólo en el art. 33 CN antes mencionado, sino también en el derecho a ser oído establecido por el art. 36 del CPCCN, valorando las opiniones expertas de entidades o personas que no son parte del proceso a los fines de enriquecer la discusión.

En particular, sostuvo que en los casos en que se debatan cuestiones de interés público "(…) a fin de resguardar el más amplio debate como garantía esencial del sistema republicano democrático, debe imperar un principio hermenéutico amplio y de apertura frente a instituciones, figuras o metodologías que, por su naturaleza, responden al objetivo de afianzar la justicia entronizado por el Preámbulo de la Constitución" y que por lo tanto en las causas de interés público "(…) se autorice a tomar intervención como Amigos del Tribunal a terceros ajenos a las partes, que cuenten con una reconocida competencia sobre la cuestión debatida y que demuestren un interés inequívoco en la resolución final del caso, a fin de que ofrezcan argumentos de trascendencia para la decisión del asunto" (acordada 28/2004). Y luego agregó que esta figura tiene el objetivo de "pluralizar y enriquecer el debate constitucional, así como de fortalecer la legitimación de las decisiones jurisdiccionales dictadas por esta Corte Suprema en cuestiones de trascendencia institucional", por lo que corresponde habilitar la presentación de personas físicas o jurídicas como *amicus* en todos los procesos judiciales donde se debatan "cuestiones de trascendencia colectiva o interés general" (acordada 7/2013).

Por otro lado, la presentación de este tipo de memoriales en derecho garantiza la participación de la sociedad civil y terceros interesados en ciertas cuestiones de trascendencia pública que se debaten ante los tribunales. Esta participación —que el amicus curiae vehiculiza— hace al principio republicano de gobierno consagrado en la Constitución Nacional. La transparencia del debate público y el acercamiento del poder judicial a los ciudadanos contribuye al fortalecimiento de las instituciones republicanas y a la calidad del sistema democrático[6].

De lo dicho se desprende la procedencia de la figura del *amicus curiae* en cualquier instancia de un proceso que se encuentra abierto, y sin que exista una limitación en función del fuero que se trate. En efecto, por su propia naturaleza, este instituto procede sin que existan al respecto restricciones formales que puedan oponérsele.

[6] Informe de la Relatora Especial sobre una vivienda adecuada como elemento integrante del derecho a un nivel de vida adecuado y sobre el derecho de no discriminación a este respecto. UN Doc A/HRC/37/53, 15 de enero de 2018, párr. 33.

En virtud de lo expuesto, nos presentamos ante V.E. con el objeto de que se nos permita exponer nuestros argumentos jurídicos a los efectos de colaborar con la resolución del presente caso sometido a estudio.

b. Sobre la Fundación Vía Libre y su trayectoria en la temática

La Fundación Vía Libre es una organización que trabaja en la intersección entre tecnología y derechos humanos: promueve y defiende derechos fundamentales en entornos mediados por tecnologías de información y comunicación. Si bien al momento de su creación se enfocaba especialmente en políticas públicas de software libre para la difusión del conocimiento, a lo largo de los años la Fundación amplió su misión a temáticas más generales de derechos sociales, económicos y culturales y derechos civiles y políticos en entornos mediados por tecnologías digitales.

La Fundación articula sus acciones de manera permanente con organizaciones afines a nivel nacional e internacional, trabaja en incidencia pública sobre políticas de estado de utilización de tecnologías apropiadas, en particular de Software Libre, a fin de cumplir con las metas de desarrollo social y económico del milenio. Hoy en día se enfoca en el seguimiento y desarrollo de políticas públicas, sensibilización pública sobre temas de agenda, creación de capacidades y promoción de debates sobre temas vinculados a las tecnologías que impactan en el ejercicio de Derechos Humanos, de acuerdo con los fines mencionados en el Estatuto Constitutivo. En este sentido, entre sus temas principales de agendas se incluyen: propiedad intelectual y acceso al conocimiento; políticas de privacidad y protección de datos personales, incluyendo dentro de ellas, la promoción de sistemas que garanticen el debido proceso, el acceso a la justicia, la inviolabilidad de las comunicaciones y el domicilio y la protección de la vida privada en toda su amplitud, tanto en el espacio privado como en la esfera pública; incorporación de tecnologías en procesos electorales desde la perspectiva de derechos civiles y políticos; regulaciones de Internet y políticas de seguridad en el entorno digital y la protección legal de la comunidad de seguridad informática a fin de que pueda desarrollar plenamente sus tareas de prevención, investigación, análisis y reporte de vulnerabilidades en los sistemas informáticos.

De esta manera, dos de sus ejes principales de trabajo actuales son el derecho a la privacidad y la seguridad de la información.

