

EL *HABEAS DATA*: SU DESARROLLO CONSTITUCIONAL

Néstor Pedro SAGÜÉS

SUMARIO: I. *Introducción*. II. *Dimensión constitucional del habeas data: Derecho informático y poder informático*. III. *Conflicto de derechos*. IV. *Vías de armonización*. V. *Enunciado constitucional*. VI. *El habeas data como capítulo del derecho procesal constitucional de Brasil*. VII. *Constituciones de Colombia (1991) y Paraguay*. VIII. *El habeas data en la Constitución peruana de 1993*. IX. *Reforma constitucional en Argentina (1994)*. X. *Hacia un reencuadre constitucional del habeas data*.

I. INTRODUCCIÓN

El *habeas data* es un proceso constitucional con fines diversos. Literalmente, apunta a “traer los datos” (así como el *habeas corpus* procura “traer el cuerpo”), y su objetivo principal es contener ciertos excesos del llamado “poder informático”.

Como tal, el *habeas data* genera dos órdenes de interrogantes. El primero es típicamente de derecho constitucional: ¿cuáles son los derechos en juego (y en conflicto) en el *habeas data*? ¿qué categoría de derechos debe privilegiar el legislador y el juez en el *habeas data*? La segunda esfera de problemas es propia del derecho procesal constitucional: ¿qué trámite tiene que darse al *habeas data*? ¿quién debe tener legitimación activa y pasiva? ¿cuál será el órgano competente para conocer y decidir en él?¹

II. DIMENSIÓN CONSTITUCIONAL DEL *HABEAS DATA*. DERECHO INFORMÁTICO Y PODER INFORMÁTICO

Siempre ha existido, por supuesto, la operación de recolectar, clasificar y conservar información. Lo que ocurre es que en el siglo XX, y en particular después de la aparición de las computadoras, el asunto ha tomado una dimensión insospechada.

¹ Sobre derecho procesal constitucional, véase Sagüés, Néstor Pedro, *Derecho procesal constitucional. Recurso extraordinario*, 3ª. ed., Buenos Aires, Astrea, 1993, t. I, pp. 1 y ss.

La existencia, ahora, de impresionantes bases o bancos de datos parte del supuesto de tres operadores principales en tal sistema: el “productor” de datos (quien los recolecta y los traduce en lenguaje computarizado), el gestor (que conserva y organiza aquella información, y crea el *software* indispensable para que los datos sean consultables por los usuarios), y el distribuidor, que es quien transmite (cobrando o no por su tarea) tales datos, intermediando así entre el gestor y el usuario.²

El productor, el gestor y el distribuidor cuentan con derechos constitucionales que amparan su labor. Cualquier constitución dispone de un arsenal tradicional de derechos que de modo directo o mediato sirven para tutelar esas tareas: por ejemplo, los derechos de trabajar y ejercer el comercio, la inviolabilidad de la correspondencia y papeles privados, de propiedad (incluyendo los derechos a la propiedad intelectual y, en términos generales, los “derechos intelectuales”), intimidad, etcétera.

Existe, en síntesis, un “derecho informático”, de base constitucional, que da pie a las actividades reseñadas.

El problema que evidencia la última parte del siglo XX es que, con el auge de los sistemas computarizados, ese “derecho informático” genera un “poder informático” de dimensiones insospechadas. La capacidad de registro de las computadoras, la rapidez de consulta y de transferencia de datos y la cobertura de toda esa información genera para quien la posee o puede acceder a ella una fuerte dosis de poder (contar con información es, desde ya, contar con poder), que puede ser tanto de poder económico (“la información se compra y se vende, viaja de un lugar a otro sin que el interesado lo sepa”),³ como de poder político (ya que conocer minuciosamente la vida de los demás permite, en buena medida, regular, controlar y vigilar su comportamiento).

III. CONFLICTO DE DERECHOS

Precisamente, el “derecho informático” (y sobre todo, el “poder informático”) pueden entrar en colisión con los derechos constitucionales de las personas registradas.

