

TIPOS Y SUBTIPOS DE HÁBEAS DATA EN AMÉRICA LATINA

OSCAR RAÚL PUCCINELLI*

Sumario: 1. Marco Conceptual. 2. Tipos y subtipos de hábeas data en el derecho latinoamericano. 2.1. Hábeas data propio. 2.1.1. Hábeas data informativo: subtipos localizador, finalista, exhibitorio y autoral. 2.1.2. Hábeas data aditivo: subtipos actualizador, aclaratorio e inclusorio. 2.1.3. Hábeas data rectificador o correctivo. 2.1.4. Hábeas data exclutorio o cancelatorio. 2.1.5. Hábeas data reservador. 2.1.2.6. Hábeas data disociador. 2.1.7. Hábeas data encriptador. 2.1.8. Hábeas data bloqueador. 2.1.9. Hábeas data asegurador. 2.1.10. Hábeas data impugnativo. 2.1.11. Hábeas data resarcitorio. 2.2. Hábeas data impropio. 2.2.1. Hábeas data de acceso a información pública (hábeas data público). 2.2.2. Hábeas data replicador. 3. Conclusiones.

1. Marco conceptual

Los primeros avances tecnológicos en materia de telecomunicaciones -verificados apenas antes de que la humanidad entrase de lleno en la "era informática"-, trajeron, entre muchas cuestiones anexas, la honda preocupación por los efectos perniciosos que podrían resultar del cóctel conformado a partir de la conjunción de totalitarismos y nuevas tecnologías¹.

* Abogado. Doctor en Derecho Constitucional (UBA). Profesor de Derecho Constitucional y Derecho Procesal Constitucional y Transnacional - Universidad Nacional de Rosario (Argentina).

¹ Al respecto resulta altamente ilustrativa la ya clásica obra de Orwell, "1984", que escribiera el autor en 1948 a modo de advertencia por la vía de una suerte de exorcismo literario respecto de una sociedad antiutópica que quería desalentar.

La aparición y vertiginosa evolución del fenómeno informático llevó a la configuración de una nueva forma de poder: el “poder informático”, respecto del cual el derecho debió adoptar una postura conciliadora, esto es, legitimándolo por un lado, en virtud de los innumerables beneficios que la telemática proporciona, y conteniéndolo por el otro, debido a la exponencial potenciación de los antiguos peligros generados por los rudimentarios sistemas de registro de datos.

En esa labor de contención, en el plano jurídico se generaron nuevas herramientas a disposición de las personas, tendientes a su protección frente a los abusos de este nuevo poder, entre las cuales, a fin de garantizar judicialmente el “derecho a la protección de datos”, se creó la acción procesal constitucional de hábeas data (originada en el art. 5, numeral LXXII de la Constitución brasileña), que en la Argentina se insertó en el art. 43 constitucional, en la reforma de 1994.

2. Tipos y subtipos de hábeas data en el derecho latinoamericano

En tren de aportar a la mejor comprensión de las reales potencialidades del hábeas data como instrumento procesal constitucional, en especial respecto de su radio de acción -esto es, de las diversas pretensiones que pueden articularse por su intermedio- nos ocuparemos a continuación de evaluar las diversas especies, subespecies, tipos y subtipos de hábeas data vigentes en el derecho latinoamericano, siguiendo troncalmente la propuesta clasificatoria de Sagüés².

Advertimos que cada clasificación que se esbozará pretende cumplir fines meramente didácticos, y de ningún modo implica que los tipos y subtipos aquí mencionados constituyan los únicos posibles, ni que sean compartimentos estancos y en consecuencia deban ser utilizados aisladamente, ya que, por el contrario, pueden ser incoados dos o más de manera conjunta o sucesiva en cualquier proceso de hábeas data (v.gr., pretendiendo acceder formalmente a una información de la que ya se tomó conocimiento indirecto y, para el caso de coincidencia con lo así obtenido,

² SAGÜÉS, Néstor P., “Subtipos de hábeas data”, J.A. 20/12/95, p. 31 y ss.

formulando su cuestionamiento simultáneo -p. ej., exigiendo la rectificación de los datos, su confidencialización por tratarse de datos sensibles, y para el caso que esto último no fuera factible, su exclusión del registro-).

