Protección de Datos Personales en
América Latina — Juan Pérez ante una disyuntiva de progreso y bienestar

Carlos G. Gregorio
Instituto de Investigación para la Justicia*

Introducción

En los últimos años los crecientes niveles de informatización de los servicios estatales y privados han llevado a la generación de bases de datos que incluyen información personal —y en algunos casos datos sensibles. Simultáneamente varias empresas privadas en América Latina y el Caribe comenzaron a comercializar datos personales, en casi todos los casos operando dentro de un vacío legal. Sólo en algunos países las reformas constitucionales o los procesos legislativos tuvieron en consideración la problemática desde alguno de los siguientes perfiles: habeas data, protección de datos personales, acceso a la información gubernamental, regulación de las empresas que comercializan datos personales y seguridad de las bases de datos. Un hecho significativo es que ningún país de la región dispone de leyes que regulen todos estos aspectos en forma coordinada.[1] Si bien no existe imposibilidad jurídica de una regulación única o coordinada, este hecho da la sensación que en la región ha sido imposible conciliar intereses que naturalmente pujan en sentido.

El propósito de esta nota es analizar no sólo el marco normativo actual, sino las causas y consecuencias de proteger los datos personales en América Latina y el Caribe, y cual ha sido el juego de intereses o prioridades que demoran o precipitan esta tipo de legislación.

1. La legislación sobre protección de los datos personales en América Latina

Las recientes reformas constitucionales en América Latina introdujeron la protección de los datos personales (algunas bajo la forma de *Habeas Data*), *viz.* Brasil (1988) artículo 5° — X, XII y LXXII; artículo 105 I b); Colombia (1991) artículo 15; Paraguay (1992) artículos. 33, 36 y 135; Perú (1993) artículos. 2°, 162, 203-3; Argentina (1994) artículos. 19 y 43; y, Ecuador (1998) artículos. 23.8; 23.13; 23.24; 94.

Dos textos constitucionales recientes han percibido —de alguna forma— la existencia de riesgos en el proceso de informatización. Son el caso de la Constitución Política del Perú: Artículo 2. '*Derechos fundamentales de la persona: ... (6). A que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar*'; y el de la Constitución de la República Bolivariana de Venezuela: Artículo 60. '*Toda persona tiene derecho a la protección de su honor, vida privada, intimidad, propia imagen, confidencialidad y reputación. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y ciudadanas y el pleno ejercicio de sus derechos*'.[2]

---

* www.iijusticia.edu.ar

1 El país que más se aproxima a cubrir todos estos aspectos es Panamá.

2. *Cf.* Constitución española de 1978, artículo 18 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."

A partir de este marco constitucional algunos países han ido legislando sucesivamente mecanismos de protección de los datos personales:

La Ley Argentina de Protección de Datos Personales,[3] es probablemente la más cercana al modelo europeo. Argentina es el primer país de América Latina que recibe una certificación de la Unión Europea como "un nivel adecuado de protección" (Decisión 2003/490/CE del 30 de junio de 2003),[4] que también ha sido conferida a Suiza, Hungría y a la Bailía de Guernsey, e indirectamente a Estados Unidos y Canadá por medio de la calificación de "*safe harbor*". En este mismo sentido es el único país de América Latina que cuenta con una agencia de protección de datos con alguna similitud a las europeas. Sin embargo varios artículos de la ley han sido vetados por el Poder Ejecutivo, entre ellos el artículo 47 sobre los historiales crediticios fundamentando que *"el Proyecto de Ley dispone que los bancos de datos prestadores de servicios de información crediticia deberán suprimir, o en su caso, omitir asentar, todo dato referido al incumplimiento o mora en el pago de una obligación, si ésta hubiere sido cancelada al momento de la entrada en vigencia de la presente ley. Que esta decisión generaría la pérdida de la información histórica respecto al cumplimiento crediticio de muchos deudores del sistema, lo que podría producir un encarecimiento de las operaciones de crédito bancario originado por el mayor riesgo provocado por la incertidumbre"*.[5]

Según el mapa mundial de leyes de protección de datos personales realizado por David Banisar,[6] Chile y Paraguay (además de Argentina) son los otros dos países de América Latina y el Caribe que cuentan con una legislación adecuada.[7]

La ley chilena sobre Protección de la Vida Privada (Ley 19.628 del 30 de agosto de 1999) contiene un capítulo sobre el uso de la información financiera, comercial y bancaria que en el año 2002 fue parcialmente modificado por la Ley 19.812; por esta norma *"Se exceptúa la información relacionada con los créditos concedidos por el Instituto Nacional de Desarrollo Agropecuario a sus usuarios"* al artículo 17, y además se establece que *"No podrá comunicarse la información relacionada con las deudas contraídas con empresas públicas o privadas que proporcionen servicios de electricidad, agua, teléfono y gas"*. Se modifica el artículo 18 en el sentido que *"En ningún caso pueden comunicarse los datos a que se refiere el artículo anterior, que se relacionen con una persona identificada o identificable, luego de transcurridos cinco años desde que la respectiva obligación se hizo exigible. Tampoco se podrá continuar comunicando los datos relativos a dicha obligación después de haber sido pagada o haberse extinguido por otro modo legal"*.

Por la misma ley se modifica el artículo 2º del Código del Trabajo, estableciendo que *"Ningún empleador podrá condicionar la contratación de trabajadores a la ausencia de obligaciones de carácter económico, financiero, bancario o comercial que, conforme a la ley, puedan ser comunicadas por los responsables de registros o bancos de datos*

---

3 Ley 25.326 del 2 de noviembre de 2000.

4 http://europa.eu.int/eur-lex/pri/es/oj/dat/2003/l_168/l_16820030705es00190022.pdf Artículo 1. "A efectos del apartado 2 del artículo 25 de la Directiva 95/46/CE, se considera que Argentina garantiza un nivel adecuado de protección por lo que respecta a los datos personales transferidos desde la Comunidad".

5 Decreto 995/2000, http://infoleg.mecon.gov.ar/infolegInternet/anexos/60000-64999/64791/norma.htm

6 http://www.privacyinternational.org/survey/dpmap.jpg

7 Ver Marc Rotenberg & Cedric Laurant, *Privacy and Human Rights 2004, an international survey on privacy laws and developments,* www.privacyinternational.org/survey/phr2004

personales; ni exigir para dicho fin declaración ni certificado alguno. Exceptúanse solamente los trabajadores que tengan poder para representar al empleador, tales como gerentes, subgerentes, agentes o apoderados, siempre que, en todos estos casos, estén dotados, a lo menos, de facultades generales de administración; y los trabajadores que tengan a su cargo la recaudación, administración o custodia de fondos o valores de cualquier naturaleza".

