Omnia. Derecho y sociedad

Recibido: mayo/2024
Aceptado: julio/2024

Revista de la Facultad de Ciencias Jurídicas
de la Universidad Católica de Salta (Argentina)

Repensar el *habeas data*: análisis de los desafíos y oportunidades en la era digital

Rethinking *habeas data*: analysis of the challenges and opportunities in the digital age

Fátima López Poletti[1]

Resumen

En Argentina, el *habeas data* está garantizado por el artículo 43 de la Constitución nacional, incorporado en la reforma de 1994. La inclusión de esta cláusula en la Constitución nacional ha generado ciertas controversias que han sido superadas con la sanción de la Ley de Protección de Datos Personales 25326.

En la actualidad, sin embargo, surgen nuevos cuestionamientos que exigen una revisión del instituto. La revolución digital, en particular, ha transformado la forma en que se recopilan, procesan y comparten los datos personales. Por eso, el derecho debe adaptarse a esta nueva realidad y brindar respuestas adecuadas que garanticen la protección de la privacidad y la seguridad de las personas. Las bases sobre las cuales se erigió el instituto del *habeas data* comienzan a tambalear y reclaman, de manera imperativa, un marco normativo que brinde soluciones a los problemas contemporáneos.

En este artículo se analizará cada una de las etapas del instituto del *habeas data*. En primer lugar, se evaluará la labor de la Convención Constituyente; en segundo lugar, se abordará la cuestión sobre su reglamentación; luego, se desarrollarán las cuestiones procesales de aquel; y finalmente se examinará la protección de los datos personales en la era digital. De este modo, no se busca analizar el *habeas data* como un instituto anclado en el tiempo sino

Abstract

This analysis of the judgement "C, A. M s/ Precautionary measures - Family" file 86054/2017 of the Chamber E of the Civil National Court (June 7, 2021) proposes to consider whether it is possible to prioritize legal formal requirements — such as the prior registration in the Registry of Applicants for Guardianship with Purposes of Adoption — over over the emotional reality of a child. Specifically, in the case under study, the possibility for a foster family bein as such as the best interest of the child and the right of every human being for the State to respect and protec his or her family. This is a social unit, the family, which originates from an emotional reality and precedes its legal recognition. The Supreme Court of Buenos Aires has already stated that "(...) if the child is instrumentalized to preserve a supposed intangibility of the order established by the Registry, the values are inverted, consecrating the superior interest of the Registry, not of the child".

Keywords: *habeas data* - personal data protection - informational selfdetermination - new technologies

Derecho/ Ensayo científico

Citar: López Poletti, F. (2024). Repensar el habeas data: análisis de los desafíos y oportunidades en la era digital. *Omnia. Derecho y sociedad,* 7 (2), *pp. 139-156.*

[1] Universidad Católica Argentina (UCA).

como uno en constante desarrollo, que adquiere aún más relevancia con la consolidación de la sociedad de la información.

Palabras claves: *habeas data* - protección de datos personales - autodeterminación informativa - nuevas tecnologías

INTRODUCCIÓN

En Argentina, el *habeas data* está garantizado por el artículo 43 de la Constitución nacional (CN), incorporado en la reforma de 1994. Este artículo reconoce la facultad de toda persona de acceder a sus datos personales que se encuentren en registros o bancos de datos públicos o privados destinados a proveer informes, y a exigir su rectificación, actualización, supresión o confidencialidad, en caso de falsedad o discriminación[2].

La inclusión de esta cláusula en la Constitución nacional ha sido controvertida desde sus inicios. Entre las dudas o cuestionamientos que la doctrina y la jurisprudencia han generado se encuentran los siguientes: (i) la constitucionalidad de la cláusula, ya que la Ley 24309, declarativa de la necesidad de la reforma constitucional, no previó de manera expresa el *habeas data* como sí lo hizo con el *habeas corpus* y el amparo; (ii) su naturaleza jurídica, ya que se ha discutido si se trata de una subespecie del amparo (Corte Superior de Justicia de la Nación [CSJN], "Lascano Quintana", Fallos 324:567), un amparo especial (Bazán, 2012; Gelli, 2015, pp. 639-641; y CSJN, "Martínez", Fallos 328:797) o un proceso autónomo (Gozaíni, 1994); y (iii) la necesidad de una regulación específica del *habeas data*, en particular, si la regulación debía promoverse con carácter urgente (Leguizamón, 1999) o esperar a ver cómo funcionaba en la práctica (Puccinelli, 1995 y Toricelli, 1997), y si la regulación debía limitarse a establecer los aspectos procesales (Palazzi, 1997) o consagrar los principios rectores para la protección de los datos (Altmark y Molina Quiroga, 1996).

La mayoría de estas discusiones han perdido virtualidad con la sanción de la Ley 25326, que establece un marco normativo específico para la protección de los datos personales.

En la actualidad, sin embargo, el *habeas data* plantea nuevos desafíos. Por esa razón, en este trabajo se analizará de manera integral; no como un instituto anclado en el tiempo sino como uno en constante desarrollo, que plantea cuestiones vinculadas con su naturaleza, los derechos humanos y el aspecto procesal, y adquiere aún más relevancia con la consolidación de la sociedad de la información[3].

LA INCORPORACIÓN DEL *HABEAS DATA* EN LA REFORMA CONSTITUCIONAL DE 1994: LA CONVENCIÓN CONSTITUYENTE Y UNA FIRME DECISIÓN

La Ley 24309, que declaró la necesidad de la reforma constitucional de 1994, autorizó "la consagración expresa del *habeas corpus* y el

[2] En este sentido, Masciotra ha señalado que "el constitucionalismo latinoamericano [a diferencia del sistema europeo y estadounidense] ha consagrado el *habeas data* como un derechogarantía tendiente a proteger los datos personales, que en la estela suprema del mundo normativo integra los derechos y garantías de 'tercera generación'" (Masciotra, 2003, p. 21).