En una primera aproximación, los hábeas data pueden ser clasificados paralelamente en:

a) Propios (ejercidos en estricta conexión con el tratamiento de datos de carácter personal) e impropios (utilizados para resolver problemáticas conexas, pero bien diferenciables, como el acceso a la información pública o el ejercicio del derecho de réplica).

b) Individuales y colectivos (según si es ejercido a título personal o en representación de un número determinado o indeterminado de personas)³.

³ La mayoría de los hábeas data revistados son sólo ejercibles por las personas físicas o jurídicas a las que se refieren los datos respectivos (y en los ordenamientos que así lo reconocen, como el argentino, también por los sucesores universales de las personas físicas).

De allí que se aluda al hábeas data individual, por contraposición al hábeas data colectivo, ejercible no ya en tutela de un mero interés individual, sino en representación colectiva, esto es, en la intención de tutelar no ya a un solo sujeto sino también a un grupo determinado o indeterminado de personas afectadas por un tratamiento ilegal de datos de carácter personal.

Sin embargo, el hábeas data es también ejercible en representación colectiva, esto es, con el objetivo específico, del sujeto demandante, de tutelar los datos de carácter personal de un grupo determinado o indeterminado de personas afectadas (entre las que puede o no encontrarse) frente a un tratamiento indebido de datos.

En concreto, puede ser incoado tanto por la persona registrada (cuando considera que además de ella existen otras personas afectadas igualmente por un tratamiento ilegal), como por ciertas asociaciones (vulgarmente conocidas bajo las siglas ONG) constituidas en pro de determinados fines de bien común (v.gr., de defensa del consumidor, de lucha contra la discriminación, etc.) y por el defensor del pueblo (en virtud de su usual legitimación procesal a fin de tutelar judicialmente los derechos de las personas). Así, en este hábeas data no se tutela ya un mero interés individual, sino el de muchas individualidades y a la vez uno general, y por ello se acude a la representación colectiva.

Su origen fue doctrinario, en concreto a propuesta nuestra y de Palazzi, frente a la inserción del hábeas data como subtipo de amparo en la reforma constitucional argentina de 1994 (se entendió que el Constituyente, al remitir a la acción de amparo en el mismo artículo regulada -en concreto, tratada en sus especies individual y colectivo- también habilitaba ambas posibilidades del hábeas data, en especial por funcionar, al igual que el amparo colectivo, frente a supuestos de discriminación).

c) Preventivos (persiguen evitar daños no consumados) y reparadores (cuyo objetivo es el de subsanar daños ya proferidos o que se están ocasionando).

d) Ortodoxos (los estrictamente relacionados con las facultades ordinariamente conferidas a los titulares de los de datos para operar sobre éstos) y heterodoxos (los que exceden dicha tipología y que generalmente son inferidos de los principios básicos de la protección de datos, como aquellos que pudieran ser articulados por el defensor del pueblo, en tutela de derechos de incidencia colectiva, o por los responsables o usuarios de bancos de datos, articulados respecto de otros responsables o usuarios a quienes le cedieron la información y la están tratando ilegítimamente, allí estarían tutelando derechos propios y de los registrados, ya que el incumplimiento de las pautas contractuales fijadas en desmedro de éstos le significaría extender solidariamente, a tenor de ciertas disposiciones, como el art. 11, ap. 4, de la ley argentina de protección de datos personales, la responsabilidad civil y administrativa del cesionario de los datos).

A continuación nos referiremos exclusivamente a los hábeas data propios e impropios, revistan el carácter de ortodoxos o heterodoxos, preventivos o reparadores, individuales o colectivos.