Un primer nivel de conflicto ocurre con el derecho a la privacidad: ¿es legítimo que un banco de datos acumule información sobre, por ejemplo, la

² Stiglitz, Rosana M., “Impacto de la informática en la sociedad”, en Revista *La Ley*, Buenos Aires, 1987, E-859.

³ Cfr. Heredero, Manuel, “La informática jurídica y el uso de la información personal”, en *Introducción a la informática jurídica*, Madrid, Rievero-Santodomingo, 1986, citado por Stiglitz Rosana M., *op. cit.* en nota 2, p. 860.

conducta sexual de un individuo? ¿es bueno que archive detalles sobre qué hace —y qué no hace— en su domicilio? ¿que puntualice si se embriaga o consume drogas en su casa de veraneo?

Otro frente polémico aparece con el derecho a la libertad de cultos: ¿es conveniente que una base de datos explore la religión que practica una persona? Con relación al derecho a la igualdad pueden suscitarse los mismos interrogantes si el banco de datos acumula noticias sobre el color de un habitante, ya que ello puede generar posteriormente actitudes discriminatorias.

Al mismo tiempo, las anotaciones respecto a las inclinaciones políticas, filiación ideológica, compromisos sindicales, etcétera, pueden fomentar tratos discriminatorios o perjudicar el libre ejercicio de los derechos políticos y gremiales.

A su turno, es factible observar que el registro de ciertos datos puede ser perfectamente aceptable, pero no así su divulgación a terceros. Tal sería el caso, *verbi gratia*, de ciertos movimientos contables cuyo conocimiento es comprensible para un ente oficial de recaudación impositiva (para determinar, por ejemplo, si la empresa del caso ha tributado bien o mal), pero que su transmisión a una empresa rival importaría quebrar las reglas habituales de discreción y competencia mercantil, en perjuicio para la corporación “desnudada”.

IV. VÍAS DE ARMONIZACIÓN

La compatibilidad entre el “derecho informático” y los otros derechos eventualmente perjudicados por el primero (privacidad, honor, propia imagen, igualdad, libertad de cultos y política, etcétera), no es fácil,⁴ pero sí posible.

Una vía de solución estriba en definir una zona de “información sensible”, no registrable en los bancos de datos, o con área insusceptibles de registrar. La “información sensible” cubre puntos como religión, ideas políticas, comportamiento sexual, salud moral y física, vinculaciones sindicales, raza.⁵

Otro mecanismo de adaptación consiste en auspiciar un proceso judicial expeditivo (en concreto, el *habeas data*), con los siguientes objetivos:

4 Así, se ha dicho que “resulta de todo punto de vista necesario y urgente impedir las intromisiones perturbadoras y la inadecuada difusión de datos procesados conforme a los modernos adelantos tecnológicos que pudieren afectar la esfera familiar y personal”, máxime cuando “el mero hecho de la conjunción de informaciones nominativas puede llevar a desnudar la intimidad de cada una de las personas físicas haciendo ilusorias las garantías constitucionales”. Andorno, Luis O., “La informática y el derecho a la intimidad”, en *La Ley* 1985-A-1108, con cita de Faustina Zurich de Piatti, “La revolución informática y el derecho a la privacidad”, Rosario, 1984.

5 Cfr. Correa, Carlos M. y otros, *Derecho informático*, Buenos Aires, Depalma, 1987, pp. 248 y ss.
DR. © 1998
Instituto de Investigaciones Jurídicas - Universidad Nacional Autónoma de México

1. *Derecho al acceso.* Conforme a él, cuando un sujeto está registrado de algún modo en un banco o base de datos, tiene derecho a saber lo que consta en él mismo, acerca de su persona.

Este “derecho al acceso” presenta serios problemas cuando una ley (o la propia Constitución, como es el caso de la brasileña, en su artículo 5) declara reservada la información que concierne a la seguridad de la sociedad y del Estado. En tales supuestos, la coexistencia entre el derecho personal de cada uno a saber qué se dice de él en el banco de datos (en tutela de una gama de derechos constitucionales personalísimos, como honor, privacidad, dignidad, etcétera) y los derechos de la sociedad y del Estado a la autoconservación (cosa que legitimaría el secreto, en aras de la seguridad colectiva) es una empresa harto complicada, pero que de todos modos debe hacerse.