[3] La llamada "sociedad de la información" es consecuencia de la Cuarta Revolución Industrial, también conocida como "revolución digital". Según Juan Corvalán, esta última consiste en "un proceso de desarrollo tecnológico e industrial que está vinculado con la organización de los procesos y medios de producción, al igual que las tres anteriores. Los fundamentos en los que se levanta son Internet de las cosas, robótica, dispositivos conectados, sistemas ciberfísicos, cultura *market*, ciberfábrica o Smart industries, IA" (Corvalán, 2020, p. 22).

amparo, por incorporación de un artículo nuevo en el capítulo segundo de la primera parte de la Constitución nacional" (conf. inc. "n", art. 3); es decir, no hizo referencia expresa a la acción de *habeas data*. Sin embargo, la tutela de los datos personales fue tratada por la Convención Constituyente y plasmada en el tercer párrafo del artículo 43 como una especie dentro del amparo. Sobre esto, Masciotra (2023) ha dicho:

> … No obstante la ausencia de toda referencia en la norma legal que habilitaba la reforma de nuestra Carta Fundamental, en la mayoría de los convencionales —independientemente de la agrupación política que representaran— existía una clara y firme vocación tendiente a consagrar en aquella una garantía instrumental tendiente a tutelar los datos personales. Prueba fehaciente de ello, es que se presentaron veintisiete proyectos relacionados con este tema, los que ingresaron a la Comisión de Nuevos Derechos y Garantías presidida por la Convencional Elsa Pilar Barreiro de Roulet (UCR Bs. As.[4]). (Masciotra 2003, pp. 74 y 75)

Por su parte, Mazza Gigena (2019, pp. 10931094) sostiene que dicha incorporación se justificó en los siguientes motivos: (i) la experiencia del pasado en materia de intromisión estatal y violación de derechos humanos, y (ii) la aparición de nuevas tecnologías y la proliferación de la información mediante herramientas como Internet.

Finalmente, el *habeas data* se erigió como un mecanismo tendiente a preservar la memoria histórica de los/as argentinos/as (Delich, como se cita en Convención Nacional Constituyente de 1994 [CNC1994], 1994)[5]; defender los derechos de la ciudadanía frente a todo tipo de arbitrariedad o en materia de registros ideológicos, políticos, sindicales, personales o familiares que puedan afectar el derecho a la dignidad y a la propia imagen (Biazzi, como se cita en CNC1994, 1994); facilitar la búsqueda de personas desaparecidas (Cafiero, como se cita en CNC1994, 1994); y proteger el derecho a la intimidad de los riesgos producidos por la informática (Cavagna Martínez, como se cita en CNC1994, 1994).

REGLAMENTACIÓN DEL *HABEAS DATA*: ANTECEDENTES LEGISLATIVOS, LA ACTUACIÓN DE LA CSJN Y EL ESCENARIO ACTUAL

Luego de la incorporación del artículo 43 a la Constitución nacional comenzó a considerarse la necesidad de su reglamentación. En ese sentido, se presentaron numerosas iniciativas legislativas. Masciotra (2003, pp. 115 y 116) menciona, entre otras, las siguientes:

(i) en la Cámara de Diputados: el Expte. 4367-D-94, Ley Regulatoria del Derecho a la Información, de R. Sánchez Galdeano (Mov. Pop. Fueguino T. Del Fuego); el Expte. 4670D94, Régimen Regulatorio del *Habeas Data*, de Antonio M. Hernández (UCR Córdoba); el Expte. 0815-D-95 Ley de acceso a la información, Alfredo P. Bravo, (Unión Socialista Capital Federal) y otros; el Expte. 1577-D-95 Régimen Reglamentario del *Habeas Data* (art. 43 de la CN), Ricardo Molinas (Unión Socialista Santa Fe) y otros; el Expte. 1727-D-95 Régimen de protección integral del derecho a la intimidad de las personas y de acceso a la información

[4] Unión Cívica Radical, Buenos Aires.

[5] El 12 de agosto de 1994, el convencional Delich sostuvo con relación al *habeas data*: "Estamos defendiendo el derecho de los ciudadanos de proteger su intimidad para el futuro. Esta es la memoria histórica que tenemos y que exhibimos, y lo hacemos porque nos acordamos de lo que significó no tener acceso a esos archivos espantosos".

registrada sobre las mismas, reproducción del Expte. 3423-D-92, Carlos R. Álvarez (PJ Bs. As.[6]); el Expte. 1793-D-95, Régimen de informática y libertades individuales y públicas, Carlos A. Becerra (UCR Córdoba); el Expte.2474-D-95 *habeas data*, César Arias (PJ Bs. As.); y

(ii) en el Senado: el Expte. 1384D.95, Régimen de *Habeas Data* (Reglamentación del art. 43 de la CN), José A. Romero Feris (Autonomista, Corrientes); el Expte. 2006-S-95 Derecho de *Habeas Data*, Augusto Alasino (PJ, Entre Ríos); el Expte. OIll-S-96 Régimen de *Habeas Data*, Eduardo Menem (PJ, La Rioja); el Expte. 0230-S-96 Reglamentación del art. 43 de la Constitución nacional (*habeas data*), Graciela Fernández Meijide (Alianza País, Capital Federal); el Expte. 0563-S-96 Régimen sobre *Habeas Data*, Alcides H. López (UCR, Entre Ríos); etc.

Dichas iniciativas —en particular, la presentada por Alfredo P. Bravo—, fueron utilizadas como base para sancionar el Proyecto de Ley 24745, que fue vetado por el Poder Ejecutivo mediante el Decreto 1616/1996[7]. Según los considerandos del veto, la ley sancionada: (i) creó una comisión bicameral de seguimiento de protección legislativa de datos, sin especificar ni delimitar sus facultades; (ii) omitió la previsión de supuestos de excepción para la cesión o transmisión internacional de datos entre la República Argentina y otros Estados, o con organismos internacionales o supranacionales; (iii) se extralimitó al asignar nuevas funciones al defensor del pueblo; entre otros.

La demora reglamentaria fue advertida por la Corte Suprema de Justicia de la Nación (CSJN, o la Corte) en los casos "Urteaga"[8] y "Ganora"[9], donde señaló que "la falta de reglamentación legislativa no obsta a la vigencia de ciertos derechos que, por su índole, pueden ser invocados, ejercidos y amparados sin el complemento de disposición legislativa alguna". Además, agregó: "la ausencia de normas regulatorias de los aspectos instrumentales [de la acción de *habeas data*] no es óbice para su ejercicio, pues incumbe a los órganos jurisdiccionales determinar provisoriamente —hasta tanto el Congreso Nacional proceda a su reglamentación—, las características con que tal derecho habrá de desarrollarse en los casos concretos".

Finalmente, en el año 2000, se sancionó la Ley 25326[10], que estableció un marco normativo específico para la protección de los datos personales. En particular, determinó su objeto (Cap. I), reguló los principios generales en la materia (Cap. II), enunció los derechos de los/as titulares de esos datos (Cap. III), fijó el régimen aplicable a usuarios y responsables de archivos, registros y bancos de datos (Cap. IV), enunció las funciones y atribuciones de la autoridad de aplicación y control en la materia (Cap. V), determinó los distintos tipos de sanciones (Cap. VI) y reguló los aspectos concernientes a la acción judicial (Cap. VII).

