EDITORIAL ASTREA

*Tipos y subtipos de hábeas data en América latina**

Por Oscar R. Puccinelli

1. Marco conceptual

Los peligros que desde siempre conllevó la compilación y sistematización de datos de carácter personal para las libertades individuales se reavivaron fuertemente promediando el siglo XX, cuando frente a los primeros avances tecnológicos en materia de telecomunicaciones –verificados apenas antes de que la humanidad entrase de lleno en la "era informática"–, las sociedades desarrolladas comenzaron a preocuparse por los efectos perniciosos que podrían resultar del cóctel conformado a partir de la conjunción de totalitarismos y nuevas tecnologías[1].

La inmediata aparición y vertiginosa evolución del fenómeno informático llevó a la configuración de una nueva forma de poder: el "poder informático", que como toda manifestación de aquél, no fue indiferente al derecho, que en definitiva debió adoptar una postura concertadora, 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, en concreto y fundamentalmente puestas a disposición a partir de dos fenómenos principales: la creación de un nuevo derecho con contenidos diferenciales respecto de otros de los que puede aparecer como una mera escisión (el derecho a la protección de datos) y la formulación de reglas específicas tendientes a la protección de las personas frente a los abusos de este nuevo poder. Ambos aspectos, en definitiva, provocaron acaso el nacimiento de una nueva rama del derecho, el derecho de la protección de datos.

En efecto, en cuanto a la creación de un nuevo derecho, de la antigua matriz del derecho a la intimidad se desprendieron otros conceptos, como el de "autodeterminación informativa" o "autodeterminación informática", "libertad informática", *information control*, "hábeas data" –entendido éste como "derecho" y no, como preferimos por resultar más propio y fiel a su concepción originaria, como acción procesal constitucional–, etc.[2], los que a nuestro criterio no son más que aspectos integrantes

---

* Bibliografía recomendada.

[1] Al respecto resulta altamente ilustrativa la ya clásica obra de Orwel, *1984*, que escribiera en 1948 a modo de exorcismo literario de una sociedad antiutópica que quería evitar se configurara.

[2] La doctrina española alude a la libertad informática como un nuevo derecho fundamental, propio de la tercera generación, que tiene por finalidad "garantizar la facultad de las personas de *conocer y acceder* a las informaciones que les conciernen, archivadas en bancos de datos; *controlar* su calidad, lo que implica la posibilidad de corregir o cancelar los datos inexactos o indebidamente procesados, y *disponer* sobre su transmisión" (Pérez Luño, Antonio E., *Los derechos humanos en la sociedad tecnológica*, en Losano, Mario y otros, "Libertad informática y leyes de protección de datos personales", Madrid, Centro de Estudios Políticos y Constitucionales, 1989, p. 140, citado en *Hábeas corpus, amparo, hábeas data y acción de cumplimiento: normatividad vigente*, Comisión Andina de Juristas, Lima, 1994, p. 12). También como "el control que a cada uno de nosotros nos corresponde sobre la información que nos concierne personalmente, sea íntima o no, para preservar de este modo y en último extremo, la propia identidad,

de un derecho aún más amplio, el "derecho a la protección de datos", que, como dijimos, conjuntamente con aquellas otras reglas y ciertos elementos adicionales conforman el "derecho de la protección de datos", que es definido por Hondius como "aquella parte de la legislación que protege el derecho fundamental de libertad, en particular el derecho individual a la intimidad respecto del procesamiento manual o automático de datos"[3].

Desde luego, tanto el derecho *de* la protección de datos como el derecho *a* la protección de datos, en rigor técnico no tienden, como pareciera sugerir su rotulación, a la protección del dato en sí, sino a los derechos que pueden ser lesionados a partir de su desprotección –como el honor, la intimidad, la autodeterminación informativa, etc.–, por lo que son meramente instrumentales[4].

Así las cosas, se propone entender por "derecho a la protección de datos" a la suma de principios, derechos y garantías establecidos en favor de las personas que pudieran verse perjudicadas por el tratamiento de los datos de carácter personal a ella referidos, con lo cual, al decir de Pérez Luño, "la protección de datos personales tendría por objeto prioritario asegurar el equilibrio de poderes *sobre* y la participación democrática *en* los procesos de la información y la comunicación a través de la disciplina de los sistemas de obtención, almacenamiento y transmisión de datos"[5], y por lo tanto protegería "el conjunto de bienes o intereses que puedan ser afectados por

---

nuestra dignidad y libertad" (Murillo de la Cueva, Pablo L., *Informática y protección de datos personales*, Madrid, Centro de Estudios Políticos y Constitucionales, 1993, p. 33, citado por Armagnague, Juan F., *Protección del administrado*, Bs. As., Ciudad Argentina, 1996, p. 173 y 174).

[3] Hondius, Frits W., *A decade of international data protection*, "Netherlands of International Law Review", vol. 30, n° 2, 1983, p. 105.

[4] Se alude a su instrumentalidad, porque sirven de medio para la tutela de otros derechos implicados. Esto es, el derecho a la protección de datos no por ser protector de otros pierde la categoría de derecho –y en ello está conteste la doctrina–, pues no alcanza a reunir las notas típicas de la moderna concepción de las garantías.