En Paraguay la Ley 1.682 del 16 de enero de 2001,[8] delimita los datos sensibles, la acción de *habeas data*, y establece (artículo 5) que los datos financieros podrán ser publicados solamente cuando las personas concernidas *"hubiesen otorgado autorización expresa y por escrito"*. Sobre otro tipo de datos, podrán ser publicados y difundidos (artículo 6) cuando *"los datos que consistan únicamente en nombre y apellido, documento de identidad, domicilio, edad, fecha y lugar de nacimiento, estado civil, ocupación o profesión, lugar de trabajo y teléfono ocupacional"* y *"cuando la información sea recabada en el ejercicio de sus funciones, por magistrados judiciales, fiscales, comisiones parlamentarias o por otras autoridades legalmente facultadas para ese efecto"*.

En Panamá existen dos normas: la Ley 6 de 22 de enero de 2002 que dicta normas para la trasparencia de la gestión publica, establece la acción de *habeas data* y otras disposiciones y la Ley 24 de 22 de mayo de 2002 que regula el servicio de información sobre el historial de crédito de los consumidores o clientes. Se ha incluido en la Ley 6 la acción de *habeas data* y una definición de *"Información confidencial. Todo tipo de información en manos de agentes del Estado o de cualquier institución pública que tenga relevancia con respecto a los datos médicos y psicológicos de las personas, la vida íntima de los particulares, incluyendo sus asuntos familiares, actividades maritales u orientación sexual, su historial penal y policivo, su correspondencia y conversaciones telefónicas o aquellas mantenidas por cualquier otro medio audiovisual o electrónico, así como la información pertinente a los menores de edad. Para efectos de esta Ley, también se considera como confidencial la información contenida en los registros individuales o expedientes de personal o de recursos humanos de los funcionarios"*. La ley prevé (artículo 13) *"La información definida por la presente Ley como confidencial no podrá ser divulgada, bajo ninguna circunstancia, por agentes del Estado. En el caso de que la información de carácter confidencial sea parte de procesos judiciales, las autoridades competentes tomarán las provisiones debidas para que dicha información se mantenga reservada y tengan acceso a ella únicamente las partes involucradas en el proceso judicial respectivo"*.

En Brasil la lei 9.507 del 12 de noviembre de 1997 *regula o direito de acesso a informações e disciplina o rito processual do* habeas data, aquí también varios artículos de esta ley han sido vetados por el Poder Ejecutivo.

En Colombia por el artículo 15 de la Constitución Política *"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 datos se respetarán la libertad y demás garantías consagradas en la Constitución.*

8 http://www.camdip.gov.py/leyes/2001/py1682_16012001.pdf

La correspondencia y demás formas de comunicación privada son inviolables. Sólo pueden ser interceptadas o registradas mediante orden judicial, en los casos y con las formalidades que establezca la ley". Una reciente reforma con el fin de prevenir la comisión de actos terroristas —declarada inexequible por la Corte Constitucional— permitía interceptar o registrar la correspondencia y demás formas de comunicación privada sin previa orden judicial.[9]

En Ecuador, los artículos 30 a 45 de la Ley de Control Constitucional (18 de junio de 1997) regulan el *habeas data.* El artículo 6 de la Ley Orgánica de Transparencia y Acceso a la Información Pública (4 de mayo de 2004) establece que *"Se considera información confidencial aquella información pública personal, que no está sujeta al principio de publicidad y comprende aquella derivada de sus derechos personalísimos y fundamentales, especialmente aquellos señalados en los artículos 23 y 24 de la Constitución Política de la República. El uso ilegal que se haga de la información personal, o su divulgación, dará lugar a las acciones legales pertinentes".*

En Perú el artículo 14 del Código Civil, establece que "La intimidad de la vida personal y familiar no puede ser puesta de manifiesto sin el asentimiento de la persona o si ésta ha muerto, sin el de su cónyuge, descendientes, ascendientes o hermanos, excluyentemente y en este orden". La ley 27.806 de Transparencia y Acceso a la Información Pública (13 de julio de 2002) en el artículo 15 exceptúa del derecho de acceso *"La información referida a los datos personales cuya publicidad constituya una invasión de la intimidad personal y familiar. La información referida a la salud personal, se considera comprendida dentro de la intimidad personal. En este caso, sólo el juez puede ordenar la publicación sin perjuicio de lo establecido en el inciso 5 del artículo 2 de la Constitución Política del Estado".*[10]

En Uruguay en la Ley 17.838 de Protección de Datos Personales para ser utilizados en Informes Comerciales y Acción de *Habeas Data* (1 de octubre de 2004), se exceptúa —en el artículo 2— *"el tratamiento de datos que no sean de carácter comercial como por ejemplo:* a) *datos de carácter personal que se originen en el ejercicio de las libertades de emitir opinión y de informar, así como los relativos a encuestas, estudios de mercado o semejantes, los que se regularán por las leyes especiales que les conciernan y que al efecto se dicten; y* b) *datos sensibles sobre la privacidad de las personas, entendiéndose por éstos, aquellos datos referentes al origen racial y étnico de las personas, así como sus preferencias políticas, convicciones religiosas, filosóficas o morales, afiliación sindical o información referente a su salud física o a su sexualidad y toda otra zona reservada a la libertad individual",* pero se establece que para *"Para la obtención y tratamiento de datos que no sean de carácter comercial se requerirá expresa y previa conformidad de los titulares, luego de informados del fin y alcance del registro en cuestión".*

En México no existe legislación federal de protección de datos personales, excepto en algunos aspectos regulados por la Ley Federal de Transparencia y Acceso a la Información Gubernamental (11 de junio de 2002) y la Ley para regular las Sociedades

---

9 Por el Acto Legislativo 2 de 2003 (www.secretariasenado.gov.co/leyes/ACL02003.HTM) fue modificado el texto original, y a su vez declarado inexequible por la Corte Constitucional mediante Sentencia C-816-04 de 30 de agosto de 2004 (www.secretariasenado.gov.co/leyes/SC816_04.HTM).