El riesgo que se corre, cuando se habilita una excepción al “derecho al acceso” con el argumento de la seguridad social o es tal, es que la administración pública recurra habitualmente a la excusa de tal seguridad para negarse a suministrar información.

A su vez, si no se permite tal reserva, existe el peligro de difundir (mediante el ejercicio del “derecho al acceso”) noticias que efectivamente pueden perjudicar la defensa nacional o la seguridad de todos.

Un dispositivo consiste en autorizar la excepción de la reserva estatal por razones de seguridad colectiva, pero sometida a la revisión judicial de razonabilidad de tal alegación. En tal esquema, el Poder Judicial evalúa si la excusa estatal tiene sustento que la justifique. Ello parece ser una solución equitativa.

2. *derecho a la actualización.* En esta variable, el *habeas data* permite que una persona logre que los datos relativos a ella, queden puestos al día (por ejemplo, si figuraba en el banco de datos como deudor, que se anote haber pagado su obligación; si aparece como procesado, que conste su sobreseimiento o absolución).

3. *Derecho a la rectificación.* Aquí el interesado procura que se corrija información inexacta. *Verbi gratia* si figura como abogado, siendo arquitecto; o que ha viajado a Cuba, cuando nunca lo ha hecho; o que es hijo de fulano de tal, cuando lo es de mengano, etcétera.

4. *Derecho a la confidencialidad.* En este campo, el sujeto en cuestión exige que una información que él ha proporcionado, y que ha sido legalmente requerida, permanezca secreta para los terceros. Es el caso, por ejemplo, del “secreto fiscal” o del “secreto bancario”. como el del “secreto médico”.

5. *Derecho a la exclusión.* Respecto a diversos datos conceptuados como “información sensible”, el fin del *habeas data* puede consistir en “cancelar” o “borrar” tales noticias de los bancos de datos. Como se anticipó, algunas

veces es posible registrar algún tipo de información, o algún modo de archivo; y no ciertos informes o maneras de guardarlos. Por ejemplo, la ley 23. 798 de Argentina, de “lucha contra el sida”, prohíbe “individualizar a las personas (que padecen tal mal) a través de fichas, registros o almacenamiento de datos, los cuales, a tales efectos, deberán llevarse en forma codificada” (artículo 2, inciso e).⁶

V. ENUNCIADO CONSTITUCIONAL

El derecho constitucional comparado exhibe distintas técnicas para lograr la coexistencia entre el “derecho informático” y los demás derechos constitucionales personales en conflicto.

a) una variante es que la Constitución presente el problema, dé algunas directrices fundamentales, y remita el grueso del tema a la legislación ordinaria. Así, el artículo 18, inciso 4 de la constitución española indica que “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”.

b) Otra variable es que la Constitución explicita con mayor detalle el asunto y formule reglas operativas concretas. Un buen antecedente de ello está en el artículo 35 de la Constitución de Portugal:

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 los datos, así como su actualización. No se podrá utilizar la informática para el tratamiento de datos, así como su actualización. No se podrá utilizar la informática para el tratamiento de datos referentes a convicciones políticas, fe religiosa o 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.

Una muestra de explicitación circunstanciada de cómo amalgamar los derechos que citamos, se encuentra también en el artículo 20 de la Constitución de Provincia de Río Negro (Argentina):

La ley asegura la intimidad de las personas. El uso de la información de toda índole o categoría, almacenada, procesada o distribuida a través de cualquier medio físico o electrónico, debe respetar el honor, la privacidad y el goce com-

⁶ Nos hemos referido a estas proyecciones del *habeas data* en Sagiés, Néstor Pedro, *Elementos de derecho constitucional*, Buenos Aires, Astrea, 1993, t. 2, p. 86.
DR. © 1998
Instituto de Investigaciones Jurídicas - Universidad Nacional Autónoma de México

pleto de los derechos. La ley reglamenta su utilización de acuerdo a los principios de justificación social, limitación de la recolección de datos, calidad, especificación del propósito, confidencialidad, salvaguardia de la seguridad, apertura de los registros, limitación en el tiempo y control público. Asegura el acceso de las personas afectadas a la información para su rectificación, actualización o cancelación cuando no fuera razonable su mantenimiento.⁷

c) *silencio constitucional*. A menudo, la constitución nada señala expresamente sobre el “poder informático” y su inestable coexistencia con los demás derechos constitucionales. Ellos se explica —en parte— por la novedad del problema.