Es que pese a que muchos de los denominados "derechos" que poseen tal carácter instrumental son en realidad garantías, en virtud de constituir en sí el medio técnico de tutela de ciertos derechos para cuya protección han sido creados (v.gr., el "derecho de réplica" y el "derecho de huelga"), en este caso el derecho a la protección de datos contiene reglas de fondo propias y es tutelable a través de ciertas garantías específicamente creadas para ello (v.gr., administrativas, como la Comisión Nacional de Informática y Libertades francesa, o jurisdiccionales, como el hábeas data brasileño).

En este sentido, resulta clarificador lo señalado recientemente por Bidart Campos, cuando sostuvo: "Dentro del ámbito tutelar de los derechos personales, y en afinidad con las garantías clásicas frente al Estado, hay 'derechos' denominados tales que, en rigor, sirven y se usan para la defensa de otros derechos; a aquellos denominados derechos que se dirigen a proteger otros derechos se les asigna la categoría y naturaleza de garantías… Por otro lado, también interesa captar que hay en el rubro clásico de los derechos, algunos llamados tales y definidos como tales que, por servir para defensa y tutela de otros derechos, exhiben un rostro garantizador y una semejanza con las garantías personales. En este último caso –ejemplo de los derechos de huelga y de réplica–, sugerimos una alternativa: *a*) o decir que son realmente derechos cuyo ejercicio ampara a derechos distintos, con lo que entre los derechos habría que computar una categoría enderezada a no agotar un derecho en su propio ejercicio sino a verlo como instrumento 'garantizador' de otro u otros derechos; *b*) o decir que no son realmente derechos aunque así se los apode y se los incluya en el rubro de los derechos, sino que son verdaderas garantías en cuanto mecanismos protectores de derechos" (Bidart Campos, Germán J., *Repensando las garantías constitucionales*, *LL*, 1991-B-977 y 978).

[5] Pérez Luño, Antonio E., citado por Zúñiga Urbina, Francisco, *El derecho a la intimidad y sus paradigmas*, "Ius et praxis", Facultad de Ciencias Jurídicas y Sociales de la Universidad de Talca, Chile, año 3, n° 1, "Derecho a la autodeterminación informativa y acción de hábeas data en Iberoamérica", 1997, p. 300 y 301.

la elaboración de informaciones referentes a personas identificadas o identificables"[6].

Y ese derecho a la protección de datos sería a su vez tutelable por diversas vías (v.gr., normativas, judiciales y administrativas), entre las cuales se cuentan los procedimientos secretos de carácter judicial o administrativo (v.gr., Const. de Brasil de 1988, art. 5°, § LXVII) y la acción procesal constitucional de hábeas data (art. 5°, § LXXII de la misma Const. brasileña, entre otras regulaciones), cuya misión consiste en brindar protección inmediata y efectiva a los derechos fundamentales afectados por las prácticas de almacenamiento, procesamiento y suministro de datos[7], y que en algún caso (v.gr., versión original del art. 200 de la Const. peruana de 1993) se extiende excepcionalmente a tutelar los derechos de acceso a la información pública y de "réplica" –este último instituto, en realidad configura una verdadera garantía antes que un derecho, pues, al igual que el hábeas data, es un mecanismo de tutela de otros derechos que no se sostendría si éstos desaparecieran, y por lo tanto, debido a sus especiales características, reclama un cauce procesal propio–.

A estos mecanismos de tutela propios del derecho de la protección de datos, se los puede encontrar incorporados en el plano constitucional o legal, según el ordenamiento de que se trate, pero cabe destacar que a partir de su recepción en el plano constitucional de la década del 70 por Portugal[8] y España[9], los constituyentes latinoamericanos de la década posterior si bien consagraron inicialmente reglas similares, luego fueron dotándolas de rasgos autóctonos que distinguieron a sus consti-

[6] Pérez Luño, *Los derechos humanos en la sociedad tecnológica*, en Losano y otros, "Libertad informática y leyes de protección de datos personales", p. 139.

[7] Cabe recordar que el concepto de protección de datos ha variado, pues en los primeros años de aplicación de las leyes de protección de datos la discusión se centraba en la antítesis "vida privada versus computadoras". En el actual estado tecnológico, la protección de datos es una síntesis de los intereses individuales y sociales en juego (Sieghart, Paul, *Legislation and data protection. Proceedings on the Roma Conference of problems relating to the development and aplication of legislation on data protection*, Council of Europa, Camera dei Deputati, Roma, 1983, p. 16, citado por Correa, Carlos y otros, *Derecho informático*, Bs. As., Depalma, 1994, p. 249).

[8] "Art. 35. *1*) Todos los ciudadanos tienen derecho a tomar conocimiento de los datos constantes en ficheros o registros informáticos a su respecto y del fin a que se destinan, pudiendo exigir su rectificación y actualización, sin perjuicio de lo dispuesto en la ley sobre secreto de Estado y secreto de justicia.

2) Es prohibido el acceso a ficheros y registros informáticos para conocimiento de datos personales relativos a terceros y respectiva interconexión, salvo en casos excepcionales previstos en la ley.