10 El texto corresponde al articulo 15-B. Información confidencial, inciso 5 según las modificaciones introducidas por la ley 27.927 (3 de febrero de 2003)

de Información Crediticia (15 de enero de 2002). Algunas leyes estatales de acceso a la información, como las de Guanajuato, Michoacán de Ocampo y Sinaloa contienen un capítulo dedicado a la protección de datos personales, las tres leyes contienen la obligación de declarar explícitamente la finalidad de las bases de datos generadas y difundidas por los órganos del gobierno, norma que no existe en ninguna otra legislación latinoamericana.[11]

En otros países existen leyes de acceso con algunas consideraciones sobre datos personales: Trinidad & Tobago, *Freedom of Information Act* (5 de noviembre de 1999); Belize *Freedon of Information Act* (31 de diciembre de 2000); Jamaica *Access to Information Act* (24 de Julio de 2002); y, Republica Dominicana, Ley 200-04 de Libre Acceso a la Información Publica (28 de julio de 2004)

Algunos países han desarrollado además algunas leyes que contemplan la protección de datos desde una visión sectorial, o que se relacionan de alguna forma con los datos personales, por ejemplo:

Argentina: *Ley* 25.392 *de Creación del Registro Nacional de Donantes de Células Progenitoras Hematopoyéticas* (30 de noviembre de 2000); Ley 6.879 de la Provincia de Mendoza sobre el *Registro de Deudores Alimentarios Morosos* (26 de febero de 2001);[12] Ley 23.798 *de Prevención y Lucha contra el Síndrome de Inmunodeficiencia Adquirida (SIDA)* (20 de septiembre de 1990);

Colombia: El artículo 38 de la Ley 23 de 1981 regula los datos de la historia clínica (bajo la forma de revelación de secreto del profesional médico); la Circular 004 de 2003 del Archivo General de la Nación regula *"Los espacios destinados al archivo de Historias Laborales, deben ser de acceso restringido y con las medidas de seguridad y condiciones medioambientales que garanticen la integridad y conservación física de los documentos";*

Costa Rica: Ley General sobre el VIH-SIDA (artículo 43);

Chile: Ley sobre cambio de Nombres y Apellidos;13

---

11 En Panamá el proyecto de ley 2004-A-067 para modificar la ley 24 de 2002 explicitaría (artículo 4-A) las "*Finalidades de la base de datos*. Los datos sobre historial de créditos de los consumidores o clientes suministrados por los agentes económicos a las agencias de información de datos, solo será empleada para: 1. Conocer el historial de crédito de los clientes o consumidores, en el preciso momento que estos realicen transacciones bancarias, económicas, financieras, comerciales o industriales, y siempre que medie autorización escrita del cliente o consumidor. 2. Reflejar el movimiento de pagos, abonos y cancelaciones de las obligaciones que mantienen los clientes o consumidores con los agentes económicos. 3. Servir de referencia crediticia, en cualquier momento, cuando el cliente o consumidor autorice al respectivo agente económico a obtener la información contenida en la base de datos para el propósito especificado en la autorización de que se trate. 4. Reflejar el estado de las deudas morosas por más de tres meses de los clientes o consumidores cuyo pago le hubiere sido exigido por el departamento de cobros del respectivo agente económico, y que le haya sido debidamente notificado. 5. Reflejar el estado de las deudas morosas de los clientes o consumidores exigidas por vía de mandamiento de pago judicialmente decretado o por medio de sentencia en firme proferida en proceso ordinario.

12 http://www.jus.mendoza.gov.ar/rda/ley_6879.htm

13 Ley 17.344 (http://colegioabogados.org/normas/leyes/17344-cambionombres.htm). El nombre no es sólo un elemento de individualización, sino que también es expresión de pertenencia étnico cultural; el apellido revela toda una historia familiar o un origen, e incluso aquellos apellidos que han sido traducidos, fonetizados o modificados por los errores de trascripción de los registros civiles estarían mostrando además datos migratorios. También si un apellido es frecuente o raro estaría marcando una

Ecuador: Ley Reformatoria a la *Ley de Discapacidades* [artículo 14 sobre el Registro Nacional de Discapacidades, reglamentado provisoriamente por el Reglamento General de la Ley sobre Discapacidades del 4 de febrero de 1994, ver artículos 51 y 52];

Guyana: *Domestic Violence Act* (31 de diciembre de 1996) §43.(3); y *Occupational Safety and Health Act* (9 de diciembre de 1997) §47.(m)

Paraguay: Ley sobre Información de Carácter Privado;

Perú: Normas reglamentarias para los casos de homonimia;

Trinidad & Tobago: *DNA Identification Act* [sections 39 & 40];

Uruguay: *Código de la Niñez y la Adolescencia* (14 de septiembre de 2004) artículos 218 a 222 sobre el registro de información de niños y adolescentes.

Venezuela: *Ley de Transfusión y Bancos de Sangre* [artículo 44]; Ley sobre Protección a la Privacidad de las Comunicaciones

La jurisprudencia ha tenido la carga de llenar imprecisiones y los vacíos normativos. Algunos ejemplos de casos decididos por los más altos tribunales latinoamericanos son: En Argentina: *Dirección General Impositiva vs. Colegio Público de Abogados de la Capital Federal*, 1996 (información personal que figura en los registros, archivos y bancos de datos computarizados); *Ponzetti de Balbín, Indalia vs. Editorial Atlántida, S.A.* 1984 (derecho a la intimidad —personas voluntariamente públicas); *Granada, Jorge Horacio vs. Diarios y Noticias S.A.* 1993 (responsabilidad por datos erróneos); *Urteaga vs. Estado Nacional* 1998 (acceso a la información); *Ganora vs. Estado Nacional* 1999 (Habeas data puede ser usado para todas las bases de datos gubernamentales); *Lascano Quintana vs. Veraz S.A.* 2001 (información crediticia). En Chile: *Bohme Bascuñán, Manuel vs. Clínica Alemana,* 1992 (filmaciones no autorizadas) y *CODEPU vs. Gendarmería de Chile,* 1995 (micrófonos en cárceles). En Costa Rica: *C. A., E. vs. Aludel Ltda.,* 2000 (información crediticia) y *M. M., C. vs. Aludel Ltda*., 2002 (exactitud de la información). En Colombia *In re* Manuel Cifuentes, 2000 (habeas data y principio de finalidad). En Panamá: *Guillermo Cochez vs. Ministro de Relaciones Exteriores,* 2002 (la planilla de una institución gubernamental no es de carácter reservado) y *Aluminio Estructural y otros vs. Director General de Ingresos,* 2002 (la información acopiada en ejercicio de la función fiscalizadora es de acceso restringido). En Venezuela: *N. A. y otros*, 1998 (datos sensibles, infección VIH), *R. C. M. y otros vs. Consejo Nacional Electoral*, 2000 (acceso a los padrones electorales) y *G. B., X. vs. Juzgado de Protección del Niño y del Adolescente del Estado Lara,* 2002 (redacción de sentencias judiciales); y casos sobre *passagem*[14] en Brasil.