Sobre el primero, Vía Libre tiene una amplia trayectoria en trabajo sobre **protección de datos personales y autodeterminación informacional**. En función de su *expertise* y el mandato dado por el Estatuto, desde el año 2004 trabaja insistentemente en la vigencia del derecho a la privacidad y, más específicamente, de protección de datos personales. En tanto la privacidad es un derecho fundamental para el desarrollo de la autonomía individual, el desarrollo de la personalidad y la construcción de ciudadanía y,

por lo tanto, para la construcción de sociedades democráticas, la FVL trabaja enfáticamente en su frente a la vigilancia por parte del sector público como del privado, para exigir el debido cumplimiento de los estándares normativos. Con este objetivo promueve la adopción de legislaciones adecuadas y monitorea el uso de tecnologías que puedan vulnerar garantías mínimas por su diseño y/o implementación. Dentro de esta agenda, realiza publicaciones académicas, da seguimiento a políticas públicas (por ejemplo aquellas que implican alguna clase de vigilancia), participa en debates legislativos, tiene con frecuencia apariciones en los medios y elabora constantemente materiales de difusión general. También lo hace a través de presentaciones judiciales: a modo de ejemplo, la FVL fue admitida como *amicus curiae* en la causa obrante en el fuero Contencioso Administrativo y Tributario porteño donde se discute la constitucionalidad del sistema de reconocimiento facial implementado por la Ciudad de Buenos Aires[7] en función de las garantías de privacidad, intimidad y protección de datos personales de los ciudadanos que deben ser aseguradas, quedando en evidencia también las falencias de seguridad informática que este sistema reviste.

Con respecto a esto último, es decir las cuestiones atinentes a la **seguridad de la información**, la FVL trabaja por su promoción y protección, así como por el resguardo de la comunidad que se dedica a esta cuestión, en fiel cumplimiento de su estatuto. En tanto la investigación, seguimiento, reporte y mitigación de incidentes y vulnerabilidades son tareas esenciales en una sociedad atravesada por el uso de dispositivos digitales, la FVL vela por ellas a través de construcción de conocimiento, mecanismos de comunicación pública e incidencia política y legislativa por la protección de estas prácticas. A modo de ejemplo, es parte del Comité Asesor para el Desarrollo e Implementación de Aplicaciones Seguras, creado por la Dirección Nacional de Ciberseguridad en 2021, cuyo objetivo es elaborar lineamientos y estándares para el desarrollo de aplicaciones seguras por parte del Estado Nacional; realizó investigaciones[8] sobre seguridad informática; se presentó como *amicus curiae* en la causa donde se investigaba un allanamiento indebido a un informático[9] en el marco de la pesquisa sobre filtraciones de comunicaciones de la Policía Federal Argentina, conocida como “La Gorra Leaks”, entre otros.

De hecho, en el cruce entre las agendas de protección de datos y de seguridad de la información, la FVL atiende insistentemente, entre otras, las iniciativas de implementación de tecnologías de reconocimiento facial en la Ciudad (tal como mencionamos en el punto anterior, incluyendo el amicus que presentamos, pero

---

[7] “Observatorio de Derecho Informático Argentino O.D.I.A. c/ G.C.B.A s/ Amparo – Otros”, Expte nro. 182908/2020-0.

[8] Ver, entre otras, “Hackers y Gorras” (2008) disponible en https://www.vialibre.org.ar/hackers-y-gorras/ y https://youtu.be/P06nNW40Xuc?si=TaSE12RyP3U3Niah.

[9] CFP 55276/2019, “Smaldone, Javier s/ incidente de nulidad”.

también a través de exposiciones en ámbitos legislativos[10] y comunicación en los medios, entre otras) y, más recientemente, la intención de incluir el requisito del DNI en el pasado censo nacional, que también discutimos política y judicialmente a través de una acción de amparo.

Para el abordaje de ambas agendas de trabajo, la FVL articula con diversas redes nacionales e internacionales de organizaciones de la sociedad civil expertas en la materia. Entre otras, es parte de la Iniciativa Ciudadana para el Control del Sistema de Inteligencia (ICCSI)[11], un grupo dedicado al estudio del funcionamiento de los sistemas de inteligencia y al seguimiento e impulso de mecanismos de control sobre, entre otras cuestiones, el respeto al derecho a la privacidad y la seguridad de los datos personales. Desde allí promovemos cambios normativos, investigamos y participamos en causas judiciales en torno al tema. A modo de ejemplo, en 2019 elaboramos un informe sobre interceptación legal de comunicaciones de acuerdo a estándares de derechos humanos[12] y nos manifestamos públicamente sobre el Protocolo General para la Prevención Policial del Delito con Uso de Fuentes Digitales Abiertas emitido en 2020, advirtiendo sobre sus riesgos en términos de derechos humanos y aportando argumentos técnicos en ese sentido[13].

Es por todo esto que nos interesa presentar argumentos en este caso, con la expectativa de que sean tenidos en cuenta al momento de resolver, máxime teniendo en cuenta que se trata de un caso de especial relevancia por versar sobre información personal perteneciente a un conjunto de datos que habría sido objeto de una vulneración de seguridad. En estas condiciones y atendiendo a las características de las cuestiones discutidas en autos, solicitamos a V.E. que admita nuestra presentación en calidad de amigos del tribunal y disponga su incorporación al expediente.

Corresponde aclarar, por último, que la Fundación Vía Libre viene a apoyar a la parte actora en este proceso, que no ha recibido asesoramiento ni ayuda económica de cualquier especie y que el resultado del proceso tampoco representa para esta organización ningún tipo de beneficio patrimonial.