¿Si hay silencio constitucional, cabe concluir que la persona citada en un banco de datos carece de los derechos al acceso, rectificación, actualización, confidencialidad o exclusión? Una primera reacción, de tipo negativo, podría concluir que si esos derechos no están mencionados en la Constitución, no son constitucionales, aunque una ley sí podría habilitarlos (hipótesis en las que tendrían base legal, pero constitucional). No obstante, es posible afirmar que si la constitución admite de modo explícito o implícito (*vergi gratia*, mediante la cláusula de los derechos enumerados, al estilo de la enmienda IX de los Estados Unidos de América, artículo 33 de la constitución argentina o artículo 3 de la constitución del Perú de 1993) ciertos derechos constitucionales (intimidad, honor, propia imagen, no discriminación, libertad de cultos, etcétera) de tales derecho se infieren otros, también constitucionales, que son consecuencia inevitable de los primeros. Por ejemplo, del derecho a la igualdad se deduce el de borrar de los bancos de datos informes sobre mi raza o creencia religiosa.⁸

Así, el citado derecho a la exclusión o a la cancelación sería un derecho constitucional inferido.

VI. EL *HABEAS DATA* COMO CAPÍTULO DEL DERECHO PROCESAL CONSTITUCIONAL DE BRASIL

La constitución brasileña de 1988 instrumentó un amparo específico, denominado “*habeas data*”, destinado a asegurar a las personas el conocimiento

⁷ Sobre otras constituciones que han normado puntos concernientes al *habeas data*, v. por ejemplo las provincias argentinas de Córdoba (artículo 50), Tierra del Fuego (artículo 45), Jujuy (artículo 23), San Juan (artículo 26), San Luis (artículo 24), etcétera.

⁸ El decreto reglamentario 1.244/91 de la ley argentina 23.798 de lucha contra el SIDA, especificó que en los registros o almacenamiento de datos sólo deberá consignarse, con relación a los afectados por aquella dolencia, “un sistema que combine las iniciales del nombre y del apellido, día y año de nacimiento”.

de informaciones referidas a ellas, que constasen en registros o bancos de datos de entidades gubernamentales o de carácter público, y para rectificar tales datos.⁹

El sujeto activo, en el caso brasileño, es cualquier nacional o extranjero residente en el país; pero se trata del ejercicio; de un derecho personalísimo, que no debe confundirse con el ejercicio; genérico del derecho a la información que posee, por ejemplo, un periodista. En el *habeas data*, es “mi” derecho a recabar “mis” datos.¹⁰

El sujeto pasivo es el Estado propietario del banco de datos, pero también todo sujeto titular de un registro susceptible de generar información. Esto es importante, por que algunas leyes reglamentarias del “*habeas data*”, lo han ceñido al caso de registros oficiales, cuando en rigor de verdad cualquier base de datos apta para ser utilizada por terceros, debe ser sujeto pasivo del proceso que comentamos. Por el contrario, un banco de datos de uso exclusivamente personal para su titular, estaría cubierto por el derecho a la privacidad de éste, como papel o correspondencia privada, y (al menos al principio) sería incuestionable mediante el *habeas data*.

Respecto al órgano competente para tramitar al *habeas data*, el derecho brasileño ha reservado jurisdicción al Supremo Tribunal Federal para juzgar originalmente los que cuestionen actos del presidente de la República y de otros dignatarios nacionales.¹¹ Se intenta de tal modo excluir a jueces de primera o de segunda instancia el conocimiento de decisión de cuestiones de posible gran importancia, donde por lo común surgirán temas próximos a la seguridad nacional.