---

vulnerabilidad diferencial para los procesos de búsqueda e identificación, pues una forma de conservar la intimidad es tener un apellido común y caer dentro de la saturación de una búsqueda

14 Práctica muy común en Brasil por la que se informa el número de consultas sobre una misma persona realizadas durante un periodo determinado, situación que indicaría —que pese ha haber sido buen pagador— podría estar comprometiendo peligrosamente su capacidad de pago.

En otros paises (por ejemplo México y Costa Rica) existen proyecto de legislación sobre protección de datos personales, o de temas conexos, por ejemplo en Guyana *e-Comerce Bill.*[15]

2. Equilibrio entre acceso a la información y protección de datos personales.

Fundamentalmente las leyes de acceso establecen criterios de confidencialidad y reserva, como una limitación al acceso a ciertos datos en la esfera pública. Los fundamentos son seguridad nacional, intimidad o precaución en ciertos actos preparatorio cuya publicidad podría limitar o impedir su eficacia. El principal problema se produce cuando el Estado acumula datos personales, y el hecho que estén almacenados en la esfera pública no necesariamente los trasforma en información gubernamental o de dominio público. Las leyes de acceso suponen, pero no enfatizan, que el derecho de acceso está dirigido a establecer como ejercen los funcionarios estatales sus funciones. Efectivamente, si ciertos datos personales o íntimos son confiados por particulares al Estado para la toma de decisiones, el derecho de acceso no necesariamente alcanzaría la totalidad de esos datos, sino sólo en la medida que esos datos son necesarios para establecer si el proceder del Estado ha sido dentro de la ley; entonces en la gran mayoría de los casos los nombres de las personas no son necesarios para realizar este control ciudadano.

La *Declaración de Principios sobre Libertad de Expresión* de la Comisión Interamericana de Derechos Humanos:[16]

> 10. "Las leyes de privacidad no deben inhibir ni restringir la investigación y difusión de información de interés público. La protección a la reputación debe estar garantizada sólo a través de sanciones civiles, en los casos en que la persona ofendida sea un funcionario público o persona pública o particular que se haya involucrado voluntariamente en asuntos de interés público. Además, en estos casos, debe probarse que en la difusión de las noticias el comunicador tuvo intención de infligir daño o pleno conocimiento de que se estaba difundiendo noticias falsas o se condujo con manifiesta negligencia en la búsqueda de la verdad o falsedad de las mismas."

introduce dos aspectos muy interesantes. En primer lugar da la sensación de un conflicto o tensión entre la libertad de expresión —y el correlativo derecho de acceso a la información— y la protección de los datos personales. Sin embargo ciertos aspectos de la protección de datos personales han sido encuadrados dentro del derecho de autodeterminación informativa (mencionado por primera vez por la Corte Constitucional de Alemania). La referencia —entonces— a la libertad de expresión (y no a un derecho de expresión) supone la existencia de dos derechos, el derecho a expresarse y el derecho a no expresarse, y precisamente este último —en realidad ambos— está íntimamente relacionado con la autodeterminación informativa, en el sentido que una persona no podría ser obligada a expresar ciertos datos personales. En la medida que sea posible establecer esta vinculación, y en esa medida, no podrá hablarse de un conflicto entre derechos que generalmente tiende a resolverse prefiriendo la libertad de expresión.

---

15 www.mintic.gov.gy/documents/Draft_E_Commerce_Bill_2005.pdf
16. www.cidh.oas.org/relatoria/spanish/Declaracion.htm

El segundo aspecto que introduce la *Declaración de Principios sobre Libertad de Expresión* es la categoría de *"funcionario público o persona pública o particular que se haya involucrado voluntariamente en asuntos de interés público"*. Este concepto extensamente desarrollado en la jurisprudencia norteamericana (y la de California en particular) no tiene prácticamente ningún desarrollo legislativo ni jurisprudencial en América Latina.[17] En el Caribe si existen leyes como la de Guyana, *Integrity Comisión Act* (24 de septiembre de 1997) y Trinidad & Tobago, *Integrity in the Public Life Act* (1999) en las que se enumeran los funcionarios públicos cuyos datos personales tienen una menor protección.

Aun así, parece cada vez más necesario generar un marco regulatorio adecuado y eficaz para evitar que el juego de derechos e intereses que están detrás del acceso y de la protección de datos personales no se transformen en riesgos o violaciones. Volviendo a la *Declaración de Principios sobre Libertad de Expresión* en América Latina, los sistemas de responsabilidad civil (o *"sanciones civiles"*) —en manos de los jueces— son muy disímiles, y aun cuando en algunos países se asemejan a la tradición europea o norteamericana, en la mayoría son económicamente irrelevantes y en algunos casos han sido declaradas inconstitucionales.[18]

3. Registros Estatales

Tradicionalmente los gobiernos asumieron la responsabilidad de generar y gestionar los registros civiles, de capacidad de las personas y los de propiedad. Hace ya algunos años —y manteniendo aun los libros o fichas como sistema de registro— se fueron generando otros registros públicos, por ejemplo en casi todos los países de la región existen registros de antecedentes penales y carcelarios adecuadamente legislados. Sin embargo, fue en los últimos años que los procesos de informatización de la función pública y la posibilidad de acceder y tramitar vía Internet provocaron la proliferación de todo tipo de sistemas de información con datos personales. En estos casos la información —accesible en forma rápida y oportuna— ha sido vista como una necesidad para establecer servicios estatales más eficientes y también más trasparentes. En este sentido muchos servicios públicos como escuelas; hospitales; teléfonos, recaudación de impuestos, entre otros, comenzaron a registrar datos personales e información que hace a las actividades de las personas. En algunos casos se trata de información claramente sensible como, por ejemplo niños en riesgo que están recibiendo medidas estatales de protección, pero la gran dificultad consiste en pasar de una definición enumerativa de datos sensibles (como la de la Directiva Europea 95/46/CE) a una definición que surja del uso efectivo que se hace de esos datos; concretamente sí esos datos se están o pueden utilizarse para discriminar injustamente.