2.1. Hábeas data propio

2.1.1. Hábeas data informativo: subtipos localizador, finalista, exhibitorio y autorial

El hábeas data informativo, como se anticipó, es aquél que no está destinado a operar sobre los datos registrados, sino que solamente procura recabar la información necesaria para permitir a su promotor decidir a

Luego fue reconocido normativamente de manera expresa en la Constitución venezolana de 1999, al disponer, en su art. 281, inc. 3°, que entre las atribuciones del Defensor del Pueblo se encuentra la de interponer las acciones de inconstitucionalidad, amparo, hábeas corpus, hábeas data y las demás acciones o recursos necesarios para ejercer las atribuciones señaladas en los ordinales anteriores, cuando fuere procedente de conformidad con la ley.”

partir de ésta -si es que la información no la obtuvo antes por vía extrajudicial- si los datos y el sistema de información está funcionando legalmente o si, por el contrario no lo está y por lo tanto solicitará operaciones sobre los asientos registrados o sobre el sistema de información en sí mismo. Se subdivide en tres subtipos:

a) *localizador*, destinado a indagar sobre la existencia y ubicación de bancos y bases de datos, y encuentra su razón lógica en que, para poder ejercer los derechos reconocidos por las normas protectoras de datos de carácter personal, resulta necesario previamente localizar las fuentes potencialmente generadoras de información lesiva. Varios países -v.gr., España, a través de su Ley Orgánica sobre el Régimen del Tratamiento Automatizado de Datos, de 1999, y Argentina, en su ley 25.326-, con el objeto de garantizar el ejercicio de los derechos de aquellos que se encuentren potencialmente afectados, establecen la obligatoriedad de inscribir a las bases y bancos de datos ante el órgano de aplicación de la ley.

b) *finalista*, reconocido con el objeto de determinar para qué se creó el registro, lo que permitirá luego a su promotor establecer si las categorías de los datos almacenados se corresponden con la finalidad declarada en el acto de su creación.

c) *exhibitorio*, dirigido a conocer qué datos de carácter personal se encuentran almacenados en determinado sistema de información y verificar el cumplimiento de los demás requisitos que le exige la ley para proceder a la registración de aquéllos (v.gr., consentimiento informado del interesado).

d) *autorral*, cuyo propósito es inquirir acerca de quién proporcionó los datos con que cuenta la base o banco de datos.

Desde luego, tal legitimación colectiva nunca podrá servir para acceder directamente a los datos de personas distintas del impetrante (en especial, en los casos en que es incoado por una persona física o de existencia ideal), sino para reparar lesiones de orden colectivo (cuando, v.gr., se solicita la eliminación de una determinada categoría de datos que son incompatibles con la finalidad del registro y pueden causar discriminación), en cuyo caso sólo el juez del hábeas data y en todo caso el funcionario legalmente legitimado para ello (v.gr., el defensor del pueblo, o el titular del órgano de control) podrán tener contacto con ellos (en el caso mencionado, a fin de verificar su eliminación).

De estos subtipos, el primero es ordinariamente de fuente legal, mientras que los tres restantes se encuentran regulados expresamente en las constituciones de Argentina, Brasil, Colombia, Ecuador, Guatemala, Paraguay, Perú y Venezuela. También lo prevén expresamente la Constitución de Portugal, y en el plano de nuestras autonomías locales, se encuentra regulado por las constituciones de Buenos Aires (Ciudad Autónoma y provincia), Córdoba, Chaco, Chubut, Jujuy, Río Negro, San Juan, San Luis y Tierra del Fuego.

También se refieren a ellos la ley argentina 25.326 (arts. 6, 13, 14 y 15) y la ley chilena sobre protección de la vida privada (Nº 19.628), arts. 9 y 12.