4. ANTECEDENTES. Breve resumen de los hechos.

En el presente caso se origina por el pedido de acceso del titular a sus datos personales en poder de una agencia del Estado (RENAPER), así como a conocer si fueron objeto de incidentes de seguridad (filtraciones) que tomaron estado público. Solicita

---

[10] Ver, por ejemplo, presentación ante la Comisión de Seguridad de la Legislatura Porteña en ocasión del debate por este tema (2020), disponible en https://youtu.be/8Lfs5qe4E7Y?si=7JV7JOprTwSeI-V7

[11] https://www.iccsi.com.ar

[12] Disponible en https://www.vialibre.org.ar/interceptacion-legal-de-comunicaciones-hacia-un-sistema-respetuoso-de-los-derechos-humanos/

[13] https://www.vialibre.org.ar/comunicado-iccsi-la-cibervigilancia-masiva-esta-prohibida/

también el conocer qué medidas de seguridad de la información se tomaron en función de esas filtraciones, independientemente de que sus datos personales hayan o no estado involucrados. Como veremos a continuación, se discute: a) el cumplimiento del derecho de acceso a los datos personales, en tanto se debate si la entrega fue parcial y/o insuficiente; b) el derecho de conocer las medidas de seguridad atinentes a una base de datos que sufrió vulneraciones -cuanto menos- parciales de seguridad en la que se encuentra información personal del actor; y c) la procedencia del *habeas data* como vía procesal idónea para conocer la existencia de estas medidas.

En concreto, el Sr. Palazzi realizó en octubre de 2021 un pedido administrativo de acceso a sus datos personales al Registro Nacional de las Personas (RENAPER), luego de que tomaran estado público varios incidentes de seguridad (eventos conocidos como "data *breach*") acaecidos en servidores de dependencias del Estado Nacional, entre ellas el mencionado Registro. De hecho, las filtraciones seguían ocurriendo al momento de efectuar la solicitud.

Este pedido no fue respondido, por lo que interpuso acción de habeas data en los términos del art. 43 CN contra el mencionado RENAPER, con fundamento en los arts. 9 y 10 de la Ley Nacional de Protección de Datos Personales N° 25.326, relativo a las obligaciones de seguridad informática y confidencialidad a cargo del Estado Nacional) para conocer sus datos personales que constan en la base de datos del organismo demandado. Seguidamente el Juez ordenó el informe previsto en el art. 39 de la mencionada ley.

Al contestar demanda, el Estado se limitó a: 1) adjuntar una breve ficha ("Formulario Único de Identificación") con algunos datos personales que no incluye, de mínima, otros que es evidente que tiene en su poder, tales como fotos anteriores del DNI, huellas digitales tomadas en el pasado, etc.; y 2) informar que el actor no se encontraba entre los afectados por el incidente (es decir que reconoció la existencia del hecho, aunque afirmó que "no hubo un ingreso no autorizado a sus sistemas ni una filtración masiva de datos", sino que un usuario legítimo habría utilizado de forma indebida su acceso y luego publicado información) y por lo tanto omitir pronunciarse sobre posibles medidas de seguridad tomadas. En la misma línea, tampoco contestó el traslado de ampliación de demanda.

En este escenario dictaminó el Sr. Fiscal, que lo hizo a favor de la procedencia de la acción de hábeas data para el acceso a datos personales en poder del RENAPER, reconociendo que se trataba de información "insuficiente y parcial", exigiendo que entregue la totalidad que consta en sus archivos. En cambio, consideró que esta no era la vía procesal adecuada para conocer la existencia de medidas de seguridad adoptadas sobre el conjunto de la información en cuestión si no se encontraban directamente afectados datos personales del demandante.

Así las cosas, el 25/04/23 el Juzgado en los Contencioso Administrativo Federal nro. 4 de la Capital Federal dictó sentencia rechazando la acción interpuesta. Entendió que los datos biométricos ya habían sido entregados por el RENAPER, por lo que la petición de acceso quedaba saldada, y que la vía del habeas data resultaba improcedente para conocer medidas de seguridad tomadas sobre datos personales entre los que, según afirmó la demandada, no se encontraban los del actor. Seguidamente, el 28/04 el actor apeló esta decisión.

El rechazo de primera instancia, estimamos, resulta arbitrario a la luz de los argumentos que expondremos, con una grave afectación de los derechos a la privacidad e intimidad, así como al acceso a la justicia y a una la tutela judicial efectiva de la parte actora.

5. FUNDAMENTOS DE HECHO Y DE DERECHO

Tal como repasamos más arriba, en este caso se encuentra en discusión a) el derecho de acceso a datos personales en poder del RENAPER y su adecuada satisfacción con la información entregada, b) el derecho de acceso a medidas de seguridad tomadas sobre la base de datos a la que esta información pertenece en función de, al menos, un incidente ocurrido con un conjunto de datos personales en poder del Renaper, y c) la procedencia de la vía del Habeas Data para hacerlo. En esta presentación nos centraremos argumentos jurídicos que aporten una interpretación de los puntos b) y c) -acceso a medidas de seguridad y procedencia de la vía de hábeas data- acorde con los más altos estándares nacionales y del derecho internacional de los derechos humanos en la materia.

i. Derecho a la intimidad y a la privacidad. El acceso como condición de posibilidad.

En primer lugar, nos interesa detenernos en el derecho a la privacidad y a la intimidad, cuyo objetivo es "proteger a la persona de la intrusión de otras en una determinada esfera de reserva personal."[14], de larga trayectoria y recogido en el art. 19 de la Constitución Nacional[15].