Algunos servicios de búsqueda en Internet son irrestrictos: *e.g.* **Brasil:** Relação de Apenados (personas privadas de libertad, Estado de Paraíba);[19] Relação nominal dos presidiários fugitivos (Estado de Paraíba);20 **Costa Rica:** Descarga del Padrón Electoral

17 Gary Williams, ¿El derecho constitucional a la privacidad en California, protege a las figuras publicas de la publicación de información confidencial personal?, en *Internet y Sistema Judicial en América Latina — Reglas de Heredia* (2004) 325-338, Editorial Ad-Hoc, Buenos Aires.

18. Ver *José G. Romano Larroca vs. Editorial Perfil S.A.*, probablemente la indemnización más alta concedida en Argentina por invasión a la privacidad (60.000 dólares), y aun así es irrelevante dentro del negocio editorial [http://lac.derechos.apc.org/clegislacion.shtml?x=9471].

19 http://www.tj.pb.gov.br/apenados/_index.jsp

20 http://www.paraiba.pb.gov.br

Ordenado por Número de Cédula,[21] Registro Nacional (bienes muebles e inmuebles).[22] Otros requieren la inscripción previa, y se accede con usuario y contraseña, algunos ejemplos son: **Argentina:** Registro de Deudores Alimentarios Morosos (Provincia de Mendoza);[23] **Panamá:** Servicio de Verificación de Identidad (Tribunal Electoral);[24] **Uruguay:** Abogados y Escribanos suspendidos,[25] además se está planificando la adopción de una historia clínica electrónica única.[26] Muchos sitios han evolucionado en los últimos años y han suprimido la búsqueda por nombre y apellido, ofreciendo ahora el servicio a partir de un número personal, algunos ejemplos son: **República Dominicana:** Consulta *on line* Al Padrón Electoral;[27] **Uruguay:** verificación del padrón electoral;[28] **Venezuela:** Registro Electoral.[29]

4. Registros Privados

También se han generado exponencialmente registros privados, y en la mayoría de los casos son los mismos usuarios quienes brindan la información. Bancos, empresas de tarjetas de crédito y compañías aéreas son buenos ejemplos de cómo correlacionar datos personales vinculados a actitudes personales resulta de utilidad como prevención de determinados delitos o la optimización de algunos servicios. Así si el proveedor de una tarjeta de crédito dispone del perfil de consumo de una persona puede detectar en tiempo real alguna compra que presuntamente corresponda a una tarjeta robada, e interceptarla antes de que el delito se consume. Igualmente si una compañía aérea dispone de ciertos perfiles de sus pasajeros, puede optimizar sus servicios y hasta predecir la probabilidad de *no show* de un pasajero o en un vuelo.

Los sistemas de registro de antecedentes crediticios (bureaux de crédito),[30] han desarrollado un mecanismo de acceso al crédito (fundamentados en la necesidad de procedimientos más eficientes para acceder al crédito a sola firma, sin garantías reales o personales, y la búsqueda de incentivos para el pago, más eficaces que la ejecución judicial), especialmente en el sector del comercio. El acceso y disponibilidad del historial de pago como mecanismo para la concesión del crédito ha sido denominado "democratización del crédito" pues abrió esta posibilidad a sectores cuya única garantía es su condición de buen pagador.[31]

Aprovechando el vacío legal las empresas de riesgo crediticio ocuparon un importante lugar en el mercado, que fue seguido por una creciente litigiosidad. Cuando estas empresas eran pequeñas y nacionales, la informalidad y falta de seguridad en las bases de datos estatales, facilitó que se obtuvieran bases de datos a partir de la compra ilegal

---

21 http://www.tse.go.cr/downloads.html
22 http://196.40.22.13/rnb_inmuebles/inconfinca_id_new.html y http://196.40.22.13
23 http://www.jus.mendoza.gov.ar/rda/consultas/index.htm
24 http://www.tribunal-electoral.gob.pa/servicios/servicios-online/svi.html
25 "Profesionales Suspendidos" en http://www.poderjudicial.gub.uy/pls/portal30/portal30.rentrar
26 Ver Decreto, http://www.presidencia.gub.uy/decretos/2003093001.htm.
27 http://web.jce.do/consultas/ced2004.asp
28 http://www.corteelectoral.gub.uy/consweb/hcons_partidos.exe
29 http://www.cne.gov.ve/ce.php
30. En algunos países los antecedentes crediticios son registrados por el Estado, por ejemplo en Argentina quienes libran cheques sin fondo son registrados por el Banco Central y en El Salvador existe una base de antecedentes crediticios administrada por la Superintendencia del Sistema Financiero.
31. Rafael del Villar, Alejandro Díaz de León y Johanna Gil Hubert, *Regulación de Protección de Datos y de Sociedades de Información: Una Comparación de Países Seleccionados de América Latina, los Estados Unidos, Canadá y la Unión Europea,* Banco de México, Documentos de Investigación 2001-7.

de datos. Luego la mayoría de estas empresas en la región o fueron adquiridas por empresas transnacionales (Equifax, por ejemplo) o esta función comenzó a desarrollarse en la Cámaras de Comercio (en Brasil, por ejemplo), esto llevó a una mayor legalidad en la obtención de datos y suministro de informes.

Sin embargo estos sistemas entran en colisión con los derechos de privacidad e intimidad, y son alicientes para la discriminación laboral especialmente cuando se desarrollan en un vacío legal. Efectivamente, uno de los problemas más delicados observados es su incidencia en el acceso al empleo. Desde 2001 la Sala Constitucional de la Corte Suprema de Costa Rica ha recibido varias demandas laborales vinculadas con esta actividad, en las que algunas personas fueron despedidas o no contratadas por haber sido testigos o víctimas de delitos o por los informes crediticios de sus familiares. El problema radica en que el empleado (o potencial empleado) no es informado sobre el pedido de informes y puede ser discriminado sin percibirlo. El tema es aun más critico cuando se discrimina a un candidato a un empleo por haber realizado en el pasado acciones laborales contra su empleador (esto es posible por la disponibilidad en Internet de los juicios laborales iniciados).[32]

La dificultad reside en que algún organismo de control estatal debería cerciorarse que los datos —que se acumulan y suministran— sean legales y no discriminatorios (por ejemplo no podrían almacenar información sobre personas infectadas con VIH u otras enfermedades que no impidan socialización), pero esta tarea es de difícil concreción.