2.1.2. Hábeas data aditivo: subtipos actualizador, aclaratorio e inclusorio

El hábeas data aditivo tiene por finalidad agregar al sistema de información datos de carácter personal no asentados en éste. En este subtipo confluyen tres subtipos distintos, los dos primeros, destinados a actuar sobre los datos del interesado que ya se encuentran asentados en un banco o base de datos, y el tercero, dirigido a que los datos de aquél sean ingresados a registro en el que fueron omitidos. Así, puede aludirse al hábeas data:

a) *actualizador*, que es el diseñado para actualizar datos vetustos pero ciertos (v.gr., si alguien figura como abogado, pero ha sido designado juez, aunque el título profesional lo sigue teniendo, su perfil de ejercicio -y de identidad- es sustancialmente diferente),

b) *aclaratorio*, que es el destinado a aclarar situaciones ciertas pero que pueden ser incorrectamente interpretadas por quien acceda a los datos contenidos en el registro (v.gr., si bien un banco de datos puede coleccionar y proporcionar a terceros datos sobre las personas que han obtenido créditos comerciales y registraron atrasos en el pago, quien figure como deudor podría pretender que el banco de datos a coloque que su carácter no era de deudor principal sino de garante de la obligación contraída, o que la misma se encuentra controvertida por el deudor principal y se encuentra inhibido de cancelarla hasta tanto sea determinada su exigibilidad), e

c) *inclusorio*, cuya finalidad es la de operar sobre un registro que ha omitido asentar los datos del interesado, quien se encuentra perjudicado por dicha omisión (v.gr., el titular de un establecimiento hotelero cuyo dato no figura en un banco de datos de la Secretaría de Turismo de la Nación destinada a los turistas en los aeropuertos)⁴.

El único subtipo regulado expresamente en el plano constitucional es el hábeas data actualizador, y lo incluyen las Cartas de Argentina, Brasil, Colombia, Ecuador, Paraguay y Venezuela. También lo contienen las constituciones de Portugal y las de la Ciudad Autónoma y de la Provincia de Buenos Aires, Córdoba, Chaco, Chubut, San Juan y Tierra del Fuego.

También se refieren a ellos la ley argentina 25.326 (art. 16) y la ley chilena sobre protección de la vida privada (Nº 19.628), arts. 6 y 9.

2.1.3. *Hábeas data rectificador o correctivo*

Este subtipo está dirigido a corregir no sólo a los datos falsos (aquellos que no se corresponden siquiera mínimamente con la realidad), sino también a los inexactos o imprecisos (v.gr., el dato registrado es incompleto o puede dar lugar a más de una interpretación).

Se encuentra regulado en las constituciones de Argentina, Brasil, Colombia, Ecuador, Guatemala, Paraguay y Venezuela. Lo prevén también expresamente la Constitución de Portugal las de la Ciudad Autónoma y provincia de Buenos Aires, Córdoba, Chaco, Chubut, Jujuy, San Juan y Tierra del Fuego.

También, en el plano subconstitucional, refieren a ellos la ley argentina 25.326 (art. 16) y la ley chilena sobre protección de la vida privada (Nº 19.628), art. 6.

⁴ Apunta al respecto Bergel -citando a Roppo- que "En un cierto sentido (el derecho de inserción) es simétrico al derecho de cancelación y se funda en las circunstancias que los sujetos tienen un interés preciso en que los propios datos sean insertados en un determinado banco de datos que los omitió, insertar junto a otros datos suyos que pueden modificar su perfil o despejar dudas al respecto" (BERGEL, Salvador Darío, "El hábeas data: instrumento protector de la privacidad", en Revista de Derecho Privado y Comunitario, Nº 7, Derecho privado en la reforma constitucional, Rubinzal Culzoni, Santa Fe, 1994, p. 209).

2.1.4. *Hábeas data exclutorio o cancelatorio*

Este subtipo está diseñado a fin de eliminar total o parcialmente los datos almacenados respecto de determinada persona, cuando por algún motivo no deben mantenerse incluidos en el sistema de información de que se trate. Ello puede ocurrir en múltiples supuestos, como en el caso de la registración de cualquier tipo de datos que no se correspondan con la finalidad del banco o base de datos, de datos falsos que el registrador se niega a rectificar o actualizar, del tratamiento ilegal de los denominados "datos sensibles"⁵ (que en algunos casos no pueden ser objeto de tratamiento, y en otros sólo pueden ser tratados por escasos registros expresamente autorizados legalmente para ello, como los datos de afiliación política, por los partidos políticos), etc.