[14] *Diario de Sesiones de la Convención Constituyente de la Ciudad de Buenos Aires de 1996*, Ciudad Autónoma de Buenos Aires, Editorial Jusbaires, 2016, T. 2, p. 548. Citado en Basterra, M., "Derecho a la intimidad, privacidad y confidencialidad en la Ciudad Autónoma de Buenos Aires", en *Constitución de la Ciudad Autónoma de Buenos Aires. Edición Comentada*, Editorial Jusbaires, CABA, 2016.

[15] A los efectos de esta presentación, trataremos los conceptos de "privacidad" e "intimidad" como análogos y/o los utilizaremos de forma indistinta, tal como lo hace parte de la doctrina, la jurisprudencia y la propia CSJN (fallos 306:1892). Para profundizar sobre las discusiones doctrinarias ver, por ejemplo, Basterra, M., Op. Cit., pp. 148 y 149.

Podemos entenderlos “la facultad que tiene cada persona de disponer de una esfera, espacio privativo o reducto inderogable de libertad individual, que no puede ser invadido por terceros –ya sea que se trate de particulares o del propio Estado– mediante intromisiones que pueden asumir diversos signos. Este derecho requiere el respeto a las condiciones mínimas indispensables para que el hombre logre desarrollar sus aptitudes potenciales”[16], por lo que se interpreta en consonancia con el art. 18 y las salvaguardas a la privacidad allí descriptas.

A nivel internacional, y en términos similares, el derecho a la intimidad fue expresamente consagrado en la Declaración Universal de los Derechos del Hombre y el Pacto Internacional de Derechos Civiles y Políticos, al disponerse que nadie podrá ser objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación (arts. 12 y 17, respectivamente), tal como nos recuerda el Máximo Tribunal (“Ganora Mario Fernando y Otra s/Habeas Corpus”, 16/09/1999, fallos: 322:2139. Cons. 8).

Con el paso del tiempo y la evolución de la tecnología, este derecho fue ampliándose. Hoy ya no es entendido sólo como la ausencia de información propia en manos de terceros, sino que incluye también la capacidad de control sobre esa información: ”(…) el derecho a la intimidad no podía seguir considerándose simplemente la ausencia de información acerca de nosotros en la mente de los demás (el ‘déjenme solo’), sino que debía adquirir el carácter de un control sobre la información que nos concerniera”[17].

Por su parte, según los Estándares Interamericanos elaborados por la Red Iberoamericana de Protección de Datos (2017), este derecho busca “salvaguardar el poder de disposición y control que tiene toda persona física con respecto a la información que le concierne, fundamentalmente en atención al empleo de las tecnologías de la información y las comunicaciones que cobran cada vez mayor relevancia en todos los quehaceres de la vida cotidiana” (cons. 2) por lo que es preciso reconocer “los derechos de acceso, rectificación, cancelación, oposición y portabilidad, inclusive en el contexto de tratamientos de datos personales efectuados por motores o buscadores de Internet; derechos que complementan las condiciones necesarias para que los titulares ejerzan de manera plena su derecho a la autodeterminación informativa.” (cons. 19).

En pos de ese control, existe una serie de obligaciones del Estado en materia de protección de datos personales con un vasto desarrollo a nivel internacional, que fueron también recogidas en el ordenamiento interno. Nos referimos a los principios rectores

[16] Ekmekdjian, Miguel Ángel, *Tratado de Derecho Constitucional*, Buenos Aires, Editorial Depalma, 2005, T. II, p. 375, citado en Basterra, M., Op. Cit., p. 143.

[17] Molina Quiroga, E., “Protección de datos personales como derecho autónomo. Principios rectores. Informes de solvencia crediticia. Uso arbitrario. Daño moral y material”, 2003, publicado en SAIJ.

y derechos previstos en la ley 25.326 de Protección de Datos Personales, así como a aquellos establecidos en instrumentos internacionales, algunos vinculantes para la Argentina -como el Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal, conocido como *Convenio 108*- y otros con gran peso interpretativo por tratarse de los más altos estándares en la materia -como el Reglamento General de Protección de Datos Personales de la Unión Europea (en adelante RGPD)-.

En lo que respecta al caso de autos, **nos interesa centrarnos en aquellos que refieren al acceso de los ciudadanos a datos personales y las obligaciones del Estado al respecto**, para intentar echar luz sobre qué debe informar. En otras palabras, **qué implica ese acceso.**

En primer lugar, **el derecho de acceso** se encuentra contemplado en nuestro ordenamiento en el **art. 14 de la ley 25.326**. A su vez, el art. 15 prevé lineamientos mínimos para el **contenido de la información** que el Estado debe otorgar y los medios por los que puede hacerlo. Explicita que debe ser "clara, exenta de codificaciones y en su caso acompañada de una explicación, en lenguaje accesible al conocimiento medio de la población, de los términos que se utilicen", así como "amplia y versar sobre la totalidad del registro perteneciente al titular, aun cuando el requerimiento sólo comprenda un aspecto de los datos personales".

En su decreto reglamentario nº 1.558/2001 se establece con mayor detalle el alcance de este derecho, incluyendo "**saber si el archivo está registrado conforme a las exigencias de la Ley N 25.326**" (reglamentación art. 14, inc. f.). **Vemos que el acceso previsto por la ley vigente no refiere sólo al dato personal en sí mismo sino también a las condiciones** en que se recaba, obtiene, trata, etc. En particular, reconoce de manera explícita el derecho de los titulares de conocer **cómo está registrado ese archivo y si cumple con las obligaciones que le impone la ley**. Recordemos que ésta establece, entre otras exigencias, que al registrar el archivo se informen los medios utilizados para garantizar la **seguridad** de los datos (art. 21).