3) La informática no puede ser utilizada para el tratamiento de datos referentes a convicciones filosóficas o políticas, filiación partidaria o sindical, fe religiosa o vida privada, salvo cuando se trate de procesamiento de datos estadísticos no individualmente identificables.

4) La ley define el concepto de datos personales para efectos de registro informático, bien como de bases y bancos de datos y respectivas condiciones de acceso, constitución y utilización por entidades públicas y privadas.

5) Es prohibida la atribución de un número nacional único a los ciudadanos.

6) La ley define el régimen aplicable a los flujos de datos trasfronteras, estableciendo formas adecuadas de protección de datos personales y de otros cuya salvaguarda se justifique por razones de intereses nacionales".

(La versión original prescribía: "Todos los ciudadanos tendrán derecho a tomar conocimiento de lo que conste en forma de registros mecanográficos acerca de ellos y de la finalidad a que se destinan las informaciones, y podrán exigir la rectificación de datos, así como su actualización. No se podrá utilizar la informática para el tratamiento de datos referentes a convicciones políticas, fe religiosa o vida privada, salvo cuando se trate de la elaboración de datos no identificables para fines estadísticos. Se prohíbe atribuir un número nacional único a los ciudadanos").

[9] Art. 18, inc. *4*) "La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos".

tuciones por la consagración de mecanismos específicos tendientes a la efectiva protección de aquel derecho.

2. Evolución del hábeas data y del derecho a la protección de datos en América latina

A fin de brindar un panorama de la forma en que ingresó y se fue enraizando el derecho a la protección de datos de carácter personal en América latina, dividiremos nuestro análisis primeramente respecto de la situación de los países que cuentan con regulación constitucional de aspectos relativos a aquél, para luego hacer una breve referencia a aquellos que, si bien no cuentan con regulación específica en aquél plano, sí han incorporado disposiciones subconstitucionales.

a) Países que afrontaron constitucionalmente la regulación del derecho a la protección de datos o del hábeas data

El primer país americano en incorporar constitucionalmente disposiciones específicas fue Guatemala, que en su Constitución de 1985, dispuso: "art. 31. Toda persona tiene el derecho de conocer lo que de ella conste en archivos, fichas o cualquier otra forma de registros estatales, y la finalidad a que se dedica. Quedan prohibidos los registros y archivos de filiación política, excepto los propios de las autoridades electorales y de los partidos políticos".

Luego, en la Const. de Nicaragua de 1987, se estableció: "art. 26. Toda persona tiene derecho: *1*) A su vida privada y la de su familia. *2*) A la inviolabilidad de su domicilio, su correspondencia y sus comunicaciones de todo tipo. *3*) Al respeto de su honra y reputación. *4*) A conocer toda información que sobre ella hayan registrado las autoridades estatales, así como el derecho de saber por qué y con qué finalidad tiene esa información".

Un año más tarde, la Const. del Brasil de 1988 modificará esa tendencia –proveniente, como se dijo, de las constituciones de Portugal y España– de establecer únicamente un derecho de control sobre los datos de carácter personal o de pregonar que la informática no debe afectar a la intimidad de las personas –aunque sin establecer los principios relativos al tratamiento de los datos ni reconocer expresamente un derecho al control de los mismos–, reconocerá por primera vez una garantía específica del derecho a la protección de los datos, bautizándola "hábeas data", en clara simetría con la acción de hábeas corpus –como se observará sólo a estas dos acciones se las reconoce como "gratuitas"–.

Entre las disposiciones aplicables, cabe citar las siguientes: "art. 5°. Todos son iguales ante la ley, sin distinción de cualquier naturaleza. Se garantiza a los brasileños y a los extranjeros residentes en el país la inviolabilidad del derecho a la vida, a la libertad, a la igualdad, a la seguridad y a la propiedad, en los términos siguientes:... LXXI. Se concederá hábeas data: *a*) para asegurar el conocimiento de informaciones relativas a la persona del impetrante, que consten en registros o bancos de datos de entidades gubernamentales o de carácter público; *b*) para rectificar datos, cuando no se prefiriera hacerlo por procedimiento secreto, judicial o administrativo".

"LXXVI. Son gratuitas las acciones de hábeas corpus y hábeas data en la medida que la ley disponga los actos necesarios para el ejercicio de la ciudadanía. *1*) Serán de aplicación inmediata las normas definidoras de los derechos y garantías fundamentales. *2*) Los derechos y garantías indicados en esta Constitución no excluyen otras que deriven del régimen y principios adoptados por ella o de los tratados internacionales en que la República Federativa del Brasil sea parte".

Además de estas normas, que regulan el núcleo esencial del hábeas data brasileño, la Carta trae otras, reguladoras de aspectos secundarios, relativos a la competencia judicial para el juzgamiento de acciones de este tipo[10].

Como se habrá observado, la Constitución brasileña no trazó un dispositivo autónomo que contemplara el derecho de conocer y de rectificar datos de carácter personal, sino que ese derecho fue otorgado en el mismo dispositivo que instituye el remedio de su tutela[11].