La figura se encuentra regulada expresamente en las constituciones de Argentina, Ecuador, Paraguay y Venezuela. También lo prevén las cartas de Portugal, Ciudad Autónoma y provincia de Buenos Aires, Chaco y Chubut.

Refieren a este subtipo la ley argentina de protección de datos de carácter personal (art. 16) y la ley chilena sobre protección de la vida privada (n° 19.628), art. 6.

2.1.5. *Hábeas data reservador*

Este subtipo tiende a asegurar que un dato correcta y legítimamente almacenado sea mantenido en confidencialidad y en consecuencia sólo se comunique a quienes se encuentran legalmente autorizados

⁵ Según la Declaración sobre la regulación de datos personales automatizados, adoptada por la Asamblea General de la Organización de las Naciones Unidas en su 45ª sesión ordinaria bajo el nombre de "*Directrices para la regulación de ficheros automáticos de datos personales*" los datos sensibles son ciertos tipos de datos personales cuya utilización puede dar lugar a "discriminaciones ilegales o arbitrarias". Entre los datos que no deben ser recogidos se menciona explícitamente los que hacen referencia a raza, origen étnico, color, vida sexual, opinión política, religión, filosofía y otras creencias, así como el ser miembro de asociaciones o uniones sindicales (parágr. 5). Para un análisis más particularizado ver el trabajo de Miguel A. ERMEKDJIAN y Calogero PIZZOLO, *Hábeas data. El derecho a la intimidad frente a la revolución informática*, Depalma, Buenos Aires, 1996, p. 43.

y exclusivamente en los supuestos en que tales sujetos han sido habilitados para ello.

En general -pero no exclusivamente- se vincula a los casos de datos "sensibles" (v.gr., si el Registro Nacional de Reincidencia evacuará indiscriminadamente vía Internet los informes sobre los antecedentes penales de quienes se encuentran registrados en ellos, con lo cual vulneraría las limitaciones que la ley de su creación le impone respecto de la acotación de los legitimados para acceder a ellos y las situaciones en que pueden hacerlo).

Fue incorporado por primera vez de manera expresa en el plano constitucional en la reforma constitucional federal argentina de 1994 y ha sido objeto de ciertas críticas, no por su indudable utilidad, sino por la forma de su inclusión.⁶

También pueden encontrarse previsiones que permiten configurarlo en las constituciones de Perú y Portugal y -ya en el ámbito interno argentino-, en las Cartas de la Ciudad Autónoma y provincia de Buenos Aires, Córdoba, Chaco, Chubut, Jujuy y Tierra del Fuego.

En el plano subconstitucional está regulado por la ley argentina 25.326 (arts. 8 y 10) y la ley chilena sobre protección de la vida privada (Nº 19.628), art. 7.

⁶ Bergel entiende que la confidencialidad no es meta propia de esta garantía (Salvador Darío BERGEL, *El hábeas data: instrumento protector de la privacidad*, en "Revista de Derecho Privado y Comunitario", nº 7, *Derecho privado en la reforma constitucional*, Rubinzal Culzoni, Santa Fe, 1994, p. 216). Esta posición sólo se entiende si se parte de una interpretación literalista del art. 43 de la Constitución, y se limita al hábeas data sólo cuando exista falsedad o discriminación, y se entiende que en tales casos no corresponde sino la cancelación del dato y no su confidencialización (de todas formas, nos parece que puede ser suficiente con la reserva del dato para eliminar la potencial discriminación). Palazzi, advirtiendo las deficiencias de la formulación constitucional, también indica que en el caso de falsedad tendrá sentido pedir supresión, rectificación o actualización, pero no la confidencialidad de los datos, y que cuando éstos fueron recabados con el propósito de discriminar, el paso más lógico parece el de pedir la supresión del dato (Pablo A. PALAZZI, *El hábeas data en la Constitución nacional. (La protección de la privacidad en la "era de la información")*, "L.L.", 20/12/94, p. 14).