En el mismo sentido regula el derecho de acceso el Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal ("Convenio 108"), vinculante para la Argentina. Y en su versión actualizada ("Convenio 108+"), que entrará en vigor próximamente[18], delinea con mayor precisión en qué consiste: aclara que, por ejemplo, el encargado del tratamiento deberá informar al titular cualquier "información adicional necesaria con el fin de **asegure el tratamiento justo y transparente de los datos personales**" (nuevo art. 8.e) y que, como contracara,

[18] 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.

que éste tiene derecho a acceder en tiempos razonables y sin gastos excesivos a "la confirmación del tratamiento de los datos personales relacionados con su persona, la comunicación en forma inteligible de los datos tratados, toda la información disponible sobre su origen, el periodo de conservación, así como **cualquier otra información que el responsable del tratamiento deba proporcionar con el fin de asegurar la transparencia del tratamiento** conforme al art. 8, párrafo 1" (nuevo art. 9.1.b).

En un sentido similar, los Estándares Interamericanos antes citados establecen que el derecho de acceso asiste a los titulares frente "cualquier información relacionada con las **condiciones generales y específicas** de su tratamiento" (art. 25).

Por su parte, **RGPD** también ofrece precisiones sobre aquello que el Estado está obligado a informar además de los datos en sí mismos. También habilita a los usuarios a conocer información sobre el tratamiento y procesamiento de sus datos, entre otra serie de cuestiones. Es importante remarcar que aclara que lo hace únicamente a título enunciativo, y que puede brindarse más información cuando sea necesario para garantizar el derecho (art. 13.2.d). Es que, de acuerdo con los considerandos de la norma, "Toda persona física debe tener derecho a acceder a los datos que se hayan recopilado en relación con ella y a poder ejercer este derecho con facilidad y a intervalos razonables, con el fin de conocer y verificar la licitud del tratamiento. (…) que el interesado pueda tener conocimiento de los mismos y verificar que son exactos y que su tratamiento se ha realizado de conformidad con la presente Directiva, de modo que, si ha lugar, pueda ejercer los derechos que esta le confiere." (cons. 43).

Así, vemos cómo la finalidad del acceso tiene que ver con la comprensión de la información personal en poder del Estado o de terceros, pero también con la capacidad de ejercer otros derechos en función de eso, es decir de controlar qué información se tiene y qué se hace con ella.

En este punto es importante detenernos en el **derecho de información.** Recogido en el art. 13 de la ley 25.326, establece el derecho a solicitar información a los organismos de control. Sin embargo, este derecho debe ser interpretado de forma amplia: siguiendo los más altos estándares internacionales, apunta a garantizar "que los usuarios reciban información clara y entendible por parte de las entidades que procesan sus datos, ya sea que estas entidades los recopilaron de manera directa o a través de terceros. Toda la información provista al usuario debe ser concisa, comprensible, y de fácil acceso, debiendo utilizar lenguaje simple y claro. Esta información debe incluir detalles sobre los datos que están siendo procesados, el propósito por el que se los procesa, y la duración de su almacenamiento, cuando corresponda"[19]. De esta forma, **es imposible disociar el derecho de acceso de aquel de información:** si así fuera, y se

[19] Access Now, "La creación de un marco para la protección de datos: una guía para los legisladores sobre qué hacer y qué no", 2018. Disponible en https://www.accessnow.org/wp-content/uploads/2018/04/manual-de-proteccion-de-datos.pdf

pensara únicamente el acceso a los datos personales *stricto sensu*, **quedarían exentas de la tutela judicial efectiva todas las circunstancias que hacen también a la información personal y a la capacidad de ejercicio de todos los derechos que se desprenden del acceso** (rectificación, oposición, supresión, cancelación, etc.).

En simultáneo, tanto la ley 25.326 (cap. II) como el Convenio 108 (cap. II), vinculante para la Argentina, y el RGPD (cap. II) y otros instrumentos internacionales establecen **principios generales** relativos a la protección de datos en el mismo sentido, llenando de contenido las obligaciones estatales en la materia. En particular, entre los deberes que la ley establece se encuentran los de **seguridad** y **confidencialidad** (arts. 9 y 10 respectivamente de la ley 25.326), que obligan al Estado tomar las medidas necesarias para procesar los datos de manera segura y protegida contra consultas o tratamientos ilegítimos o no autorizados, así como contra la pérdida accidental y destrucción o daños[20].

Finalmente, en tanto nos estamos refiriendo a principios generales que rigen el tratamiento de los datos y el derecho de acceso a las condiciones que lo rodean, cabe recordar qué se entiende por **tratamiento**: según la ley de Protección de Datos Personales se trata de "operaciones y procedimientos sistemáticos, electrónicos o no, que permitan la recolección, conservación, ordenación, almacenamiento, modificación, relacionamiento, evaluación, bloqueo, destrucción, y en general el procesamiento de datos personales, así como también su cesión a terceros a través de comunicaciones, consultas, interconexiones o transferencias." (art. 2). Este tratamiento, según los principios generales imperantes, debe ser realizado "(…) de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidentales, mediante la aplicación de medidas técnicas u organizativas adecuadas." (RGPD, art. 5.1.f).