La norma tuvo una finalidad particular y distintiva, que, como lo explica Othon Sidou, implica el derecho fundamental del individuo de conocer las informaciones manipuladas y ocultas en los archivos de inteligencia gubernamental, por lo general distorsionadas u obtenidas por métodos arbitrarios[12], y responde a lo explicado por

[10] Art. 102. Compete al Supremo Tribunal Federal, principalmente, la guarda de la Constitución, cabiéndole:

I. Procesar y juzgar, originariamente:

d) el hábeas corpus, siendo paciente cualquiera de las personas referidas en los párrafos anteriores; el mandato de *segurança* y el hábeas data contra actos del presidente de la República, de las Mesas de la Cámara de Diputados y del Senado Federal, del Tribunal de Cuentas de la Unión, del procurador general de la República y del propio Supremo Tribunal Federal.

II. Juzgar, en recurso ordinario:

a) el hábeas corpus, el mandato de *segurança*, el hábeas data y el mandato de *injuncao* decididos en única instancia por los Tribunales Superiores, si la decisión fuere denegatoria.

Art. 105. Compete al Tribunal Superior de Justicia:

I. Procesar y juzgar, originariamente:

b) los mandatos de *segurança*, los hábeas data contra acto de Ministro de Estado o del propio Tribunal;

Art. 108. Compete a los Tribunales Regionales Federales:

I. Procesar y juzgar, originariamente:

c) los mandatos de *segurança* y los hábeas data contra acto del propio Tribunal o de juez federal.

Art. 109. A los jueces federales compete procesar y juzgar:

VIII. Los mandatos de *segurança* y los hábeas data contra acto de autoridad federal, exceptuados los casos de competencia de los tribunales federales;

Art. 121. Una ley complementaria dispondrá sobre la organización y competencia de los tribunales, de los jueces de derecho y de las juntas electorales.

3) Son irrecurribles las decisiones del Tribunal Superior Electoral, salvo las que contrariaren esta Constitución y las denegatorias de hábeas corpus o mandado de *segurança*.

[11] Da Silva, José A., *Curso de direito constitucional positivo*, San Pablo, Malheiros, 1992, p. 397.

[12] Conforme lo indica el autor: "Este objetivo no es nuevo, o mejor dicho, no es totalmente una invención surgida de la nueva Carta Política. Tiene antecedentes históricos, inclusive legislativos.

La ley 824, del 28 de diciembre de 1984, del Estado de Río de Janeiro, fue sancionada para consagrarlo. Y con anterioridad, en 1981, el Congreso Pontes de Miranda, reunido por la orden de Abogados y el Instituto de Abogados de Río Grande do Sul, ofreció a la Nación una 'propuesta de Constitución Democrática para Brasil', cuyo art. 2°, sobre derechos y garantías individuales, tiene idéntico objetivo, y sirvió obviamente de base para aquella ley estadual.

La esquematización del derecho es la misma, y existirían para garantizarlo los recursos ya usados en el derecho procesal brasileño. En el caso de guarda de informaciones por parte de organismos públicos, sería de aplicación la acción de amparo, y en el caso de entidades privadas, el recurso sería la acción de exhibición del art. 844, I, del Cód. de Proc. Civil, de carácter preliminar, continuada posteriormente por la acción de rectificación o de daños y perjuicios, según sea el caso.

De Abreu Dallari en cuanto el hábeas data fue incorporado a la Const. brasileña de 1988 como consecuencia de la proyección de las disposiciones sobre protección de datos de carácter personal contenidas en la Const. de Portugal de 1976, las cuales fueron establecidas, en gran medida, con el fin de permitir el acceso a las informaciones que se encontraban en poder de la arbitraria y violenta policía política, creada por Oliveira Salazar.

De manera similar, en el Brasil, la policía y el Servicio Nacional de Informaciones se ocupaban de determinar quiénes eran los opositores al régimen de facto que culminó en 1985, y de perseguirlos. Por ello, con la misma finalidad que motivó la incorporación de la norma portuguesa, y en la inteligencia de facilitar el ingreso a tales archivos y permitir actuar sobre ellos, se consagró el hábeas data.

Sin embargo, los fines originariamente buscados con este nuevo instituto encontraron ciertos escollos a la hora de la aplicación efectiva, en particular por la creencia acerca de que el Estado debe tener secretos, lo cual es un vicio tradicional que viene del pasado colonial, mantenido incluso hasta mucho tiempo después de la independencia latinoamericana, por efecto del régimen de monarquía constitucional[13].

Luego de sancionada la norma constitucional, el art. 5°, inc. LXXII no fue sino reglamentado escuetamente diez años más tarde, en 1998, pero limitándose dicha regulación a los aspectos procesales del hábeas data, sin tratar conjunta ni separadamente las reglas relativas al tratamiento de los datos de carácter personal. Otras disposiciones relacionadas con el derecho a la protección de datos provienen de las disposiciones de la ley federal de defensa del consumidor, de 1990, que refiere concretamente a los bancos públicos de datos.