El trámite de *habeas data* ofrece dos posibilidades principales: o se aceptan las reglas habituales de cualquier amparo (pauta seguida, por ejemplo, por la ley 4444 de la provincia de Jujuy, Argentina), aunque existan algunas pequeñas variaciones de procedimiento; o se programa un nuevo y distinto amparo, con plazos generalmente breves (así, la ley 2384 de la Provincia de Río Negro, Argentina, contempla una demanda, traslado por dos días de prueba y sentencia en cinco días).¹²

9 Sobre el *habeas data* en Brasil, *cf.* Othon Sidou, J.M., *habeas data, mandado de injucao, Habeas corpus, Mandado de seguranca, acao popular*, 3ª ed., Río de Janeiro, ed. Forense, 1989, pp. 446 y ss. En concreto, el artículo 5-LXXII de la Constitución: “Se concede *habeas data*: a) para asegurar el conocimiento de informaciones relativas a la persona del solicitante, contenidas en registros o bancos de datos de entidades gubernamentales o de carácter público; b) para la rectificación de datos, cuando no se prefriere hacerlo por procedimiento secreto de carácter judicial o administrativo”.

10 Da Silva José Alfredo, *Curso de direito constitucional positivo*, 8a. ed., San Pablo, Malheiros, 1992, p. 397.

11 Othon Sidou, J.M., *op. cit.* en nota 9, p. 450.

12 Véase Sagüés, Néstor Pedro, *Derecho procesal constitucional. Acción de amparo*, 3ª ed., Buenos Aires, Astrea, 1992, t. 3, pp. 654 y ss.

La elección de una u otra variante es a todas luces una cuestión accesoria. En principio, el amparo genérico debe ser un trámite ágil y comprimido, y de ahí que —como regla— no se justificaría para el *habeas data* otra reducción suplementaria. No obstante, los particularismos locales pueden exigir una instrumentación peculiar para este último.

La sentencia del *habeas data* detalla Othon Sidou, es constitutiva y condenatoria (cuando hace lugar al mismo), con vigor de cosa juzgada cuando adquiera firmeza, si es pasible de recursos.

VII. CONSTITUCIONES DE COLOMBIA (1991) Y PARAGUAY (1992)

El modelo brasileño se ha extendido a otras constituciones. Así, la de Colombia, después de afirmar en su artículo 15 que todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, con obligación del Estado de respetarlos y hacerlos respetar, agrega:

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 datos se respetarán la libertad y demás garantías consagradas en la Constitución.

La constitución del Paraguay de 1992 dedica al instituto un artículo especial, el 135, bajo el rótulo de “*habeas data*”. En concreto, puntualiza que

Toda persona podrá 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, la rectificación o la destrucción de aquéllos, si fuesen erróneos o afectaran ilegítimamente sus derechos.

En el caso paraguayo, interesa subrayar que la tutela del *habeas data* pasa a cubrir, además de derechos personalísimos (privacidad, no discriminación) y no patrimoniales (convicciones religiosas, ideas políticas, etcétera), áreas de tipo patrimonial, ya que se lo planea, también, para atacar información equivocada sobre los bienes de un individuo o corporación (la voz “persona” que encabeza el mentado artículo 135, puede en efecto cubrir a las personas ideales).

VIII. EL *HABEAS DATA* EN LA CONSTITUCIÓN PERUANA DE 1993.

El artículo 200 de la nueva constitución del Perú, menciona en su inciso tercero, como “garantía constitucional”, a “la acción de *habeas 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 artículo 2º, incisos 5, 6 y 7 de la Constitución”.

Estos últimos refieren a distintos rubros. Por un lado al derecho genérico a la información, a obtener “de cualquier entidad pública, en el plazo legal”, con excepción de las informaciones que afecten la intimidad personal y las excluidas por ley o por razones de seguridad nacional. Añade el inciso 5º que el secreto bancario y la reserva tributaria pueden levantarse a pedido de juez, del Fiscal de la Nación o de una comisión investigadora del Congreso, con arreglo a la ley. El inciso 6º del artículo 2 enuncia el derecho a “que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar”. Finalmente, el inciso 7 enuncia el derecho “al honor y a la buena reputación, a la intimidad personal y familiar así como a la voz y a la imagen propias”, así como el derecho de réplica, también llamado de rectificación o respuesta.