De todo lo dicho se desprenden algunas cuestiones centrales: por un lado, el derecho de acceso no se limita a los datos personales en sentido estricto, sino que, interpretado en conjunto con el derecho de información, también abarca la posibilidad de conocer el tratamiento que se les da y la legalidad del archivo en el que se encuentran. Es que proteger la intimidad hoy en día implica asegurar la disposición y control de toda persona física de la información que le concierne. Pretender entender el acceso a los datos personales autónomamente y en sentido formal, denegando la posibilidad de conocer las condiciones en las que se encuentra, trata y resguarda no sólo desconoce la normativa vigente sino que además termina por desnaturalizarlo. Recordemos, además, que el acceso y la información son las condiciones de posibilidad para el ejercicio de otros tantos derechos con respecto a datos personales que protegen la intimidad, la libertad de expresión, la autodeterminación informacional, entre otros.

[20] Cfr. GDPR arts. 5 y 6. Para más información ver Access Now, Op. Cit., p.7.

Por otro, surge claramente entre los deberes del Estado se encuentra garantizar la confidencialidad y seguridad de los datos, así como registrar y mantener el archivo en las condiciones exigidas por la Ley Nacional de Protección de Datos Personales. Interpretando estas obligaciones en consonancia con los derechos mencionados que asisten a los titulares, **es difícil sostener que la rendición de cuentas sobre ellas pueda mantenerse por fuera del control de los usuarios. Una afirmación de tal calibre no haría más que redundar en la desnaturalización del andamiaje jurídico de protección de la privacidad y del ejercicio de los derechos que ésta habilita.**

Es que dar acceso a datos que forman parte de un conjunto que es de público conocimiento sufrió alguna clase de vulneración -como en el caso de autos- pero omitir información sobre medidas de seguridad tomadas previamente y/o en consecuencia, es hacerlo de forma **incompleta.** El efecto es tanto **la desnaturalización del derecho de acceso** en sí mismo como **la de los demás derechos que se ejercen en consecuencia**: es que "acceso" implica conocer su contenido pero también su tratamiento (incluyendo su resguardo) para poder actuar en consecuencia, siempre en pos de garantizar la privacidad, intimidad y autodeterminación informativa.

Finalmente, en este punto es esencial aclarar que no debería exigirse que los datos del titular hayan estado efectivamente entre aquellos expuestos (cuestión que, en cualquier caso, debería probar acabadamente el Estado y no limitarse a afirmarlo dogmáticamente), en tanto no hay duda sobre su pertenencia a una base de datos o conjunto de datos que fue objeto de una vulneración de seguridad, sobre la que se deberían haber tomado medidas posteriores.

ii. La finalidad de la acción de *habeas data*

La segunda cuestión discutida en el caso de autos donde nos interesa aportar argumentos tiene que ver con la procedencia de la vía del *habeas data*, previsto en el art. 43 CN. Como dijimos, se trata de ejercer el derecho de acceso e información sobre datos personales, en las condiciones en que lo prevé la ley, es decir conociendo también información sobre su tratamiento, procedencia, registro y legalidad del archivo donde se encuentran, etc.

Recordemos que esta vía representa "(…)·una especie de tutela preventiva que tiene el propósito de detener o postergar una acción previsiblemente lesiva de una garantía, confiriéndole autonomía típica a un proceso de carácter urgente" (CSJN, "Di Nunzio Daniel F. c/ The First National Bank Of Boston y otros s/Habeas Data", 21/11/2016, fallos 329:5239, cons. 6 voto del Dr. Lorenzetti).

Así, en el caso concreto, el *habeas data* no sólo sería la vía idónea por tratarse del acceso a datos personales (en sentido amplio, entendiendo todo lo que esto implica) sino también por el objetivo último que éste persigue. En palabras de la CSJN, se trata

de **la protección del derecho a la intimidad y la posibilidad de controlar la veracidad de la información y el uso que de ella se haga**, en ejercicio del derecho a la **autodeterminación informativa**. (Fallos 322:2139. Cons. 8).

Así, el Máximo Tribunal explica que el *habeas data* "(…) busca proteger la identidad personal y garantiza que el interesado -él y sólo él- tome conocimiento de los datos a él referidos y de su finalidad, que consten en registros o bancos públicos o los privados destinados a proveer informes. Constituye, por tanto, una garantía frente a informes falsos o discriminatorios que pudieran contener y autoriza a obtener su supresión, rectificación, **confidencialidad** o actualización. Se trata, pues, de una dimensión del derecho a la intimidad, en conexión de sentido con el art. 19 de la Constitución Nacional; constituye la acción que garantiza el derecho que toda persona tiene "a decidir por sí misma en qué medida compartirá con los demás sus sentimientos, pensamiento y los hechos de su vida personal" (caso "Ponzetti de Balbín", Fallos: 306:1892)." (Fallos: 322:213).