En 1991, Colombia reguló constitucionalmente aspectos concretos del tratamiento de datos de carácter personal, aunque no siguió el esquema brasileño y mantuvo el esquema anterior, estableciendo: “art. 15. Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas. En la recolección, tratamiento y circulación de los datos se respetarán la libertad y demás garantías consagradas en la Constitución”.

El derecho reconocido en el art. 15 fue defendido rápida y reiteradamente a través de la acción de tutela consagrada en el art. 86 de la Carta política, y debido al sistema mixto de control de constitucionalidad imperante en el país, la Corte Constitucional tuvo oportunidad de emitir una buena cantidad de fallos sumamente valiosos, donde desarrolló muy puntualmente los principios que deben respetarse en el tratamiento de datos de carácter personal, y denomina al derecho contenido en la

---

La garantía se incluyó en el Anteproyecto de Constitución elaborado en 1986 por la mencionada Comisión de juristas convocada por el Poder Ejecutivo, que no obtuvo aprobación oficial, quedando archivado. Fue en dicho Anteproyecto que apareció la denominación hábeas data” (Othon Sidou, José M., *As garantias ativas dos direitos coletivos*, 3ª ed., Río de Janeiro, Forense, 1989, p. 452).

[13] De Abreu Dallari, Dalmo, disertación pronunciada en el “Seminario Iberoamericano sobre acción de hábeas data”, organizado por la Facultad de Ciencias Jurídicas y Sociales de la Universidad de Talca, Chile, 9 a 11 de abril de 1997.

norma constitucional derechamente como “de hábeas data”, sin seguir el molde brasileño que concibe al hábeas data exclusivamente como acción.

Pese a los reiterados intentos de reglamentación legal de la figura –que sólo puede hacerse mediante una ley estatutaria, con las mayorías especiales constitucionalmente requeridas para ello–, hasta el momento no se ha dictado una ley que válidamente la reglamente, ya que fueron declarados inexequibles por la Corte Constitucional tanto el proyecto de ley por la cual se dictaban algunas disposiciones “sobre el ejercicio de la actividad de recolección, manejo, conservación y divulgación de información comercial” (n° 12/93 Senado y 127/93, Cámara, sentencia C-008/95), y la ley 510, de 1999, por la que se regulan aspectos relativos a los datos tratados por las entidades financieras (sentencias C-384, C-729 y C-841 de 2000)[14].

Un año después, la Const. paraguaya de 1992 incorporó la siguiente previsión: “art. 135. Toda persona puede acceder a la información y a los datos que sobre sí misma, o sobre sus bienes, obren en registros oficiales o privados de carácter público, así como conocer el uso que se haga de los mismos y de su finalidad. Podrá solicitar ante el magistrado competente la actualización, rectificación o la destrucción de aquéllos, si fuesen erróneos o afectaran ilegítimamente sus derechos”.

Entre las motivaciones de los constituyentes paraguayos se destaca la especial atención que pusieron en las preocupaciones de sus pares brasileños, y ello se vio reflejado cuando a poco de entrada en vigencia la norma se interpuso un hábeas data contra la policía nacional –por vía penal– para que ésta le exhibiera al peticionante las constancias que sobre su persona obraban en los registros de aquélla, con lo cual se logró ubicar una importante cantidad de documentos sobre la denominada “Operación Cóndor” –de intercambio de prisioneros entre las dictaduras sudamericanas–, donde obraba abundante información sobre desaparecidos y declaraciones de personas respecto de las cuales la policía siempre había negado que hubieran pasado por sus dependencias, formándose, a partir de ellos, los “archivos del horror”[15].

La regla constitucional fue reglamentada de manera parcial mediante la ley 1682, de 2001, referida a los bancos de datos de titularidad privada, y a través de una reciente reforma al Código Penal (arts. 141 a 148)[16].

---

[14] Conforme lo explica Remolina Angarita, al presente sólo existen algunos artículos de leyes y decretos vigentes que de manera directa o indirecta se refieren al tema, como el art. 95 de la ley 270 de 1996, Estatutaria de la Administración de Justicia, según la cual: “Los procesos que se tramiten con soporte informático garantizarán... la confidencialidad, privacidad y seguridad de los datos de carácter personal que contengan en los términos que establezca la ley”; el art. 32, inc. *c*, de la ley 527 de 1999, dispone que: “Las entidades de certificación deben: garantizar la protección, confidencialidad y debido uso de la información suministrada por el suscriptor”, y el art. 6°, del decr. 1524/02, que al referirse a los ISP y proveedores de servicios de alojamiento, establece: “Para todos los efectos la información recolectada o conocida en desarrollo de los controles aquí descritos, será utilizada únicamente para los fines de la ley 679 de 2001, y en ningún caso podrá ser suministrada a terceros o con detrimento de los derechos de que trata el art. 15 de la Constitución Política”.

[15] Benítez, Luis M., *La acción de hábeas data en el derecho paraguayo*, “Ius et praxis”, Facultad de Ciencias Jurídicas y Sociales de la Universidad de Talca, Chile, año 3, n° 1, “Derecho a la autodeterminación informativa y acción de hábeas data en Iberoamérica”, 1997, p. 116.