[6] Partido Justicialista, Buenos Aires.

[7] Publicado en el Boletín Oficial el 30 de diciembre de 1996.

[8] CSJN, "Urteaga", Fallos 321:2767, cons. 9 y 10, 1998.

[9] CSJN, "Ganora", Fallos 322:2139, cons. 8, 1999.

[10] Dicha ley se originó en el Senado, se aprobó con modificaciones en la Cámara de Diputados, se consideró nuevamente por el primero y se promulgó parcialmente por el Poder Ejecutivo mediante el Decreto 995/2000. El presidente de aquel entonces, Fernando de la Rúa, vetó dos disposiciones referidas a la dirección y administración del órgano de control (art. 29, ptos. 2 y 3) y a una suerte de amnistía para los deudores en mora (art. 47).

NATURALEZA JURÍDICA Y OBJETO DE TUTELA. LA CUESTIÓN DE LOS RECLAMOS POR DAÑOS Y PERJUICIOS

Naturaleza jurídica

La omisión de toda referencia al *habeas data* en la Ley 24309, su ubicación constitucional y la expresión "[t]oda persona podrá interponer esta acción…", sentó las bases necesarias para que, en principio, aquella sea considerada como una especie de amparo. Es que, como señala Puccinelli (2015, p. 6), la independencia del *habeas data* "habría traído como consecuencia su inconstitucionalidad por falta de habilitación legal".

La remisión inicial a la acción de amparo generó dudas y cuestionamientos vinculados con los presupuestos exigibles para su interposición[11]. En particular, si la promoción del *habeas data* requiere acreditar una ilegalidad o arbitrariedad manifiesta[12].

Con base en estas discusiones, surgieron al menos dos grandes teorías esbozadas por la CSJN. La primera, elaborada en el caso "Lascano Quintana"[13], sostiene que el *habeas data* solo se puede interponer cuando existe arbitrariedad o ilegalidad manifiesta.

La segunda, en cambio, sostiene que tal recaudo no es exigible porque la Ley 25326, reglamentaria de tal acción, no lo demanda[14]. De este modo, el *habeas data* procede ante la mera falsedad en el contenido de los datos o la discriminación que de ellos pudiere resultar (Gelli, 2015, pp. 635656).

Derechos tutelados

Ahora bien, precisar los derechos que el *habeas data* protege no es una tarea sencilla ya que, como señala Gelli (2015, p. 651), resguarda "una multiplicidad de derechos sustantivos, tantos como pudieran verse afectados por la difusión, falsedad o efecto discriminatorio del tratamiento de [los datos personales]".

Sin perjuicio, puede afirmarse que en una perspectiva clásica, el *habeas data* protege los derechos a la privacidad, identidad y honor. En cambio, desde una perspectiva moderna, ampara la autodeterminación informativa, es decir, "el derecho a la libre disposición de los datos personales" (Gozaíni, 2023, p. 26)[15].

Masciotra (2003, pp. 128-154), en una propuesta superadora, considera que el *habeas data* debe funcionar como una garantía instrumental polifuncional, tendiente a tutelar una pluralidad de derechos, tales como la intimidad, la privacidad, la autodeterminación

[11] Para un análisis exhaustivo sobre las dudas, cuestionamientos y teorías relativas a la naturaleza jurídica del *habeas data*, véase Sacristán, E., "*Habeas data*: una especie de acción de amparo". En Cassagne, J. C. (Ed.), *Tratado general de derecho procesal administrativo,* Tomo II, 2011, pp. 663707, https://www.estelasacristan.com.ar/publicaciones/Habeas%20data%20-%20Una%20especie%20de%20accion%20de%20amparo%20-%202da%20edicion.pdf y Masciotra, 2003. Véanse referencias bibliográficas.

[12] También se ha discutido si la acción de *habeas data* es susceptible de caducidad. Al respecto, véase Puccinelli, 2015, p. 7.

[13] CSJN, "Lascano Quintana", Fallos 324:567, 2001.

[14] CSJN, "Martínez", Fallos 328:797, 2005.

[15] También se ha definido como una "serie de facultades que tiene toda persona para ejercer el control sobre la información personal que le concierne, contenida en registros ya sean públicos, privados o informáticos, a fin de enfrentar las posibles extralimitaciones de los mismos" (Tribunal Constitucional de Perú, Sala I, Pesquera Virgen del Valle SAC c/ Megatrack SAC, 2007) o como "la facultad de disponer sobre la revelación y el uso de los datos personales que integra todas las fases de elaboración y tratamiento de datos" (Masciotra, 2003, p. 139).

informativa, la verdad, la identidad, el honor, la imagen, la voz y la información.

Reclamos por daños y perjuicios

A las dificultades que plantea la precisión de los derechos tutelados por el *habeas data*, debe sumarse la cuestión sobre la posibilidad de reclamar daños y perjuicios en el ejercicio de dicha acción. Al respecto, la Sala I de la Cámara Civil y Comercial Federal sostuvo que los reclamos resarcitorios son ajenos a los fines que tuvo el legislador al crear la acción de *habeas data* y que, además, exceden el marco de la Ley de Protección de Datos Personales[16].

Corolario

A modo de conclusión, el *habeas data* es una garantía autónoma, independiente del amparo, que tiene un objeto preciso y concreto que consiste en permitir a las personas interesadas controlar la veracidad de la información y el uso que de ella se haga, sin que sea posible reclamar una indemnización por infracciones a las normas de protección de datos personales en el ejercicio de dicha acción.

GENERALIDADES: ASPECTOS PROCESALES DEL *HABEAS DATA*

La Ley de Protección de Datos Personales 25326 regula ciertos aspectos procesales de la acción de *habeas data*, a saber: cuestiones de legitimación, requisitos de procedencia de la acción, jurisdicción, competencia y procedimiento aplicable. A continuación, se abordará cada uno de ellos.

Legitimación: sujetos protegidos y obligados por la ley

La Ley 25326 reconoce una legitimación activa amplia que se proyecta en tres direcciones (art. 34). De este modo, puede promover la acción de *habeas data*:

- El afectado, sus tutores o curadores y los sucesores de las personas humanas, sean en línea directa o colateral hasta el segundo grado, por sí o por apoderado.
- Las personas jurídicas con domicilio legal o delegaciones o sucursales en el país, mediante sus representantes legales o apoderados designados al efecto.
- El defensor del pueblo, quien podrá intervenir en forma coadyuvante.