Vemos entonces cómo el fin último de esta figura es garantizar la privacidad, estableciendo una vía de acceso y de reclamo que asegure, entre otras, la confidencialidad de estos datos. Cabe preguntarse, entonces, cómo podría quedar por fuera del acceso aquello que hace a la seguridad y preservación de la confidencialidad de los datos, máxime cuando es de público conocimiento una situación que los coloca en estado de vulnerabilidad. **Dicho de otro modo, si el responsable de esos datos tiene obligaciones explícitas, si el titular de los datos tiene derecho a comprender el conjunto de datos que tiene sobre uno el Estado -en este caso- y verificar la legalidad de esa preservación, si la función del *habeas data* es el acceso en sentido amplio a información personal con el objetivo último de garantizar el derecho a la intimidad y a la privacidad, que incluye también la capacidad de controlar la información en manos de terceros, ¿qué vía procesal podría ser más idónea que esta?**

Más aún, en caso de dudas sobre la interpretación del concepto de "datos personales" que el *habeas data* busca tutelar, el Máximo Tribunal tiene dicho que la garantía de la vía expedita y rápida rige siempre que el Estado esté obligado a proporcionar datos, aunque no se trate de "datos personales" *stricto sensu*, dado que una interpretación de este tipo terminaría por negar parcialmente el derecho a la información que la Constitución busca garantizar en forma amplia, con la sola limitación de la protección de la intimidad del dueño de los datos (cfr. Fallos 321:2767, cons. 12).

De hecho, en la misma decisión la CSJN le reconoce al *habeas data* la función esencial como herramienta de control de la información propia en poder del Estado así como de sus actos públicos, en el ejercicio del principio de control público de los actos de gobierno: "(…) Dado que el hábeas data se orienta a la protección de la intimidad, el giro 'datos a ella referidos' debe ser entendido como el reaseguro del derecho básico protegido por la norma, como medio de garantizar que sea el titular de los datos el que

pueda obtener el desarme informativo del Estado, o de quien fuere, para poder decidir acerca del destino y contenido de dichos datos. **Pero, además, en tanto el texto constitucional permite ejercer un control activo sobre los datos, a fin de supervisar no sólo el contenido de la información en sí, sino también aquello que atañe a su finalidad, es evidente que se trata, a la vez, de un instrumento de control.** Por lo tanto, no es posible derivar de la citada expresión un permiso genérico para que el Estado se exima de su 'deber de información', pues ello significaría divertir su sentido fundamental." (Fallos 321:2767, cons. 13, voto del Dr. Petracchi).

En este punto, es claro que en el caso concreto una interpretación contraria -es decir, limitándolo únicamente como herramienta para el acceso a datos personales en sentido estricto y restringido- no haría más que desnaturalizar esta herramienta: ¿qué otra forma podría garantizar de forma acabada el derecho a acceder a información propia en poder del Estado, a controlar su finalidad y por lo tanto la legalidad de la actuación estatal, en resguardo finalmente de la propia privacidad?

Es que, en este sentido, entiende el Máximo **Tribunal la acción de *habeas data* tiene una doble función:** "está entrañablemente vinculada al **derecho a la intimidad**, como un instrumento destinado a evitar injerencias extrañas en la vida privada, **pero también a fin de proteger el honor, el derecho a la identidad y a la propia imagen**." (CNACAF, Sala V, "Torres Abad, Carmen c/ EN-JGM s/ habeas data", 03/07/2018, cons. V). La acción en cuestión busca no sólo efectivizar controles a los que debe someterse el estado de derecho en cuanto a la información que recopila sobre sus ciudadanos, sino que también protege el derecho a la intimidad, en **tanto su no-exhibición representa en sí misma una lesión a este derecho** (Fallos 321:2767, cons.14) por no saber qué conoce el Estado sobre uno, qué busca hacer con esa información y de qué medidas adopta para asegurar su protección.

ii.a. Derecho a la tutela judicial efectiva

Finalmente, es importante enmarcar estos estándares **en la primacía fundamental del derecho a la tutela judicial efectiva** (art. 18 CN, arts. 8 y 25 CADH) en caso de duda.

La Corte Suprema ha prestado especial atención al establecimiento de medios procesales idóneos para la protección de derechos, destacando, con cita a la Corte Interamericana de Derechos Humanos, que "*la cuestión de los medios procesales destinados a la protección y, en su caso, reparación de los derechos y libertades humanos, se erigió como uno de los capítulos fundamentales del mencionado Derecho Internacional, impulsada por dos comprobaciones elementales: por un lado, que la existencia de estas garantías constituye uno de los 'pilares básicos' del Estado de Derecho en una sociedad democrática, pero que, por el otro, 'no basta con que los*

recursos existan formalmente, sino es preciso que sean efectivos, es decir, se debe brindar a la persona la posibilidad real de interponer un recurso [...] que permita alcanzar, en su caso, la protección judicial requerida'" (Fallos: 334:1387).

El artículo 25 de la CADH apunta a proteger de manera real y efectiva a las personas frente a una vulneración de sus derechos. Para esto, exige que los Estados prevean en sus ordenamientos jurídicos recursos sencillos, rápidos y efectivos para la protección y garantía de derechos humanos. Al respecto, señala la Comisión Interamericana que "*un recurso no es efectivo cuando es 'ilusorio', demasiado gravoso para la víctima*" (CIDH, El acceso a la justicia como garantía de los derechos económicos, sociales y culturales, párr. 251).