[16] Para un análisis pormenorizado ver Palazzi, Pablo A., *La transmisión internacional de datos personales y la protección de la privacidad*, Bs. As., Ad Hoc, 2002, p. 70 y siguientes.

En 1993, la Const. peruana será la primera en tratar de una manera más integral la problemática del acceso y control de la información –pública y personal– pues incorpora al hábeas data como una acción con múltiples objetivos, pero definiendo aparte el contenido del derecho a la protección de los datos.

Así, se dispuso en la Carta: "art. 200. Son garantías constitucionales:... *3*) La acción de hábeas data, que procede contra el hecho u omisión por parte de cualquier autoridad, funcionario o persona, que vulnera o amenaza los derechos a que se refiere el art. 2°, incs. 5°, 6° y 7°, de la Const." y "art. 2°. Toda persona tiene derecho... *5*) A solicitar sin expresión de causa la información que requiera y a recibirla de cualquier entidad pública, en el plazo legal, con el costo que suponga su pedido. Se exceptúan las informaciones que afectan la intimidad personal y las que expresamente se excluyan por ley o por razones de seguridad nacional... *6*) A que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal o familiar. *7*) Al honor y a la buena reputación, a la intimidad personal y familiar así como a la voz y a la imagen propias".

Esta previsión fue duramente criticada por su excesiva amplitud, tanto por la mayoría de la doctrina especializada como por los medios de prensa, que entendían coartada su libertad de expresión por la viabilización del derecho de réplica previsto en el art. 2°, inc. 7°. Las presiones fueron tales que –como lo apunta Vega Mere– el propio autor de la norma fue quien propició la reforma de la Constitución en este aspecto[17], y ello trajo como consecuencia –como lo indica Eguiguren Praeli–, la cesión del gobierno y la primer reforma constitucional –operada por la ley 26.470 y promovida por el propio oficialismo parlamentario–, en mérito de la cual se suprimió al hábeas data como medio de viabilización de la rectificación de informaciones, pero manteniendo la figura respecto de los derechos mencionados en los incs. 5° y 6° del art. 2° de la Carta Política[18].

Quedó así estructurado el hábeas data como medio para operar sobre los datos de carácter personal ("hábeas data propio") y como vía para acceder a la información pública ("hábeas data impropio"), resultando en la práctica los más trascendentes los articulados para el acceso a información pública, ya que han contribuido concretamente a la tutela de derechos de dificultosa efectivización, como el derecho al ambiente[19].

Sin perjuicio de algunas reglas de carácter administrativo, como la res. ministerial 662/96 sobre requerimiento de informaciones y secreto de las telecomunicaciones, las reglas constitucionales sólo fueron reglamentadas en su faz procesal por la

[17] Vega Mere, Yuri, *Derecho privado*, Lima, Grijley, 1996, p. 190 y 192.

[18] Eguiguren Praeli, Francisco J., *El hábeas data y su desarrollo en el Perú*, ponencia presentada en el "Seminario Iberoamericano sobre acción de hábeas data", organizado por la Facultad de Ciencias Jurídicas y Sociales de la Universidad de Talca, Chile, 9 a 11 de abril de 1997.

[19] Los dos primeros casos de hábeas data impropio fueron interpuestos: el primero, por la Sociedad Peruana de Derecho Ambiental contra el Ministerio de Energía y Minas para que suministre información sobre elementos tóxicos utilizados por una empresa privada, ante la negativa de aquél a entregarle información sobre la cancha de relaves de la empresa minera aurífera Retama (MARSA); y el segundo, por la Asociación Civil "Labor", de Ilo, contra el director general de minería, solicitando se le proporcione copia de los estudios de impacto ambiental presentados por la empresa minera Southern Perú Cooper Corporation para la instalación de una planta de ácido sulfúrico en la fundición de cobre en Ilo, así como de la resolución que había aprobado la instalación de depósitos de aquél ácido en el casco urbano del referido puerto.

ley 26.301, de 1994, y por la ley 27.489, referida a las actividades de las centrales privadas de información de riesgos crediticios y de protección al titular de la información.

En 1994 se reforma la Constitución federal argentina y el hábeas data es incluido –aunque sin ser rotulado así– como acción y como subtipo de amparo en el párr. 3° del art. 43, luego de regular, en los dos primeros párrafos a las acciones de amparo individual y colectivo.

La disposición reza: "art. 43 ...Toda persona podrá interponer esta acción para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o los privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir la supresión, rectificación, confidencialidad o actualización de aquéllos. No podrá afectarse el secreto de las fuentes de información periodística".

La norma ha tenido un amplio desarrollo jurisprudencial, con fallos –en especial los resueltos por la Corte Suprema de Justicia de la Nación– que le han otorgado una especial amplitud al instituto y lo han llevado a exceder considerablemente los contornos establecidos en el art. 43 constitucional. Incluso, ha sido objeto de permanente debate en el Congreso nacional desde la incorporación constitucional del instituto, hasta que en el 2000 finalmente se dictó una ley de protección de datos de carácter personal (25.326), que incluye entre sus disposiciones un sector en el que se reglamenta la acción de hábeas data para las causas que se ventilen ante la justicia federal.