La norma prevé una limitación: la pretensión de *habeas data* no puede ser utilizada para obtener datos de terceros.

Por su parte, en relación con la legitimación pasiva, la acción procederá respecto de los responsables y usuarios de bancos de datos públicos, y de los privados destinados a proveer informes (art. 35).

Requisitos de procedencia de la acción

La acción de protección de datos personales procederá:

- Para tomar conocimiento de los datos personales almacenados en archivos, registros o bancos de datos públicos o privados destinados a proporcionar informes, y de la finalidad de aquellos.
- En los casos en que se presuma la falsedad, inexactitud, desactualización de la información de que se trata, o el tratamiento de datos cuyo registro se encuentra prohibido, para exigir su rectificación, supresión, confidencialidad o actualización.

[16] Cámara Civil y Comercial Federal , Sala I, "La Rocca, Vicente José c/ Cencosud S.A. s/ *Habeas Data* (Art. 43 CN)", 2023.

Competencia

La ley establece que será competente para entender en la acción de *habeas data* el juez del domicilio del actor, el del domicilio del demandado o el del lugar en el que el hecho o acto se exteriorice o pudiera tener efecto, a elección del actor.

Jurisdicción

Por su parte, la ley contempló la jurisdicción federal en dos casos concretos: (i) cuando la acción se interponga en contra de archivos de datos públicos de organismos nacionales, y (ii) cuando los archivos de datos se encuentren interconectados en redes interjurisdiccionales, nacionales o internacionales.

Procedimiento aplicable

La norma establece que la acción de *habeas data* tramitará según las disposiciones de la propia Ley de Datos Personales y por el procedimiento que corresponde a la acción de amparo común, y supletoriamente por las normas del Código Procesal Civil y Comercial de la Nación, en lo atinente al juicio sumarísimo.

Si bien ni el texto de la constitución ni las disposiciones de la ley reglamentaria mencionan la necesidad de agotar la vía administrativa, Mazza Gigena (2019, pp. 11051106) señala que, en la práctica, el funcionamiento de los registros públicos suele funcionar de acuerdo con su propia reglamentación interna.

OPERATIVIDAD DEL *HABEAS DATA*: TIPOS DE ACCIONES Y DATOS. BANCOS DE DATOS AFECTADOS

Para ejercer la acción de protección de datos personales a la que nos referimos en el apartado anterior, es preciso saber qué tipo de acciones existen, qué tipo de datos protege la ley y en qué bancos y bases de datos están almacenados. A continuación se abordarán dichas cuestiones.

Tipos de *habeas data*

Sagües (1997, pp. 143-146) sostiene que existen los siguientes tipos de *habeas data*:

- Informativo: es aquel que procura recabar información obrante en registros o bancos de datos públicos o privados destinados a proveer informes. Dentro de estos, incluye tres subespecies: (i) exhibitorio, que tiene por objeto tomar conocimiento de los datos registrados; (ii) finalista, que busca saber para qué y para quién se registran los datos, y (iii) autoral, tiene como fin averiguar quién obtuvo los datos obrantes en los registros o bancos.
- Aditivo: su propósito es agregar más datos a los que deberían constar en el respectivo banco o registro. Por ejemplo, en el caso de quien aparece como deudor a pesar de haber satisfecho su obligación.
- Rectificador: apunta a corregir errores en los registros o bancos. La CSJN ha fijado un límite a su interposición cuando la rectificación se orienta hacia los registros sacramentales. En el caso "R.A. c/ Arzobispado de Salta s/ *habeas data*", se consideró que la rectificación de los registros de bautismo y confirmación con motivo de adecuación al nombre e identidad de género autopercibida por su accionante es improcedente porque "implica una interferencia inaceptable en la autonomía interna reconocida [al Arzobispado]", a la libertad religiosa y de culto, y al derecho canónico[17].
- Reservador: es aquel que exige la confidencialidad de datos ciertos, pero susceptibles de causar daños.

[17] CSJN, "R.A. c/ Arzobispado de Salta s/ *habeas data*", Fallos: 346:333, cons. 9, 10 y 11, 2023.

- Cancelatorio o exclutorio: es el que busca suprimir los datos sensibles obrantes en registros o bancos.
- Mixto: aquel que comprende a más de uno de los descriptos anteriormente.

Por su parte, Andrés Gil Domínguez (2014) incorpora el concepto de *habeas data* digital (o de Internet) a la clásica tipificación y lo define como el "proceso administrativo o judicial rápido, sencillo y gratuito que tiene por objeto proteger el derecho a la intimidad en Internet mediante el bloqueo de acceso por intermedio de los motores de búsqueda de los contenidos dañosos producidos en la *web*". Además, considera que incluye las siguientes subespecies: (i) interno, (ii) administrativo y judicial, (iii) autosatisfactivo o de oficio. El apartado VII ahondará en esta cuestión.

Tipos de datos y tratamiento

La ley protege expresamente dos tipos de datos: los datos personales y los datos sensibles. Sin embargo, existe un proyecto de reforma elaborado por la Agencia de Acceso a la Información Pública que amplía dicho catálogo. Además, ambos regulan cuestiones vinculadas con su tratamiento[18].

A continuación, cada uno de los textos normativos se compara.

[18] Para acceder al proyecto de reforma, véase: https://www.argentina.gob.ar/sites/default/files/mensajeyproyecto_leypdp2023.pdf.

Tabla 1

Tipos de datos y tratamiento en la Ley 25326 y el proyecto de reforma elaborado por la Agencia de Acceso a la Información Pública

	Ley 25326	**Proyecto de reforma**
Tipos de datos	- Datos personales: información de cualquier tipo, referida a personas humanas o jurídicas determinadas o determinables; - Datos sensibles: son datos personales que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual. - Datos de acceso irrestricto: no están definidos pero su existencia surge del art. 5, pto. 2, inc. c). Son aquellos cuyo tratamiento no requiere consentimiento. Es decir, nombre y apellido, documento nacional de identidad, identificación tributaria y previsional, ocupación, fecha de nacimiento y domicilio.	• Datos personales: Información referida a personas humanas determinadas o determinables; • Datos personales sensibles: Aquellos que se refieren a la esfera íntima de su titular o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para este; • Datos biométricos: aquellos obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona humana, que permitan o confirmen su identificación única, tales como imágenes faciales o datos dactiloscópicos, entre otros; • Datos genéticos: aquellos datos relativos a las características genéticas heredadas o adquiridas de una persona humana que proporcionen una información sobre su fisiología o salud.
Tratamiento de datos - Concepto	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.	Cualquier operación o conjunto de operaciones, automatizada, parcialmente automatizada o no automatizada, realizada sobre datos personales, que permita, de manera enunciativa, la recolección, conservación, organización, estructuración, almacenamiento, modificación, relacionamiento, evaluación, bloqueo o destrucción, publicación y, en general, su procesamiento, así como también su cesión a través de comunicaciones, consultas, interconexiones o transferencias.