En ese sentido, la Corte Suprema ha advertido que los jueces deben buscar soluciones procesales que utilicen las vías más expeditivas, a fin de evitar la frustración de derechos fundamentales (Fallos, 337:1361, 327:2127 y 2413; 332, 1394, entre otros), en condiciones que "*el objeto de las demandas de amparo la tutela inmediata de los derechos humanos acogidos en la Constitución Nacional*" ("Outon"- Fallos: 267:215, cons.17). De hecho, la operatividad del derecho fundamental a la tutela jurisdiccional efectiva impone al legislador la obligación de diseñar técnicas orgánico-funcionales y procesales, verdaderas y propias instituciones equilibradoras de las posiciones concretas de las partes en litigio, adecuadas para la salvaguarda de los derechos, y a los jueces el deber de prestar su protección en los casos concretos (BERIZONCE Roberto: Fundamentos y confines de las tutelas procesales diferenciadas; p. 7 y ss).

En supuestos como el presente, donde se trata de la defensa del derecho fundamental a la privacidad así como a la seguridad sobre información en poder estatal, es de suma importancia institucional la efectiva tutela judicial que asegure que los derechos no se tornen ilusorios y las personas afectadas no permanezcan en una situación de indefensión. En esta línea, nuestra Corte Suprema explicó que "*la relevancia y la delicadeza de los aludidos bienes [se refiere a la propiedad indígena] deben guiar a los magistrados no sólo en el esclarecimiento y decisión de los puntos de derecho sustancial, sino también, por cierto, de los vinculados con la 'protección judicial' prevista en la Convención Americana sobre Derechos Humanos (art. 25), que exhibe jerarquía constitucional, máxime cuando los denominados recursos de amparo, especialmente en el terreno sub examine,* ***no deben resultar 'ilusorios o inefectivos'***" (Fallos: 331:2119, el destacado nos pertenece).

Es que, tal como entiende la CSJN, "Cuando la pretensión se relaciona con derechos fundamentales, la interpretación de la ley debe estar guiada por la finalidad de lograr una tutela efectiva, lo que se presenta como una prioridad cuando la distancia entre lo declarado y la aplicación concreta perturba al ciudadano. Los jueces deben evitar interpretaciones que presenten como legítimas aquellas conductas que cumplen con la ley de modo aparente o parcial, causando el perjuicio que la norma quiere evitar."

(Fallos 329:5239, cons. 5 voto del Dr. Lorenzetti). De hecho, **este principio interpretativo se vuelve especialmente relevante en el caso concreto en tanto el Renaper no opuso excepciones a la entrega de la información que lleven a evaluar la restricción del derecho de acceso;** simplemente omitió entregarla luego de informar que el actor no se encontraba entre los titulares de datos filtrados**.** En este sentido, el Tribunal continúa explicando que "Toda la regulación relativa a la información se propone un aumento en su circulación y es contraria a su restricción. Mayor información significa mayor transparencia y menos conflictos (…) No se advierte por qué razón existe una negativa a aclarar un dato, siendo que, a un costo bajo y razonable, se evitan conflictos para terceros".

En función de lo expuesto hasta aquí, rechazar el recurso de habeas data cuando se trata de acceder a datos personales en poder del Estado y a medidas de seguridad tomadas sobre una base o archivo donde éstos se encuentran (independientemente de que hayan o no sido parte del subconjunto vulnerado), no hace más que desnaturalizar la acción y, por lo tanto, dejar sin tutela judicial efectiva al actor frente a una conducta estatal.

6. CONCLUSIÓN

Las circunstancias reseñadas en este amicus curiae tienen por finalidad aportar al tribunal elementos de convicción para la resolución del recurso basados en la evolución de la jurisprudencia y la doctrina nacional e internacional sobre la debida protección de datos personales, el alcance del acceso a ellos y la vía judicial idónea para hacerlo.

A través de lo expuesto es evidente que debe asegurarse el derecho del titular de los datos a comprender el conjunto de datos que tiene sobre él el Estado, incluyendo las medidas de seguridad para su preservación, máxime cuando éstos son parte de un conjunto que fue objeto de vulneraciones públicamente conocidas. A la vez, si la función del habeas data es el acceso en sentido amplio a información personal con el objetivo último de garantizar el derecho a la intimidad y a la privacidad, es claro que es esta la vía idónea para acceder a la información descripta, de acuerdo con la jurisprudencia nacional y los estándares internacionales aplicables.

7. RESERVA DEL CASO FEDERAL

Para el supuesto de que no se haga lugar a la intervención solicitada en calidad de amicus curiae, formulamos expresa reserva del caso federal por encontrarse en juego derechos constitucionales tales como el derecho a intimidad y a la privacidad (arts. 19 CN, 11 CADH, 17 PIDCP), así como la garantía del debido proceso (arts. 18 CN y 8 CADH)

y el derecho de peticionar a las autoridades (art. 14, CN y arts. XXIV y XVIII de la Declaración Americana de los Derechos y Deberes del Hombre).

8. PETITORIO

Por todo lo expuesto, solicitamos:

a) Se tenga a la Fundación para la Difusión del Conocimiento y el Desarrollo Sustentable “Vía Libre” por presentada en calidad de amicus curiae, y por constituido el domicilio legal denunciado.

b) Se declare la admisibilidad formal del presente amicus curiae y se tengan las presentes argumentaciones a la hora de dictar sentencia en estas actuaciones.

c) Se tengan por presentadas las copias simples que se acompañan del Estatuto y la inscripción ante la IPJ de la Fundación.

d) Se tenga presente la reserva de caso federal formulada.

Proveer de conformidad,

ES DERECHO