Recientemente este mismo procedimiento de almacenar historiales personales se ha extendido a otras actividades, como el mercado inmobiliario (personas que han sido desalojadas por no pagar sus arrendamientos) o bancaria (que va desde libradores de cheques sin fondo a listas de clientes molestos, donde molesto se define como alguien que ha realizado más de dos quejas).

La difusión de información en Internet ha generado algunas situaciones particulares, por ejemplo existen sitios sobre búsqueda libre en Internet por nombre y apellido (no se incluyen los sitios judiciales que serán tratados aparte): **Argentina:** Personas desaparecidas en la Argentina entre 1975 y 1983,[33] Personas Desaparecidas y Responsables de desapariciones,[34] Ex-Alumnos del Colegio Nacional de Buenos Aires;[35] **Chile:** Médicos Colegiados (Colegio Medico de Chile);[36] **Guatemala:** búsqueda de bodas,[37] (corresponde a bodas de hace dos meses y las de los próximos seis meses); **México:** Sociedad Mexicana de Oncológica (profesionales matriculados),[38] Ganadores del sorteo de Libretón (participan en los sorteos mensuales todas las cuentas de ahorro denominadas *El Libretón* de Bancomer BBVA, vigentes al mes anterior a la

32. Presionados por quejas y consientes de posibles acciones discriminatorias algunos Poderes Judiciales han desactivado estas funciones de búsqueda en sus *websites*, el Poder Judicial que canceló su buscador formalmente es el Tribunal Superior do Trabalho de Brasil (30/08/2002) precedida por una decisión similar del Tribunal Regional do Trabalho da 24° Região (Estado do Mato Grosso do Sul) del 13/12/2001. Ver Mário Antônio Lobato de Paiva , *"A difusão de informações judiciais na Internet e seus efeitos na esfera trabalhista"*

33. http://www.sinolvido.org/newQuery.jsp

34 http://www.nuncamas.org/formularios/formular.htm

35 http://www.cnba.uba.ar/exalumnos/busqueda.php

36 http://www.colegiomedico.cl/medicos_colegiados.asp

37 http://www.granboda.cemaco.com/buscar.asp

38 http://www.smeo.org.mx/Busqueda.php

realización de cada sorteo y cuyo saldo promedio en dicho mes, sea igual o mayor a $3,000.00. La participación no es voluntaria);[39] **Uruguay:** Búsqueda de Escribanos Jubilados;[40] **Venezuela:** Egresados de la Universidad de Carabobo.[41]

Entre estos algunos tienen características totalmente distintas, pues hacen a personas públicas o a la seguridad pública: **Argentina:** Militares responsables de desapariciones;[42] **Ecuador:** Directorio de Candidatos para las Elecciones del 2002.[43]

Esto muestra la necesidad de formular recomendaciones, buenas prácticas y claridad sobre que tipo de acceso es razonable para cada servicio.

5. Políticas Publicas

5.1. En el Poder Ejecutivo

Prácticamente no existen políticas publicas explicitas sobre acumulación, uso y seguridad de las bases de datos con datos personales. Probablemente la causa se deba a que estos sistemas fueron desarrollados por equipos informáticos, internos o externos, que no percibieron que estos desarrollos podían tener algún impacto en los derechos. Cierta brecha generacional, en la que las autoridades públicas desconocían la arquitectura informática puede haber incidido en la continuidad y crecimiento de estos sistemas.

Ciertamente hay dos puntos débiles en la generación de registros públicos, *viz.* la falta de una definición previa y explicita de *"finalidad"* en función de la cual podrían definirse políticas que equilibren beneficios con vulnerabilidad; y la inexistencia de políticas de seguridad de los datos, tanto en aspectos prácticos como en sanciones penales y procedimientos probatorios para el robo de información.

En la práctica muchos de los datos acumulados son innecesarios para la función pública, o al menos los beneficios que aporta su almacenamiento son menores que la vulnerabilidad que generan. Por ejemplo, la ley Argentina (pre-informática) de partidos políticos establecía que la Justicia Electoral registrara la afiliación a los partidos políticos, así al afiliarse a un partido se completaba una ficha de cartón que era enviada al registro para verificar que esa persona no estaba afiliada a otro partido. El fundamento de este registro y del procedimiento se relacionaba con la contribución económica que hace el Estado a los partidos políticos, que se realiza en función del número de afiliados. Con la informatización creciente de los últimos años, pareció razonable —claro desde el punto de vista informático, no del jurídico— informatizar estos datos e incorporarlos al padrón electoral. Una vez que la base de datos esta disponible, es natural que se piense en otros usos ajenos a la finalidad original, así fue que un partido político solicitó —en virtud e tratarse de información pública— que se le expidiera una copia del padrón, incluyendo los datos de afiliación. El caso llegó a la justicia electoral y en el fallo es posible ver como los jueces terminan tomando

39 http://www.bancomer.com.mx/ganadores/busca13.html
40 http://cavern.montevideo.com.uy/cajanotarial/hbusqueda.cgi
41 http://150.186.52.79:8069/busquedas/egresados/egre.html
42 http://www.nuncamas.org/formularios/respons.asp
43 http://www.viviendolademocracia.org/seccional.jsp

decisiones sin la perspectiva histórica ni analizando las consecuencias en forma amplia.[44]

Casos como este pueden extenderse rápidamente a los datos de migración, datos genéticos, escolares, por ejemplo.

5.2. Información judicial

La información judicial representa el paradigma más crítico de información personal y datos personales —*i.e.* de carácter privado— que ingresan a la esfera pública. Además es frecuente que estos datos se relacionen con aspectos íntimos de las personas, *e.g.* conflictos interpersonales como divorcios o delitos, responsabilidades, datos de salud. Cuando el dato ingresa en la esfera pública, éste es inmediatamente visto como un dato de acceso publico y a veces de dominio público. Guillermo Cosentino ha escrito muchos argumentos que deben ser tenidos en cuenta para entender que esta conclusión no es tan inmediata como parece.[45]

La informatización de la información judicial ha conducido al mismo tiempo a una dilema y a una paradoja. La tendencia predominante en América Latina y el Caribe es a facilitar el acceso a la información procesal directamente vía Internet, aquí debe entenderse que la ineficiencia (lentitud) que aqueja ya históricamente a los procesos judiciales necesitara reacciones casi heroicas; cuando se pudo ver que disponibilizar datos por Internet era un cambio hacia la eficiencia, no existieron dudas.