Tratamiento de datos personales - Requisitos	Es lícito, solo si: (i) Existe consentimiento del titular; (ii) Los datos se obtienen de fuentes de acceso público irrestricto; (iii) se recaban para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal; (iv) se trata de listados cuyos datos se limiten a nombre, documento nacional de identidad, identificación tributaria o previsional, ocupación, fecha de nacimiento, domicilio; (v) derivan de una relación contractual, científica o profesional del titular de los datos, y resulten necesarios para su desarrollo o cumplimiento; y (vi) se trata de las operaciones que realicen las entidades financieras y de las informaciones que reciban de sus clientes conforme las disposiciones de la Ley de Entidades Financieras.	Es lícito, solo si: (i) Existe consentimiento del titular; (ii) Es en ejercicio de las funciones propias del Estado y necesario para el cumplimiento de sus fines; (iii) Es necesario para el cumplimiento de una obligación legal aplicable al responsable o encargado del tratamiento; (iv) Es necesario para la ejecución de un contrato en el que el titular de los datos es parte o para la aplicación de medidas contractuales; (v) Es necesario para salvaguardar el interés vital del titular de los datos o de terceros. Este supuesto se subordina a que no prevalezcan los intereses o derechos del titular de los datos, y este se encuentre física o jurídicamente incapacitado para otorgar su consentimiento; (vi) Es necesario para la satisfacción del interés legítimo del responsable del tratamiento. Este supuesto también se subordina a que no prevalezcan los intereses o derechos del titular de los datos, particularmente cuando se trate de un niño, niña o adolescente.
Forma del consentimiento	Debe ser previo, libre, expreso e informado y debe constar por escrito o por otro medio que se le equipare, de acuerdo con las circunstancias.	Debe ser previo, libre, específico, informado e inequívoco, para una o varias finalidades determinadas, ya sea mediante una declaración o una clara acción afirmativa.
Revocación del consentimiento	Solo se admite en los casos de cesión.	Se admite en cualquier caso, excepto cuando existe un deber legal o contractual para continuar con el tratamiento de datos.

Tratamiento de datos sensibles	Es excepcional. Solo se admite cuando: (i) medien razones de interés general autorizadas por ley; o (ii) para finalidades estadísticas o científicas cuando no puedan ser identificados sus titulares. Está prohibida la formación de archivos, bancos o registros que almacenen información que directa o indirectamente revele datos sensibles. Los datos relativos a antecedentes penales o contravencionales solo pueden ser objeto de tratamiento por parte de las autoridades públicas competentes, en el marco de las leyes y reglamentaciones respectivas. Por su parte, los establecimientos sanitarios públicos o privados y los profesionales vinculados a las ciencias de la salud pueden recolectar y tratar los datos personales relativos a la salud física o mental de los pacientes que a ellos acudan o que estén o hubieren estado bajo tratamiento de aquellos, respetando los principios del secreto profesional.	Es excepcional. Solo se admite cuando: (i) Existe consentimiento del titular; (ii) Es necesario para salvaguardar un interés vital del titular de los datos y este se encuentre física o legalmente incapacitado para prestar el consentimiento. Además, es necesario que los representantes no puedan otorgar el consentimiento en tiempo oportuno; (iii) Es efectuado por establecimientos sanitarios públicos o privados o por profesionales vinculados a la ciencia de la salud con la finalidad de un tratamiento médico específico; (iv) Se realiza en el marco de actividades legítimas de una fundación, asociación o cualquier otro organismo sin fines de lucro, que tengan un objeto político, filosófico, religioso o sindical; (v) Sea necesario para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial; (vi) Tuviera una finalidad histórica, de archivo de interés público o aporte al proceso de memoria, verdad y justicia frente a crímenes de lesa humanidad; (vii) Sea necesario para el cumplimiento de obligaciones o el ejercicio de derechos en el ámbito del derecho del trabajo y la seguridad social, la salud pública y la protección social; (viii) sea necesario en el ejercicio de funciones de los poderes del Estado, en cumplimiento de sus competencias; (ix) se realiza en el marco de la asistencia humanitaria.

Bancos y bases de datos contempladas. La cuestión de los bancos de datos y las fuentes de información periodística

La reglamentación alcanza dos tipos de archivos, registros, bases o bancos de datos: los públicos, y los privados destinados a proveer informes.

A) Archivos, registros, bases o bancos de datos públicos

Es importante definir qué es un archivo, base, registro o banco público. Puccinelli (2014, pp. 13 y 14) señala que la expresión correcta es "bancos públicos de datos", ya que lo público se predica de los bancos y no de los datos. Se trata, entonces, de "bancos de datos personales de titularidad pública".

El problema radica en la tensión existente entre la publicidad que reclama el *habeas data* y el límite impuesto por el "secreto de Estado". De este modo, se ha sostenido que la información obrante en las fuerzas y organismos de seguridad no reviste carácter público por "obvias razones de seguridad"[19].

Sin embargo, la CSJN ("Ganora", 1999), reconoció el derecho a interponer la acción de *habeas data* para tomar conocimiento de los datos registrados por organismos del Estado. De este modo, si bien se reconoce la excepción impuesta por razones de seguridad pública y defensa nacional, se exige que esta sea invocada por la persona interesada y debidamente acreditada[20].

Esta discusión terminó con la incorporación del artículo 23 de la Ley de Datos Personales, referido exclusivamente a datos almacenados o registrados por fuerzas de seguridad o defensa. Así, se estableció que:

- Los datos personales que se almacenan en los bancos de datos de las fuerzas armadas, fuerzas de seguridad, organismos policiales y de inteligencia, están sujetos al régimen de dicha ley. Estos datos pueden ser: a) datos personales almacenados para fines administrativos y, b) antecedentes personales que se proporcionen a las autoridades administrativas o judiciales que los requieran en virtud de disposiciones legales.
- Las fuerzas armadas, fuerzas de seguridad, organismos policiales y de inteligencia pueden tratar datos personales sin el consentimiento de las personas afectadas, pero solo para fines de defensa nacional o seguridad pública. Los datos personales tratados deben ser necesarios para cumplir con las misiones legales de estas instituciones. Los archivos que contienen estos datos deben ser específicos y estar destinados a este propósito. También deben clasificarse por categorías, según su grado de fiabilidad.
- Los datos personales registrados con fines policiales se eliminarán cuando ya no sean necesarios para la investigación que los motivó.