Una apreciación global del régimen del *habeas data* peruano conduce a afirmar que tienen un radio de acción decididamente amplio, probablemente excesivo. Para empezar, engloba al derecho de réplica, instituto que es debidamente distinto al *habeas data*. Este pecado conceptual, dicho sea en favor del constituyente peruano, no fue original: ya lo había cometido la ley 2384 de la provincia de argentina de Río Negro.

Por los demás, el *habeas data* tiene como meta natural tutelar a las personas por excesos del poder informático, y no, en términos generales, por cualquier lesión que se infieran, por cualquier medio, a su honor, privacidad o propia imagen, o a la intimidad familiar y la voz.

Para decirlo más claro, y como su nombre lo indica, el *habeas data* es un amparo especial referente a datos (y a “datos” registrados en bancos o bases de datos).

A raíz de la amplitud de sus términos, el *habeas data* peruano ha hecho preguntarse a muchos, si no podía emplearse para imponer, sobretexto de tutelar el honor y la privacidad, la censura previa a periódicos, radioemisoras o canales de televisión. Una errónea interpretación del inciso 5º del artículo 2 de la constitución, cuando se menciona a los “servicios informáticos” como sujetos pasibles, mediante el *habeas data*, de no suministrar información, ha permitido auspiciar aquella hipótesis de la censura previa.

Sin embargo, hay que distinguir entre “servicio informático” o “servicio informativo”. La constitución, cuando menciona a los primeros, habla claramente de los servicios informáticos “computarizados o no”. Es decir, a bancos o bases de datos. No alude a medios de comunicación.

Paralelamente, el inciso 4 del artículo 2 de la nueva constitución excluye enfáticamente cualquier clase de censura o previa autorización para ejercer las libertades de información, opinión, expresión y difusión del pensamiento, con lo que, según una interpretación orgánica y sistémica de la Constitución, cualquier programación del *habeas data*, en tutela de los derechos de los incisos 5, 6 y 7 del mencionado artículo 2, debe compatibilizarse con la directriz de “no censura” del inciso 4 del mismo artículo.

De todos modos, el caso peruano evidencia la necesidad de reducir al *habeas data* a sus objetivos propios: acceder, actualizar, rectificar, excitar (en su caso) información, y reservarla algunas veces en virtud del principio de confidencialidad; y no aumentarlo con otros propósitos o en protección de otros derechos, para lo cual está la acción de amparo general.¹³

IX. REFORMA CONSTITUCIONAL EN ARGENTINA (1994)

El 16 de agosto de 1994 la convención constituyente nacional, reunida en la ciudad de Santa Fe, aprobó un nuevo artículo constitucional que contempla específicamente al *habeas data*, aunque sin darle de modo explícito esa denominación.¹⁴

Los detalles de esta figura son los siguientes:

a) amparo particular: la constitución programa al *habeas data* como una variable de la acción de amparo, tesis por cierto correcta.

b) legitimación. En cuanto la legitimación activa, el nuevo texto habilita para ello a “toda persona” con lo que, entendemos, cabe aceptar que puede plantearlo (como en el caso paraguayo) tanto un individuo como una persona

13 Sobre el *habeas data* en Perú, *cfr.* Núñez Ponce, Julio, “El *habeas data* y la protección jurídica de la información computarizada”, en *Jus et praxis*, Lima, Universidad de Lima, 1993, núm. 21/2, pp. 193 y ss.; Abud Yupanqui, Samuel, “*Habeas data* y conflicto entre órganos constitucionales. Dos nuevos procesos constitucionales”, en Comisión Andina de Juristas, *La Constitución de 1993. Análisis y comentarios*, Lima, 1994, serie “Lecturas sobre temas constitucionales 10”, pp. 265 y ss., quien critica los desbordes del instituto en la nueva constitución, y su innecesariedad, atento las normas en materia de amparo.