La información procesal que se publica hace fundamentalmente a datos y decisiones de las partes, pero la publicación de sentencias judiciales —en las que evidentemente debe estar fundamentado como el sistema judicial resuelve los conflictos que le son sometidos— hace inequívocamente a la función pública, y por tanto, debe ser trasparente.

Es contradictorio que en algunos países (*e.g.* Ecuador, México) la información procesal tenga amplia difusión en Internet, mientras que prácticamente no se publican sentencias judiciales en los sitios oficiales en Internet. La razón más probable es que muchos jueces están acostumbrados a redactar sentencias —en el mejor de los casos— para ser leídas sólo por juristas —y en el peor de los casos, en un español extraño y primitivo, que oculta imprecisiones y una pobre fundamentación.

La paradoja se presenta cuando se percibe que prácticamente ningún sitio en Internet de los poderes judiciales de la región publica edictos. Los edictos son los documentos judiciales vinculados a datos personales que necesitan mayor difusión y accesibilidad, pues de su acceso depende el derecho de defensa. En teoría los edictos tendrían que resultar accesibles no sólo por buscadores en los sitios judiciales, sino también por buscadores universales (Google, Altavista, Yahoo), en la práctica sólo existe un sitio privado en Ecuador desarrollado por el periódico La Hora con un buscador para edictos.

---

44 Ver el fallo de la Cámara Nacional Electoral (Argentina): *Susana T. Sánchez Morteo, coapoderada del Partido Nacionalista Constitucional*, http://www.iijlac.org/modules.php?name=Articulos&artid=46

45 Guillermo Cosentino, 'La información judicial es pública, pero contiene datos privados. Cómo enfocar esta dualidad', en *El acceso a la información judicial en México: una visión comparada* (2005) 247-267, UNAM, http://www.bibliojuridica.org/libros/4/1646/19.pdf

Todos estos conflictos y paradojas son el resultado de procesos de informatización realizados en un vacío de políticas públicas. Llenar este vacío, proponiendo recomendaciones, fue el objetivo de las *Reglas de Heredia*.

Estas *Reglas* están aun muy lejos de ser el estándar en América Latina y el Caribe, ya que absolutamente ningún poder judicial de la región las cumple en un contexto de trasparencia. Existen notables aproximaciones, como la del Poder Judicial de Nayarit (México) que permite acceder a la información procesal sólo con el número de caso, pero no difunde ninguna sentencia; igual situación puede decirse de la Cámara de Apelaciones en lo Civil de la Ciudad de Buenos Aires, en este caso son sólo accesibles las sentencias de primera instancia y vinculadas al número de caso, o del Tribunal Superior do Trabalho de Brasil, que inhibió la búsqueda procesal por nombre del empleado, pero mantiene la búsqueda sobre las decisiones.

En términos de política pública judicial, está perfilándose una tendencia que se podría traducir así: existe derecho de acceso a la información judicial en función de cierto criterio —jurídico o fáctico— de búsqueda, pero no existe el derecho a una descarga de la totalidad de las bases de datos judiciales. Esta hipótesis se deduce del hecho que algunos sitios de los poderes judiciales (el primero en América Latina ha sido el Tribunal de Justiça do Estado do Rio Grande do Sul, Brasil) han agregado a la consulta un texto en formato grafico que es necesario ingresar en forma de caracteres para acceder a los resultados de la búsqueda, este es un procedimiento para evitar que programas o robots generen automáticamente búsquedas que tienen por sola finalidad la descarga completa de la base de datos. Esta práctica es una actividad comercial supuestamente lucrativa, un ejemplo de ello es el Buró de Informaciones Legales (México) que descarga diariamente toda la información procesal publicada por los poderes judiciales estatales y la vende a sus clientes.[46]

6. Progreso económico vs. protección de datos

En varios aspectos el uso y difusión de los datos personales es visto como necesario para facilitar el progreso económico. En primer lugar los sistemas de registro de antecedentes crediticios (burós o bureaux de crédito),[47] han desarrollado un mecanismo —muy eficiente— de acceso al crédito y de disuasión del no pago de las deudas. Los mecanismos de trasparencia son vistos también como una forma eficaz de evitar la corrupción en el sector público.

En general se ha instalado la hipótesis que una sociedad más trasparente en instituciones y personas debería conducir a una sociedad con menos conflictos, incluso algunos autores del género de ciencia-ficción han ideado comunidades que han evolucionado para que las mentes de las personas sean absolutamente trasparentes y por tanto ya no tenga sentido la mentira.

Si en alguna medida se ha producido esta evolución, ésta ha sido absolutamente asimétrica. Mientras que se pide trasparencia para el Estado y para la vida de las personas, las grandes corporaciones mantienen secretos comerciales y todas sus

46 www.bil.com.mx

47. En algunos países los antecedentes crediticios son registrados por el Estado, por ejemplo en Argentina quienes libran cheques sin fondo son registrados por el Banco Central y en El Salvador existe una base de antecedentes crediticios administrada por la Superintendencia del Sistema Financiero.

decisiones —como los procesos de contratación de personal— son naturalmente reservadas e indiscutibles. En la práctica son ellas las que han creado listas negras o bases de datos de clientes molestos, que se traducen en mecanismos que tienden a optimizar la rentabilidad de sus decisiones.

Conclusiones

En los últimos años la sociedad latinoamericana se ha visto presionada en diferentes sentidos. Las corrientes contrapuestas de opinión entre Europa y EE.UU., sobre la protección de datos personales, se ven claramente fotografiadas en la legislación (o en las lagunas normativas) de algunos países en América Latina.[48] Así Argentina es el modelo de la aproximación a Europa, y entre los factores que han gravitado es necesario resaltar el uso que las dictaduras militares hicieron de los datos personales en la desaparición de personas. México es el modelo de aproximación a EE.UU. que queda de manifiesto con la fuertísima política de transparencia que ha puesto en marcha el gobierno de presidente Vicente Fox, que también debe ser vista desde una historia de opacidad pública.

Además de estos ejemplos —que podrían denominarse *Europa vs. EE.UU.*— que pesa sobre legisladores, jueces, gobernantes y sociedad civil latinoamericana, está presente también otro predicamento mucho más cotidiano, que contrapone *"protección de datos personales vs. progreso económico y social"*.