Posteriormente, en el 2001 la ley fue reglamentada por decr. 1558/01, y en el 2002 fue creado e integrado dentro del ámbito del Ministerio de Justicia y Derechos Humanos, el órgano de control dispuesto por la ley (la Dirección Nacional de Protección de Datos Personales), que ha dictado diversas disposiciones administrativas de aplicación obligatoria en toda la República. Por tratarse de un país federal, además de las regulaciones nacionales, los Estados federados han regulado expresamente, en sus constituciones (y en algunos pocos casos también fueron dictadas leyes), aspectos del hábeas data[20].

En 1996, Ecuador reforma su Constitución e incluye la siguiente previsión: art. 30. Del hábeas data. "Toda persona tiene derecho a acceder a los documentos, bancos de datos e informes que sobre sí misma o sobre sus bienes consten en entidades públicas o privadas, así como conocer el uso que se haga de ellos y su finalidad.

Igualmente, podrá solicitar ante el funcionario o juez competente la actualización, rectificación, eliminación o anulación de aquellos si fueren erróneos o afectaren ilegítimamente sus derechos.

[20] Art. 16, Const. de la Ciudad Autónoma de Buenos Aires; art. 20, Const. de la Provincia de Buenos Aires; art. 50, Const. de la Provincia de Córdoba; art. 19, Const. de la Provincia de Chaco; art. 56, Const. de la Provincia de Chubut; art. 23, Const. de la Provincia de Jujuy; art. 30, Const. de la Provincia de La Rioja; art. 20, Const. de la Provincia de Río Negro; art. 22, Const. de la Provincia de Salta; art. 26, Const. de la Provincia de San Juan; art. 21, Const. de la Provincia de San Luis; art. 45, Const. de la Provincia de Tierra del Fuego.

Se exceptúan los documentos reservados por razones de seguridad nacional". La norma se reglamentó por la ley del control constitucional, donde entre los arts. 34 y 45 crea un capítulo específico titulado "Del hábeas data".

Un año después, en 1997, se reglamentará la faz procesal de la garantía constitucionalmente consagrada a través de la ley de control constitucional (arts. 34 y 35).

En 1998, se sucederá una nueva reforma constitucional y se regulará al hábeas data de la siguiente manera: "art. 94. Toda persona tendrá derecho a acceder a los documentos, bancos de datos e informes que sobre sí misma, o sobre sus bienes, consten en entidades públicas o privadas, así como a conocer el uso que se haga de ellos y su propósito. Podrá solicitar ante el funcionario respectivo, la actualización de los datos o su rectificación, eliminación o anulación, si fueren erróneos o afectaren ilegítimamente sus derechos. Si la falta de atención causare perjuicio, el afectado podrá demandar indemnización. La ley establecerá un procedimiento especial para acceder a los datos personales que consten en los archivos relacionados con la defensa nacional".

En 1999, Venezuela reformó integralmente su Constitución, insertando las siguientes previsiones: "art. 27. Toda persona tiene derecho a ser amparada por los tribunales en el goce y ejercicio de los derechos y garantías constitucionales, aún de aquellos inherentes a la persona que no figuren expresamente en esta Constitución o en los instrumentos internacionales sobre derechos humanos.

El procedimiento de la acción de amparo constitucional será oral, público, breve, gratuito y no sujeto a formalidad, y el juez competente tendrá potestad para restablecer inmediatamente la situación jurídica infringida o la situación que más se asemeje a ella. Todo tiempo será hábil y el tribunal lo tramitará con preferencia a cualquier otro asunto.

La acción de amparo a la libertad o seguridad podrá ser interpuesta por cualquier persona, y el detenido o detenida será puesto bajo la custodia del tribunal de manera inmediata, sin dilación alguna.

El ejercicio de este derecho no puede ser afectado, en modo alguno, por la declaración del estado de excepción o de la restricción de garantías constitucionales".

Art. 28. "Toda persona tiene derecho de acceder a la información y a los datos que sobre sí misma o sobre sus bienes consten en registros oficiales o privados, con las excepciones que establezca la ley, así como de conocer el uso que se haga de los mismos y su finalidad, y a solicitar ante el tribunal competente la actualización, la rectificación o la destrucción de aquéllos, si fuesen erróneos o afectasen ilegítimamente sus derechos. Igualmente, podrá acceder a documentos de cualquier naturaleza que contengan información cuyo conocimiento sea de interés para comunidades o grupos de personas. Queda a salvo el secreto de las fuentes de información periodística y de otras profesiones que determine la ley".

El art. 281 establece que son atribuciones del defensor del pueblo: *3*) "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".

La norma contiene cuanto menos, tres aciertos: el primero, el de incluir la versión de hábeas data impropio, que había sido incorporado por primera vez en la Constitución peruana; el segundo, el de extender la garantía de confidencialidad de la fuente de la información a otras profesiones distintas del periodismo, y el tercero, que constituye una novedad distintiva, el reconocimiento de la facultad del defensor del pueblo de interponer la acción de hábeas data, lo que en definitiva puede considerarse la partida de nacimiento normativa del hábeas data colectivo[21].

b) Países que cuentan con normas subconstitucionales relativas al derecho a la protección de datos o al hábeas data

Además de las reglas subconstitucionales incorporadas por los Estados que han regulado constitucionalmente la figura a las que ya hemos hecho referencia, unos pocos países han dictado leyes relativas a la protección de datos de carácter personal.