14 Véase Puccinelli, Óscar, “*Habeas data*”, trabajo presentado ante la convención constituyente, en prensa. El autor siguió la tesis de Pérez Luño, sostenida también por el Tribunal Constitucional alemán, del “derecho a la autodeterminación informativa”, a fin de acceder a la información, rectificarla, excluirla, etcétera. Véase Pérez Luño, Antonio Enrique, “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 constitucionales, 1989, pp. 140 y ss.

de existencia ideal. Pero no es una acción popular sólo puede articularla el afectado (el artículo constitucional prevé el *habeas data* “para tomar conocimiento de los datos “a ella referidos”, vale decir, concernientes al peticionante concreto).

Respecto a la legitimación pasiva, el *habeas data* queda programado con relación a “registros o bancos de datos públicos, o los privados destinados a proveer informes”. Por ende, podrá plantearse contra autoridades públicas o particulares que dirijan bases o registros que suministren informes.

En el debate habido en la asamblea, el convencional Iván J. M. Cunetl mencionó por agregar, después de las palabras “proveer informes”, la expresión “de uso público”. El fin de ese añadido, dijo, era “evitar que a través de este recurso pudiera peligrosamente existir algún riesgo para el secreto profesional de abogados, contadores, etcétera.” Su idea, sin embargo, no fue aceptada.

Respecto a particulares, en síntesis, el flamante texto es por un lado amplio, porque basta que la base de datos esté destinada a proveer informes, para que pueda prosperar el *habeas data*; pero por otro es de alguna medida restrictivo, ya que no es suficiente con que el registro privado sea susceptible de generar información: debe hallarse pensado para proveer informes. Desde luego, la ley reglamentaria podría ampliar la órbita de actuación de este proceso constitucional.

c) derechos tutelados. Quizá por apresuramiento, el nuevo texto contempla el *habeas data* para supuestos de “falsedad o discriminación”, y no para otras hipótesis clásicas de esta figura, como la protección de la privacidad o el honor.

Este problema puede resolverse teniendo en cuenta que el amparo de la intimidad o el honor se vincula a menudo con falsedad o discriminación; y que así no fuera, una norma reglamentaria del *habeas data* estaría habilitada para proyectarlo para aquellos derechos. De todos modos, es posible concluir que si la privacidad y el honor son derechos de raigambre constitucional, deben lo mismo protegerse por el vehículo que sea necesario a tales fines, y que por ello el *habeas data* no podría negarse en la especie.

Volviendo al texto constitucional, el promotor del *habeas data* tendrá que alegar, para plantearlo con buen suceso, que los registros del caso incluyen información que es inexacta, o que puede provocar discriminación. ¿Es necesario que la falsedad o eventual discriminación le cause perjuicio? En rigor de verdad, el eventual daño es obvio en los supuestos de discriminación, o al menos está siempre latente. En cuanto los datos falsos, si se admite que el valor verdad integra el mundo jurídico,¹⁵ cabe reconocer al interesado aptitud

para promover al *habeas data*, en resguardo de la simple verdad, aunque la inexactitud de un registro no le ocasione un agravio diferente o especial.

d) objetivos. El *habeas data* argentino tiene las siguientes metas: acceder a la información; suprimirla; rectificarla; actualizarla, y también (esto por moción del referido convencional Cunen), asegurar el principio de confidencialidad. Cubre, entonces, los cinco objetivos fundamentales del instituto, que ya hemos descripto.

Un interrogante significativo que plantea este *habeas data* es si la autoridad pública podría alegar razones de seguridad del Estado, o similares, para negarse a suministrar información.

En principio, y como el texto constitucional no incluye la aludida excepción para la operatividad de este proceso, la respuesta será negativa. Sin embargo, cabe tener presente que como variante que es de la acción de amparo, el *habeas data* está sometido a las previsiones constitucionales de aquélla, entre las que se cita, según el nuevo texto constitucional, la necesidad de que el acto lesivo padezca de una “arbitrariedad o ilegalidad manifiesta”. Por ello, si existe la negativa estatal que apuntamos, tendrá el juez del hábeas data que evaluar su grado de razonabilidad o de irrazonabilidad —en el caso concreto—, y decidir en su consecuencia. De cualquier manera, sería provechoso que la ley reglamentaria futura atienda esta cuestión.

e) el *habeas data* y los medios de difusión. Alertada por el debate generado sobre la posible incompatibilidad entre este proceso y la libertad de expresión, y ante el riesgo de utilizársele para borrar datos de los archivos de prensa, y aún de empleársele como censura previa, la parte final del nuevo párrafo constitucional argentino advierte que con el *habeas data* “No podrá afectarse el secreto de las fuentes de información periodística”.