La amenaza de terrorismo —que ha impactado las prácticas de privacidad en otras regiones— no es quizás la más relevante en América Latina (aunque si hay algún indicio en Colombia); más probablemente las fuertes expectativas sobre la lucha contra la corrupción, eficiencia administrativa, seguridad ciudadana, democratización del crédito, son vistas por muchos como más prioritarias que la protección de la vida privada. El problema surge de la hipótesis subyacente que estima que con un espacio mucho menor de privacidad e intimidad —con personas más trasparentes— podría garantizarse una sociedad con mayor estado de bienestar. La idea no es ajena a otros planos de discusión en los que las garantías jurídicas son vistas como un costo muy alto para los ciudadanos "honestos", el argumento es: "póngase en el lugar de una persona que se llama Juan Pérez que nunca fue parte de un proceso judicial, que paga sus deudas, es propietario de su casa y vive en una familia tipo; y entenderá porque no tiene nada que ocultar".

La idea de llamarle Juan Pérez es usar nombre que saturaría cualquier búsqueda informática, para resaltar las ventajas implícitas de los grupos suficientemente grandes. Contrariamente las víctimas están mayoritariamente entre las minorías, de allí que la sociedad democrática evolucionó al crear garantías individuales. El concepto tradicional de los derechos de las minorías, ha tenido un amplio desarrollo en instrumentos internacionales (Naciones Unidas) que se basan en la protección de los derechos humanos, las libertades individuales y los principios de no discriminación e igualdad — se estimaba que si se aplicaban efectivamente las disposiciones de no discriminación, serían innecesarias las disposiciones especiales sobre los derechos de las minorías. Hoy

48 Ver Carlos G. Gregorio, 'Protección de Datos Personales: Europa vs. Estados Unidos, todo un dilema para América Latina', en *'Transparentar al Estado: la Experiencia Mexicana de Acceso a la Información'*, Hugo Concha Cantú, Sergio López-Ayllón, Lucy Tacher Epelstein (eds.), (2004)

la accesibilidad a datos personales —y no necesariamente a datos sensibles— permite construir grupos difusos de personas que coinciden en algún perfil.[49] De esta forma surgen entre los ciudadanos diferentes sensibilidades con respecto a algunos grupos: ... no es igual pensar en el grupo de personas que alguna vez iniciaron una acción laboral contra su ex empleador; o que se han divorciado recientemente; o que son portadores de VIH, o que son o han sido dirigentes sindicales; ... que en el grupo de personas que han fallado alguna vez en sus obligaciones de pago; o que han sido condenados por algún delito, y (con una sensibilidad aun mayor), por ejemplo, si este delito es una agresión sexual contra niños.[50] Siempre ha existido demanda sobre los datos personales de alguna persona para predecir su conducta futura, pero los riesgos de tornarlos más accesibles o no, son distintos en cada caso.

El balance que es necesario hacer entre derechos e intereses en juego para inhibir, permitir o facilitar el acceso a ciertos datos personales se asemeja —por ejemplo— a una polémica reiterada —al menos en América Latina— en la que se discute y contraponen las garantías del debido proceso con la seguridad pública; o en una versión aun mucho más pedestre: si aumenta la inseguridad pública, algunos piden reducir la edad de imputabilidad penal.

Llevar a la práctica un equilibrio entre derechos supone —en cada caso particular— tener en cuenta, al definir contenidos y forma de acceso, cuál es la finalidad y cuáles son los riesgos. Por ejemplo, el Poder Judicial de Mendoza (Argentina) ha habilitado tres tipos de búsquedas que implican datos personales y las ha desarrollado con tres procedimientos totalmente distintos:[51] el acceso al *Registro de Deudores Alimentarios Morosos* requiere inscribirse e identificarse para la búsqueda; la consulta en el *Registro de Juicios Universales* (sucesiones, quiebras y concursos) es libre, sin identificación del usuario, por nombre y apellido o por documento de identidad, se obtiene información sobre la existencia del proceso, fecha de inicio y el juzgado donde está radicado el juicio; el *Registro de Detenidos* es sólo accesible por el número de expediente y se obtiene información sobre si está detenido o no, además "no se consignarán nombres ni datos personales a fin de proteger la identidad del detenido".[52] Las formas de consulta y los resultados están orientados a proteger algunos derechos, minimizando los riesgos.

La accesibilidad y difusión de datos permite la generación de clases o minorías difusas, que por su condición pueden ser discriminadas, aun al extremo de no percibirlo. La protección de los datos personales —ya sea como privacidad o autodeterminación

---

49 Isidro Cisneros, *Derechos humanos de los pueblos indígenas en México,* 2004, identifica minorías permanentes, ocasionales, móviles, difusas o corporativas, y distingue las "minorías corporativas" —minoría organizada de la subjetividad jurídica a la cual se vinculan por tendencia las pretensiones de actuar en nombre y por cuenta de todos los pertenecientes a la minoría sobre cuya adhesión se reivindica— de las "minorías difusas" —como una minoría no-organizada jurídicamente en términos unitarios, por completo desestructurada, libre por lo que se refiere a la pertenencia y cuyos adherentes no están sujetos a ninguna instrucción particular y pueden ejercer a título por completo individual los derechos, (http://directorio.cdhdf.org.mx/libros/pueblosindi.pdf)

50 En algunos países existe una fuerte corriente de opinión según la cual se demanda un libre acceso a los antecedentes penales de otras personas, hoy la mayoría de las legislaciones en América Latina prevé que éstos son solo accesibles ante el pedido de un juez o de la persona concernida. Ver: *Public Attitudes Toward Uses of Criminal History Information*, 2001, http://www.ojp.usdoj.gov/bjs/pub/pdf/pauchi.pdf.

51 www.jus.mendoza.gov.ar

52 Acordada 18. 324 bis (www.jus.mendoza.gov.ar/documental/detenidos/index.php) de 17 de marzo de 2004.

informativa— tiene por resultado dificultar la identificación de personas por características íntimas que las hacen más vulnerables. Poner en práctica esta protección requiere que la definición de “datos sensibles” —y en consecuencia, indiscutiblemente protegidos— no sea una enumeración estática, sino una definición basada en el riesgo de discriminación. Pero mantener un equilibrio de derechos (intimidad, seguridad pública, derecho de defensa, acceso al crédito, etc.) y crear un sistema de vigilancia para detectar que datos son usados para discriminar y por quienes, no es una tarea simple, y menos aun en un contexto de presiones e intereses económicos.