2.1.6. *Hábeas data disociador*

Ordinariamente, las normas sobre protección de datos de carácter personal (y también otras, como las que regulan el secreto estadístico), prevén la posibilidad de que uno o más datos referidos a una persona determinada pueda ser valorado dentro de determinados parámetros (v.gr., pertenencia grupal, ubicación social, sexo, edad, estado de salud, etc.), pero sin que quien opera sobre los mismos tenga acceso a conocer la identidad de la persona a la cual se refieren esos datos. Esto se hace a partir de un proceso de desvinculación del dato mediante técnicas de disociación, que como regla no deben permitir la identificación de quien fue registrado. La falta de cumplimiento de estas normas habilita al perjudicado a plantear un hábeas data disociador, precisamente para que ese dato sea sometido a las técnicas correctas que aseguren el cumplimiento de la finalidad legal.

Este subtipo tiene similitud con los hábeas datas reservador y exclutorio, por cuanto en definitiva apunta a que los datos en cuestión puedan ser valorados dentro de determinados parámetros -aunque sin conocer la identidad del registrado- y a que se eliminen las referencias de esos datos respecto del promoviente, pero difiere de ellos en cuanto a que no necesariamente implica la eliminación de un dato del registro ni su confidencialización, sino su transformación en otro respecto del cual no puede predicarse la identidad de su titular.

Entre sus diversas utilidades puede ser eficaz para, por ejemplo, contrarrestar violaciones a las normas que autorizan a recoger datos anónimos con fines epidemiológicos (v.gr., comunicación de enfermos de sida en los términos que impone la ley 23.798, es decir, codificados de manera que no pueda predicarse precisamente el titular de los datos).

Se refiere a la disociación de datos la ley argentina 25.326 (arts. 11 y 28), y también la ley chilena sobre protección de la vida privada (n° 19.628), art.3.

2.1.7. *Hábeas data encriptador*

Más allá del derecho a que determinados datos sean reservados o disociados, en algunos supuestos, y a fin de brindar mayor seguridad y agilidad a la operación sobre determinados datos, puede ser necesario acudir a técnicas de encriptación, lo que implica en definitiva otra pers-

pectiva, donde el dato está de algún modo oculto, y sólo puede ser conocido por quienes cuenten con la clave para descifrarlos⁷.

Este subtipo entonces está dirigido a que se lleve a cabo tal tarea de encriptación, y no cuenta hasta el momento con reconocimiento legal expreso en el ámbito latinoamericano.

2.1.8. *Hábeas data bloqueador*

Muy emparentado al hábeas data reservador y al exclutorio se presenta un subtipo ligeramente distinto, que pretende “trabar” el tratamiento -generalmente en lo relativo a la transmisión o cesión a terceros- de los datos asentados en un registro.

Ese impedimento de comunicación de los datos puede o no ser temporalmente limitado, según las circunstancias. El bloqueo transitorio comúnmente se peticiona y ordena judicialmente como medida cautelar dentro del marco de una pretensión de fondo que, para que no se frustre, requiere de esa traba (v.gr., por la que se pretende la eliminación de un dato discriminatorio), mientras que el bloqueo definitivo ordinariamente surgirá de una decisión de fondo por la que no pueda solicitarse la eliminación del dato, pero sí su bloqueo por haber expirado el tiempo legal para su comunicación generalizada a terceros.

La ley argentina de protección de datos personales prevé el primero de estos supuestos (art. 38), y se refiere a éste la ley chilena sobre protección de la vida privada (n° 19.628), en el art. 6.

2.1.9. *Hábeas data asegurador*

Uno de los más importantes principios relativos al tratamiento de datos es el que indica que, para que un tratamiento sea legal, debe garan-

⁷ Según Villalobos, encriptación “es el proceso de convertir un mensaje en texto cifrado, utilizando una clave. De esta manera, el mensaje se hace ilegible por los símbolos y grafías aparentemente sin sentido que contiene. Sin embargo, el destinatario, que se supone tiene otra clave similar, puede descifrarlo.” (VILLALOBOS A., Edgardo A., *Diccionario de Derecho Informático*, Panamá, 2002, p.71).

tizarse la seguridad de los datos, pues de nada sirve que se reconozcan los derechos a operar sobre los bancos de datos si los procedimientos técnicos utilizados para dicho tratamiento permiten fugas o alteraciones ilegales de la información almacenada.