La regla es prudente, y pone punto final a la discusión aludida. La armonización entre la libertad de expresión y los demás derechos y garantías constitucionales no es siempre fácil, y la convención constituyente optó por privilegiar en este tema a la primera, seguramente por el carácter sistémico que tiene (es decir, como elemento indispensable para el flujo de ideas en el régimen democrático).

X. HACIA UN REENCUADRE CONSTITUCIONAL DEL *HABEAS DATA*

La experiencia habida hasta el momento muestra un incremento progresivo de la “constitucionalización” del *habeas data*, en el sentido que tal proceso está apareciendo cada vez más en las cartas constitucionales. Al mismo tiempo,

emergen ya ciertos problemas en torno a esa constitucionalización, que conviene atender con premura.

a) uno de ellos, tal vez el principal, es la desnaturalización del instituto, vale decir, su uso para fines anómalos, como por ejemplo viabilizar el derecho de réplica respecto a los medios de difusión por medio del *habeas data*. Otra, la de destinarlo para tutelar en términos genéricos el honor, el derecho a la propia imagen o la voz, como ha ocurrido en la última constitución peruana.

Debe tenerse presente, en este punto, que el *habeas data* es un mecanismo de defensa contra los excesos del “poder informático” (no confundir con el poder informativo), y para tutelar derechos constitucionales de tipo personalísimo precisamente en el ámbito de la informática, y no en otras áreas. Para la protección general de los derechos personales, está la acción de amparo común.

b) otra cuestión importante gira sobre el perfil constitucional del *habeas data*. La constitución puede limitarse a una mención escueta de esta figura, cosa en principio acertada, en cuyo caso confía su desenvolvimiento a la judicatura y al Poder Legislativo; o en cambio, entrar a describirla con mayor o menor detalle. El problema es que si el constituyente prefiere la “ruta de la descripción”, puede pecar por exceso (si prescribe reglas detallistas que después resultan poco felices, o que exigen enmiendas difíciles de concretar con relación a un documento constitucional), o por omisión (*verbi gratia*, si enuncia dos o tres finalidades del *habeas data*, y deja en el tintero las restantes).

Aunque algunos, y tal vez muchos, de esos defectos reglamentaristas del constituyente pueden encontrar remedio en la legislación infraconstitucional complementaria que dicte el legislador, y sobre todo, en una jurisprudencia inteligente que pula y adapte razonablemente el texto constitucional, lo cierto es que conviene prevenirlos; y en la duda, es mejor que el constituyente guarde silencio a que hable incorrectamente.

c) otro asunto digno de destacarse es que al establecer el *habeas data*, el constituyente debe tener en claro que está definiendo un conflicto de derechos: derechos de quien recluta y distribuye datos, por un lado, y derechos del registrado, por el otro. Nada es aquí gratuito; todo tiene un costo jurídicopolítico, porque lo que se concede a uno se quita al otro, y viceversa. Bueno es entonces evaluar con cautela el activo y el pasivo de cada opción constitucional, e incluso meditar los efectos y las reacciones que puede despertar en un medio social concreto tal elección.

En ese orden de ideas, el riesgo más frecuente en que puede incurrirse es afectar la operatividad de los medios de comunicación social (para subsanar lo cual hubo que colocar una advertencia específica, en la última reforma

constitucional argentina), o la privacidad de los archivos y bases de datos privados no destinados a generar información. Otro punto urticante es el problema de la seguridad del Estado, y el secreto consecuente en esas zonas. Aquí el dilema es harto complejo y difícil de solucionar. En última instancia habrá que respetar tal reserva, pero sometiendo el juicio de razonabilidad sobre su extensión y la presencia misma de estar implicada en ella la seguridad de la comunidad, al veredicto del Poder Judicial. De lo contrario, sería muy fácil al Estado eludir al *habeas data*, so pretexto de que la información requerida debe silenciarse por los aludidos motivos de seguridad.