B) Bancos, registros, archivos o ficheros privados

La Constitución nacional y la Ley de Protección de Datos Personales establecen que la acción de *habeas data* puede aplicarse a los bancos, registros, archivos o ficheros privados que estén destinados a proveer informes. Sin embargo, esta disposición fue ampliamente

[19] CN Crim. y Correc., sala de feria, "Ganora", 1997.

[20] En materia de derecho de acceso a la información, la seguridad pública se erige como una excepción a la publicidad. En esos casos, se exige que la procedencia de las excepciones a la publicidad esté supeditada al cumplimiento de dos principios: el de legalidad y el de proporcionalidad en sentido estricto. Al respecto, véase López Poletti, 2022, pp. 89110. https://doi.org/10.26422/RIDH.2022.1201.lop. Consúltese apartado bibliográfico.

debatida en la Convención Constituyente y generó dos posiciones sobre el alcance de la acción: una amplia y otra restrictiva.

El Decreto 1558/01 al reglamentar la Ley 25326, optó por la posición amplia. Entendió que la acción de *habeas data* también puede aplicarse a los bancos de datos privados que excedan el uso exclusivamente personal y los que tienen como finalidad la cesión o transferencia de datos personales, independientemente de que la circulación del informe o la información producida sea a título oneroso o gratuito.

Es decir, el Decreto 1558/01 incluyó tanto a los bancos de datos que proveen informes aun cuando no estén destinados a ello o que en definitiva divulguen información sin forma de informes. En definitiva, señala Puccinelli (2015, p. 15), habrá legitimación pasiva siempre que se verifique un supuesto de tratamiento que exceda el uso estrictamente personal en el sentido acordado a la garantía de inviolabilidad de los "papeles privados" acordada por el artículo 18 de la Constitución nacional.

Por último, se señala que dentro de las bases o registros privados, la ley otorgó un tratamiento especial a las siguientes categorías: (i) prestación de servicios informatizados de datos personales, (ii) prestación de servicios de información crediticia, (iii) archivos, registros o bancos de datos con fines de publicidad, y (iv) archivos, registros o bancos de datos relativos a encuestas[21].

C) Las bases de datos y las fuentes de información periodística

El *habeas data* encuentra su límite en el derecho a la libertad de expresión y de prensa, al disponer que no podrán afectarse las bases de datos ni las fuentes de información periodística[22]. Algunos autores critican esta disposición por considerar que: (i) viola la igualdad de trato, ya que excluye a los demás profesionales implicados por el secreto (Quiroga Lavié, 2003, pp. 254263); y (ii) limita la protección del *habeas data* al derecho de rectificación o respuesta, que operará una vez que la noticia se haya difundido.

Sin perjuicio, se ha concluido que el secreto de las fuentes de información periodística no es un derecho absoluto; es decir, puede ceder cuando: (i) razones de orden público de relevante jerarquía lo aconsejen (*v. gr*., sustanciación de una causa penal), (ii) no vulnera el derecho de no autoincriminarse y (iii) no afecta los límites previstos por el artículo 28 de la Constitución nacional[23].

¿UN HORIZONTE POSIBLE? LA PROTECCIÓN DE DATOS EN LA ERA DIGITAL

La revolución digital ha transformado la forma en que se recopilan, procesan y comparten los datos personales. De esta manera, se plantean escenarios no contemplados por la normativa vigente. Por eso, el derecho debe adaptarse a esta nueva realidad y brindar respuestas adecuadas que garanticen la protección de la privacidad y la seguridad de las personas.

[21] Al respecto, véase Mazza Gigena, 2019, pp. 1102-1104.

[22] Gelli (2015, p. 649), sostiene que el privilegio de los periodistas no es un fuero personal sino que opera en resguardo del descubrimiento de la verdad que, a su vez, permite investigar delitos y ejercer un control democrático sobre los actos de gobierno. Es decir, el objetivo de dicha protección consiste en favorecer el derecho de información de los ciudadanos y permitir un debate libre y desinhibido de las cuestiones de interés público.

[23] CF de San Martín, "Gorriarán", 1996.

En este sentido, se vuelve importante mencionar dos cuestiones que van en línea con dichas actualizaciones: la labor de la jurisprudencia y el proyecto de reforma de la Ley 25326 presentado por la Agencia de Acceso a la Información Pública en su carácter de autoridad de aplicación y control (conf. arts. 29 y 30, Ley 25326).

Avances jurisprudenciales

La labor jurisprudencial ha dado pasos importantes en este sentido, pues ha permitido (i) crear un nuevo tipo de *habeas data*, conocido como *habeas* Internet; (ii) evaluar cuestiones vinculadas con la actividad y la responsabilidad de los motores de búsqueda que posibilitan el acceso a los contenidos producidos en Internet; (iii) analizar el llamado "derecho al olvido" o, en palabras de Bertoni (2014), "el derecho a no ser indexado por el buscador"; y (iv) abordar el alcance de la libertad de expresión en los discursos de denuncia política con perspectiva de género formulados en redes sociales.

A) El habeas Internet

Andrés Gil Domínguez introdujo este concepto a la clásica tipificación. Según entiende, el caso "Gil Domínguez, Andrés Favio c/ Dirección General de Defensa y Protección del Consumidor del GCBA y otros s/ amparo" es un antecedente valioso en este tema. En él se ordenó a la Dirección General de Defensa y Protección del Consumidor del Gobierno de la Ciudad Autónoma de Buenos Aires que adoptara, en un plazo de 180 días, las medidas necesarias para exigir a los proveedores de servicios de búsqueda y enlaces o motores de búsqueda en Internet domiciliados en la Ciudad de Buenos Aires que incorporaran de manera obligatoria un protocolo interno de protección al derecho a la intimidad de los usuarios de Internet.

Sin perjuicio de reconocer dicho antecedente, considera que su creación jurisprudencial se consolidó con el caso "Rodríguez, María Belén". Allí, la CSJN debió resolver si los buscadores genéricos de Internet —en el caso, Google—, en tanto intermediarios, eran responsables por la información que se encontraba disponible en la *web*. Para ello, la mayoría distinguió entre los siguientes supuestos:

- Cuando el daño a la intimidad es grosero: se debe interponer un *habeas* Internet interno con el objeto de obtener el bloqueo de acceso y, si esto no sucede, el motor de búsqueda respectivo deberá responder civilmente. El factor de atribución es subjetivo.
- Cuando el daño a la intimidad es opinable, dudoso o exige un esclarecimiento: se debe interponer un *habeas* Internet judicial o administrativo, para que el juez o la autoridad administrativa competente disponga la orden de bloqueo de acceso a los contenidos lesivos.