Así, Chile ha dictado en 1999 la ley 19.628 sobre protección de la vida privada, y México reformó en el año 2000 su ley federal de protección al consumidor, incorporando como capítulo VIII *bis* reglas concretas con relación a las transacciones efectuadas a través de medios electrónicos, ópticos o de cualquier otra tecnología[22].

3. 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 Sagüés[23].

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, 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–).

---

[21] Esto lo hemos venido pregonando desde hace varios años, ya que tal accionar permitiría evitar la consumación de perjuicios generalizados, como puede ocurrir, v.gr., por la incorporación masiva de datos sensibles, donde un escaso porcentaje de los afectados estaría en condiciones (por varios motivos, incluidos los económicos) de accionar individualmente para lograr su supresión, y la intervención del defensor del pueblo sería crucial para evitar tales violaciones generalizadas.

[22] Una explicación detallada de estas reglas puede consultarse en Palazzi, *La transmisión internacional de datos personales y la protección de la privacidad*, p. 68, 70, 171 y 195.

[23] Sagüés, Néstor P., *Subtipos de hábeas data*, *JA*, 1995-IV-352.

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)[24].

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

[24] 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).

Luego fue reconocido normativamente de manera expresa en la Const. 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.

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 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 al hábeas data propio e impropio, revistan el carácter de ortodoxos o heterodoxos, preventivos o reparadores, individuales o colectivos.

a) Hábeas data propio

1) *Hábeas data informativo*. 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 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) autoral, cuyo propósito es inquirir acerca de quién proporcionó los datos con que cuenta la base o banco de datos.

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 prevé expresamente la Const. de Portugal, y en el plano de nuestras autonomías locales, se encuentra regulado por las Constituciones de Buenos Aires, Ciudad Autónoma de Buenos Aires, 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 (19.628), arts. 9° y 12.

2) *Hábeas data aditivo*. 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 al 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 colectar 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), y

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)[25].

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 (19.628), arts. 6° y 9°.

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.

[25] 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 D., *El hábeas data: instrumento protector de la privacidad*, en “Revista de Derecho Privado y Comunitario”, n° 7, “Derecho privado en la reforma constitucional”, Santa Fe, Rubinzal Culzoni, 1994, p. 209).

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 (19.628), art. 6°.

4) *Hábeas data exclutorio o cancelatorio*. Este subtipo esta 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" [26] (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), etcétera.

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 (19.628), art. 6°.

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 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 evacuara 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[27].

---

[26] 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 (§ 5). (Para un análisis más particularizado ver el trabajo de Ekmekdjian, Miguel Á. - Pizzolo (h.), Calogero, *Hábeas data. El derecho a la intimidad frente a la revolución informática*, Bs. As., Depalma, 1996, p. 43).

[27] Bergel entiende que la confidencialidad no es meta propia de esta garantía (Bergel, Salvador D., *El hábeas data: instrumento protector de la privacidad*, en "Revista de Derecho Privado y Comunitario", n° 7, "Derecho privado en la reforma constitucional", Santa Fe, Rubinzal Culzoni, 1994, p. 216). Esta posición sólo se entiende si se parte de una interpretación literalista del art. 43 de la Const., 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

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 (19.628), art. 7°.

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 (19.628), art. 3°.

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 perspectiva, donde el dato está de algún modo oculto, y sólo puede ser conocido por quienes cuenten con la clave para descifrarlos[28].

---

el propósito de discriminar, el paso más lógico parece el de pedir la supresión del dato (Palazzi, Pablo A., *El hábeas data en la Constitución nacional. La protección de la privacidad en la "era de la información"*, *JA*, 1995-IV-710).

[28] 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, Edgardo A., *Diccionario de derecho informático*, Panamá, 2002, p. 71).

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.

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 (19.628), en el art. 6°.

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 garantizarse 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 por 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 (19.628), lo trata en su art. 11.

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.

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[29], pero no recurrimos a tal rótulo a fin no confundirlo con la clasificación entre hábeas data 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 pretenciones 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 personal; el art. 31 de la ley argentina de protección de datos personales, y la ley chilena sobre protección de la vida privada, art. 11).

b) 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.

---

[29] 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 limitada).

El término *reparación* nos da la idea de que su objetivo esencial es el de llevar las cosas al estado anterior, dentro de lo posible, 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. Por 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 daños o averías; satisfacción tras ofensa o agravio, e indemnización (Ossorio, Manuel, *Diccionario de ciencias jurídicas, políticas y sociales*, Bs. As., Heliasta, 2001, p. 865).

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.

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) *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 agraviada 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".

Las duras críticas de la doctrina y de las entidades periodísticas provocaron la eliminación de la remisión a este derecho por la reforma constitucional realizada por la ley 26.470, por lo que ya no subsiste esta vía para el ejercicio de la réplica, que se vehiculiza ahora por la ruta del amparo.

4. 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 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 dere-

cho 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.