Por tal motivo, cabe la utilización de este subtipo para lograr la constatación judicial de las condiciones en que opera el sistema de información que contiene los datos y -en su caso- la imposición de condiciones técnicas mínimas de seguridad para que se pueda proseguir con el tratamiento de datos de carácter personal, bajo apercibimientos de cancelación del registro o bien de exclusión de los datos en él registrados.

El hábeas data asegurador se asimila al reservador por cuanto ambos persiguen la efectiva vigencia de la confidencialidad y permiten el control técnico de la actividad del registrador, pero es de otro lado más amplio en el sentido de que no opera sólo respecto de datos confidenciales, sino de cualquier tipo de datos.

La ley argentina de protección de datos personales prevé este supuesto (art. 9), y la ley chilena sobre protección de la vida privada (nº 19.628), lo trata en su art. 11.

2.1.10. Hábeas data impugnativo

Las normas sobre protección de datos suelen prever el derecho del registrado a impugnar las valoraciones que de sus datos realice el registrador, como asimismo a que se adopten decisiones judiciales o administrativas con único fundamento en el resultado del tratamiento informatizado de datos de carácter personal que suministren una definición del perfil o personalidad del interesado.

Este subtipo presenta cierta similitud con el hábeas data rectificador o correctivo, si por vía de esa impugnación se pretende establecer una conclusión distinta a la que aparece en el registro, y con el exclutorio, cuando a través de esa impugnación se persigue la eliminación total de dicha valoración o decisión.

La ley argentina de protección de datos personales prevé el derecho de impugnación de las valoraciones personales en su art. 20.

2.1.11. *Hábeas data resarcitorio*

Este subtipo, al que rotulamos resarcitorio aunque preferiríamos denominarlo “reparador” -pues se vincula con lo que los iusprivatistas denominan actualmente *derecho a la reparación*⁸, pero no recurrimos a tal rótulo a fin no confundirlo con la clasificación entre hábeas datas preventivos y reparadores-, tiende precisamente a lograr la satisfacción de indemnizaciones, y en los países que ello es factible -en la mayoría de los ordenamientos que regulan el hábeas data o las acciones procesales constitucionales por las que se vehiculiza el derecho a la protección de datos no pueden articularse pretensiones resarcitorias-, suele utilizarse conjuntamente con otras pretensiones conexas, como la rectificación o exclusión de los datos.

La Constitución del Ecuador lo prevé de manera expresa al regular el hábeas data, y en Colombia se han admitido regularmente acciones de tutela frente a la violación del “derecho de hábeas data” donde se pretendían indemnizaciones por los perjuicios sufridos por el accionante.

Asimismo, algunas leyes sobre protección de datos también se ocupan de destacar la pertinencia de la reparación de los daños causados por la violación de las normas del derecho a la protección de datos (v.gr., el art. 19 de la ley española 15/99 de protección de datos de carácter perso-

⁸ Desde el ángulo lexicológico, preferimos utilizar el término *reparación*, pese a que suele aludirse a un “derecho de daños” y también existen otros términos que ordinariamente suelen ser utilizado como sinónimos del que proponemos (v.gr., *indemnización* o *resarcimiento*). En esta inteligencia, la voz “reparación” nos parece conceptualmente más apropiada, especialmente porque el término *indemnización*, a pesar de que lexicológicamente pareciera cubrir todos los daños ocasionados (indemne: sin daño), ello no siempre es así (v.gr., en el caso de las expropiaciones si bien se exige la indemnización previa y justa, la extensión del resarcimiento es más limitado). El término *reparación* nos da la idea de que su objetivo esencial es el de llevar las cosas al estado lo más similar posible al anterior al momento en que se produjo el daño, aunque, por cierto, no en todos los casos borra la totalidad de los aspectos que fueron modificados por efecto del hecho, acto u omisión generadora del daño. De otro lado, la *indemnización* suele ser asociada más a la compensación pecuniaria, que a las otras formas de reparación y la voz “reparación” tiene tres acepciones, que incluye a esta última: arreglo de años o averías; satisfacción tras ofensa o agravio; indemnización (OSSORIO, Manuel, *Diccionario de ciencias jurídicas, políticas y sociales*, Heliasta, 1986, p. 663).