La minoría, en cambio, defendió la idea de un *habeas* Internet autosatisfactivo o de oficio; es decir, aquel en virtud del cual el motor de búsqueda bloquea inmediatamente las publicaciones con contenido expresamente prohibido o del cual resulta una palmaria ilicitud (por ejemplo, la incitación directa y pública al genocidio).

B) Actividad y responsabilidad de los motores de búsqueda

En el caso "Rodríguez, María Belén" y "Gimbutas, Carolina", la CSJN estableció un estándar donde conviven de forma ponderada la libertad de expresión y el derecho a la intimidad en el ámbito de intermediación generado por la actividad de los motores de búsqueda. De este modo, se trata de (i) intermediarios que (ii) pueden tener responsabilidad subjetiva si " (…) una vez notificados válidamente de la infracción, no actúan con la debida diligencia".

C) Derecho al olvido

El derecho al olvido es "la facultad que tiene una persona de requerir a un buscador de Internet que desvincule, desindexe o deje de relacionar su nombre con determinados resultados de búsqueda que afectan su honor, privacidad o imagen personal" (González Tocci, 2022).

En nuestro país no está regulado normativamente pero la CSJN se expidió al respecto en el caso "Denegri"[24]. Allí debió resolver si la aplicación del derecho al olvido por parte de una persona pública (Natalia Denegri), vinculada a un asunto de interés público (caso Coppola), producido hace más de veinte años, sobre información veraz y obtenida lícitamente, implicaba una restricción indebida a la libertad de expresión.

En síntesis, se resolvió que el derecho a la desindexación no procede:

- Cuando el tratamiento de la información reviste interés público;
- Cuando la información es lícita; y
- Por el mero paso del tiempo, ya que en caso de admitirse, pondría en peligro la historia que formó parte de un debate público y la memoria social.

La CSJN entendió, por lo tanto, que en el caso no hay una real vulneración del derecho al honor que justifique un sacrificio al interés general como consecuencia de la desindexación de contenido lícito, veraz y público en los que la actora participó voluntariamente.

D) Libertad de expresión y discursos de denuncia política con perspectiva de género

La Cámara Federal de Apelaciones de La Plata, al resolver el caso "CF c/Facebook Argentina SRL s/ *habeas data*", estableció un precedente importante para la libertad de expresión en redes sociales, particularmente en lo que respecta al discurso sobre género[25].

En este caso, revocó la decisión de primera instancia que ordenó: (i) suprimir publicaciones en Facebook e Instagram de una página de una agrupación feminista donde se denunciaba a un militante político universitario como "abusador, manipulador y machista"; e (ii) informar la identidad del titular de las cuentas por las cuales se procedió a compartir tal información.

Para así decidir, entendió que:

(i) "Las manifestaciones de una agrupación que enarbola la defensa de las mujeres e identidades disidentes, denunciando que un militante se involucra en prácticas incompatibles con dichos ideales, debe considerarse un discurso amparado constitucionalmente";
(ii) se trata de "un discurso de denuncia política, no de descalificación personal" que "no (...) desnuda un hecho privado [sino que] procura exhibir la insostenible dualidad de conductas que le atribuyen a un militante propio";
(iii) el contenido de la publicación reviste interés público y se refiere a la conducta de un actor de la vida política universitaria, por lo tanto, cuenta con una protección constitucional prevalente de la libertad de expresión sobre el derecho al honor e impide su eliminación.

Proyecto de reforma de la Ley 25326

El 30 de junio de 2023, la Agencia de Acceso a la Información Pública, en su carácter de autoridad de aplicación y control (conf. arts. 29 y 30, Ley 25326), presentó un proyecto de reforma de la Ley 25326, cuya elaboración contó con diversos sectores de la sociedad por me-

[24] CSJN, "Denegri", Fallos: 345:482, 2023.

[25] Para un análisis exhaustivo de la cuestión, véase Fossaceca y López Poletti, 2020, pp. 11191142.

dio de mesas de debate y consulta pública, y siguió los lineamientos de legislaciones comparadas como el Reglamento General de Protección de Datos de la Unión Europea[26] y la Ley General de Protección de Datos de Brasil.

El proyecto consta de 83 artículos, distribuidos en 11 capítulos y se destaca por (i) incorporar los principios de extraterritorialidad, licitud, lealtad, transparencia, finalidad, minimización de datos, exactitud y seguridad; (ii) establecer reglas claras sobre la comunicación y conservación de la información crediticia; (iii) incluir los derechos de acceso, rectificación, oposición, supresión y limitación, incluso sobre decisiones automatizadas; (iv) crear la figura del delegado de protección de datos; (v) crear un registro nacional para la protección de datos personales; (vi) establecer un consejo federal para la transparencia y protección de datos personales; entre otros.

Si bien dicho proyecto ha recibido críticas —vinculadas con la falta de inclusión de definiciones clave como "nube", "exportador" e "importador" de datos, la falta de especificación respecto del tratamiento de datos alojados fuera del país y en centros de datos extranjeros, y la dificultad de implementar la figura del delegado de protección de datos personales en las pequeñas y medianas empresas (PyME)—, es un paso significativo que coloca en agenda un debate necesario: la actualización de la ley nacional a la luz del nuevo contexto internacional y tecnológico en la materia.

CONCLUSIÓN

En la sociedad de la información, el *habeas data* se erige como una herramienta constitucional importante. La privacidad informativa, la protección de los datos personales y el riesgo de que estos sean utilizados de forma indebida o abusiva justifican la decisión de la Convención Constituyente de incorporar este derechogarantía en el tercer párrafo del artículo 43.

Si bien la reglamentación establece los principales lineamientos y normas procesales que rigen la materia, la rápida evolución de las nuevas tecnologías y el flujo constante de datos personales exigen una protección más adecuada de este instituto. En efecto, la falta de una regulación específica para los casos de extracción, almacenamiento y descarga de grandes volúmenes de información en Argentina, como el *data mining* y los servicios de la nube, deja un vacío legal que puede ser aprovechado por los responsables de tratamiento de datos personales para vulnerar la privacidad de las personas.