nal; el art. 31 de la ley argentina de protección de datos personales, y la ley chilena sobre protección de la vida privada, art. 11).

2.2. *Hábeas data impropio*

El hábeas data impropio, como se adelantó, no está dirigido a la protección de datos de carácter personal asentados en bases o bancos de datos, sino a obtener información pública que le es indebidamente negada al legitimado activo, o replicar información de carácter personal difundida a través de los medios de difusión tradicionales.

Puede estar regulado de manera conjunta con reglas sobre protección de datos de carácter personal, como ocurre en las Constituciones de Perú y Venezuela, o bien independientemente de ellas.

2.2.1. *Hábeas data de acceso a información pública (hábeas data público)*

Como ya fuera expresado inicialmente, algunas constituciones (como las de España y -en el plano interno argentino-, las de las provincias de Chaco, Formosa, Río Negro, San Luis y San Juan), contienen reglas que garantizan el libre acceso a la información pública (que en algunos casos incluso declaran restringibles si hubiera en juego asuntos vitales para la seguridad del Estado, como en las constituciones de San Juan y Perú). Adicionalmente, algunas constituciones establecen acciones procesales constitucionales específicas para su tutela, dentro de las cuales la del Perú adjudica al hábeas data tal naturaleza protectoria.

Algunos autores rotulan a este tipo de hábeas data impropio como “hábeas data público”, pero tal denominación nos parece que puede llevar a confusión por no ser claramente definitoria de sus alcances.

2.2.2. *Hábeas data replicador*

La única constitución que previó al hábeas data como medio de ejercicio del derecho de réplica fue la carta peruana de 1993, que en su art.

200 inc. 3 dispuso que la acción de hábeas data procedía, entre otros supuestos, contra el hecho u omisión por parte de cualquier autoridad, funcionario o persona, que vulnera o amenaza los derechos “Al honor y a la buena reputación, a la intimidad personal y familiar así como a la voz y a la imagen propias. Toda persona afectada por informaciones o agravada en cualquier medio de comunicación social, tiene derecho que éste se rectifique en forma gratuita, inmediata y proporcional, sin perjuicio de las responsabilidades de ley”.

3. Conclusiones

En el derecho latinoamericano coexisten actualmente múltiples e interesantes variantes de un instituto que (ya sea reconocido como derecho o como acción procesal constitucional), pese al escaso tiempo transcurrido desde su aparición, se ha desplegado vertiginosamente, emergiendo como un instrumento altamente garantizador de los derechos amenazados por el indebido tratamiento de los datos de carácter personal.

Tal vez las diferencias regulatorias aquí revistadas sean precisamente las que, en ese rápido despliegue, han provocado confusiones conceptuales, y en ocasiones han llevado a amputaciones inaceptables del derecho a la protección de datos (y en especial, del hábeas data), pero el saldo es positivo y esperanzador.

Obvio es que resta mucho por hacer, pero las experiencias relatadas han servido y sirven de formidable plataforma para las regulaciones por venir, que deben rápidamente superar las todavía tímidas regulaciones nacionales -no sólo del derecho a la protección de datos de carácter personal, sino también de los derechos de acceso a la información pública y de réplica- existentes en América Latina.

Desde luego, en ese tránsito no debe perderse la perspectiva de la necesidad urgente de adoptar una convención regional relativa a la protección de datos de carácter personal, que ayudará a la homogeneización de criterios y a brindar mayor seguridad al tratamiento de éstos en nuestras sociedades.