Si bien los avances jurisprudenciales en Argentina constituyen un paso importante, no resultan suficientes para paliar las problemáticas actuales. Tal vez, el proyecto de reforma presentado por la Agencia de Acceso a la Información Pública pueda dar luz a este debate y contribuir a mejorar el marco jurídico de protección de datos personales.

[26] Al respecto, Mazza Gigena (2019, p. 1112) señala que dicho reglamento aborda varios aspectos fundamentales sobre la protección de datos. Entre ellos, señala los siguientes: (i) enumera los derechos de los titulares de los datos, (ii) establece la obligatoriedad de solicitar un consentimiento claro a la persona respecto del tratamiento de sus datos personales, el fácil acceso del interesado a sus propios datos, el derecho de rectificación, supresión y "derecho al olvido", el derecho de oponerse al uso de datos personales a efectos de elaboración de perfiles, y el derecho a la portabilidad de los datos de un prestador de servicios a otro, un método basado en riesgos (a mayor riesgo de vulnerar la protección de datos, mayor deben ser las medidas de seguridad que se implementen), la obligación de los Estados miembro de crear una autoridad de control independiente a nivel nacional y de establecer estándares comunes en los casos transfronterizos importantes en que estén implicadas varias autoridades nacionales de control.

REFERENCIAS BIBLIOGRÁFICAS

Altmark, D.; Molina Quiroga, E. (1996). Habeas data. *La Ley*, A, 1554-1569.

Bazán, V. (2012). El *habeas data* como proceso constitucional autónomo. Protección del derecho a la autodeterminación informativa. *La Ley*, A, 1052-1077.

Bertoni, E. (2014). *El derecho al olvido: un insulto a la historia latinoamericana*. http://ebertoni.blogspot.com.ar/

Convención Nacional Constituyente de 1994 (1994). *Diario de Sesiones de la Convención Nacional Constituyente,* t. IV., Sesión 3.º, Reunión 30.º, pp. 40994116, 41174154 y 41554163.

Corvalán, J. (2020). *Perfiles digitales humanos. Proteger datos en la era de la inteligencia artificial. Retos y desafíos del tratamiento automatizado*. La Ley, p. 22.

Fossaceca, C. A., y López Poletti, F., (2020). Los nuevos aires que se respiran en el derecho. *Erreius*, año 6 (12), 1119-1142.

Gelli, M.A. (2015). *Constitución de la Nación Argentina. Comentada y Concordada*, Tomo I. La Ley.

Gil Domínguez, A. (2014). La Corte Suprema de Justicia y el nacimiento jurisprudencial de habeas internet. *Revista de Derecho de Familia y las personas,* (11), 135-139.

González Tocci, L., (2022). Los contornos del derecho al olvido: breves y primeras reflexiones a propósito del caso "Denegri". *La Ley*, D, 10-12.

Gozaíni, O. (2022). Perspectiva constitucional y convencional del proceso de *habeas data*. En Falke, I., *Habeas data*. IJ Editores, pp. 15-39.

Leguizamón, H. (1999). *El habeas data como medida autosatisfactiva en el marco de un proceso monitorio* [ponencia]. XX Congreso Nacional de Derecho Procesal, Universidad de Buenos Aires, pp. 318.

López Poletti, F. (2022). El principio de proporcionalidad en el derecho de acceso a la información pública: usos y potencialidades para mitigar la discrecionalidad estatal al invocar una excepción legal. Una mirada desde el derecho argentino y la teoría de Robert Alexy. *Revista Internacional de Derechos Humanos, 12*(1), 89-110.

Masciotra, M. (2003). *El habeas data: la garantía polifuncional*. Librería Editora Platense, pp. 128164, p. 21.

Mazza Gigena, O. (2019). Protección de los datos personales: el *habeas data* y su regulación constitucional. En Gargarella, R., y Guidi, S., *Constitución de la Nación Argentina comentada,* Tomo I. La Ley, pp. 1091-1114.

Palazzi, P. A. (1997). Algunas reflexiones sobre el *habeas data* a tres años de la reforma de la Constitución nacional. *El Derecho, 134*, 939-959.

Puccinelli, O. (2015). El habeas data a veinte años de su incorporación en la Constitución Argentina. *Revista de derecho, comunicaciones y nuevas tecnologías*, (13), 425.

——— (1995). *Habeas data*: aportes para una eventual reglamentación. *El Derecho, 161*, 913930.

Quiroga Lavié, H. (2003). *Constitución de la Nación Argentina comentada.* Zavalía.

Sagüés, N. P. (1997). El *habeas data* en Argentina (orden nacional). *Ius et Praxis, 3* (1), 177191.

Toricelli, M. (1997). La idea del constituyente sobre el *habeas data*. Su posible desvirtuación por la ley reglamentaria". *Doctrina Judicial*, 1997-3-577.

JURISPRUDENCIA

(2023) CSJN, "Denegri", Fallos: 345:482, 2023.

(2023) CSJN, "R.A. c/ Arzobispado de Salta s/ *habeas data*", cons. 9, 10 y 11, 2023.

(2023) Cámara Civil y Comercial Federal, Sala I, "La Rocca, Vicente José c/ Cencosud S.A. s/ *habeas data* (Art. 43 CN)", 2023.
(2020) Cám. Fed. de La Plata, C.F. c/Facebook Argentina SRL s/ *habeas data*, 2020.
(2017) CSJN, "Gimbutas", Fallos 340:1236, 2017.
(2014) CSJN, "Rodríguez, María Belén", Fallos 337:1174, 2014.
(2005) CSJN, "Martínez", Fallos 328:797, 2005.
(2001) CSJN, "Lascano Quintana", Fallos 324:567, 2001.
(1999) CSJN, "Ganora", Fallos 322:2139, cons. 8, 1999.
(1998) CSJN, "Urteaga", Fallos 321:2767, cons. 9 y 10, 1998.
(1997) CN Crim. y Correc., sala de feria, Ganora, 1997.
(1996) CF de San Martín, "Gorriarán", 1996.

Fátima López Poletti
Perfil académico y profesional: Abogada egresada de la Universidad Católica Argentina (UCA). Maestranda en Derecho Constitucional y Derechos Humanos por la Universidad de Palermo. Diplomada en Argumentación Jurídica, Interpretación Constitucional y Valor del Precedente (Observatorio de Abogados). Docente de Derecho Constitucional en la Facultad de Derecho de la Universidad Católica Argentina (2021). Miembro de la Asociación Argentina de Derecho Constitucional.
fatimalopezpoletti@gmail.com
Identificador ORCID: 0000-0001-9883-7287