

## PROTECCIÓN DE DATOS PERSONALES: EUROPA VS. ESTADOS UNIDOS, TODO UN DILEMA PARA AMÉRICA LATINA

Carlos G. GREGORIO

SUMARIO: I. *Introducción*. II *Ficheros públicos y privados*. III. *Evolución del right to privacy en los Estados Unidos*. IV. *Protección de datos en Europa*. V. *Protección de datos personales en América Latina*. VI. *Las diferencias más visibles entre las posturas*. VII. *Riesgos actuales para los datos personales*. VIII. *Conclusión*.

### I. INTRODUCCIÓN

La generalización del registro de datos personales tuvo un impulso significativo a partir del Concilio de Trento (1563), que dictó normas regularizando el modo de llevar los libros parroquiales de bautismos y matrimonios. Luego la práctica impuso las defunciones, y con el tiempo, estos asientos fueron utilizados y admitidos como prueba en los contenciosos civiles.<sup>1</sup> También con el tiempo y por la creciente relevancia social de los datos, las autoridades civiles crearon los Registros Civiles (por ejemplo en España 1749, Francia 1793 y Alemania 1874) y también los Registros de Propiedad. Originalmente los registros se realizaban en libros en blanco en forma actuada, que luego fueron sustituidos por libros con textos impresos en los que se completaban los datos personales. La utilidad de estos libros dependía del sistema de generación de índices;<sup>2</sup> así cada libro

1 Existen registros anteriores pero carecen de generalidad, corresponden a cofradías, órdenes de caballería, etcétera.

2 Durante siglos los seres humanos necesitaron ampliar y proteger su memoria. Desde las pinturas rupestres, los iconos, la transmisión oral, la imprenta, y en cierta medida el arte y la historia, todos fueron mecanismos para apoyar la memoria. El hombre ha creado innumerables sistemas de registro, pero su principal problema fue encontrar mecanismos de búsqueda en esos registros. Así los “índices”

que naturalmente registraba los datos cronológicamente, tenía unas páginas al final para crear índices alfabéticos por apellidos.<sup>3</sup> Los libros se guardaban en el lugar donde se generaban los datos, sólo los libros muy antiguos (si lograban sobrevivir a la voracidad de los ratones) sufrían un proceso de centralización.

Hasta hace muy poco tiempo los registros tenían un valor fundamentalmente local (no centralizado, que se traducía, por tanto, en un débil control estatal), con herramientas muy rudimentarias de búsqueda, y su uso se limitaba a las necesidades de las personas que pretendían establecer parentesco, propiedad u otra relación jurídica.

Los sistemas de registro suelen crearse para proteger algún derecho específico, pero también pueden convertirse en obstáculo para otros derechos. En 1890 Rui Barbosa —ministro de Hacienda del Brasil en la época de la abolición la esclavitud— ordenó requisar y quemar todos los papeles, libros y documentos relacionados con los esclavos. Entre los fundamentos menciona que la República está obligada a destruir los vestigios de tan funesta institución, por honor de la patria y en homenaje a los nuevos ciudadanos. Esta decisión ejemplifica que existe una fuerte relación entre registros y derechos.<sup>4</sup>

En 1890 Samuel Warren y Louis D. Brandeis escriben su célebre ensayo *The Right To Privacy*,<sup>5</sup> Y en él dicen: “Recent inventions and business methods call attention to the next step which must be taken for the protec-

podieron resolver las búsquedas en los registros en papel. Pero existen otros procedimientos, por ejemplo, en las comunidades agrarias de Bolivia luego de llegar a un acuerdo sobre los límites de las tierras de labranza, se señalaban con muros de piedras (poyos), pero no se consideraba este medio simbólico como suficiente, se agregaba un poderoso sistema de registro; se traían varios niños pequeños a ese lugar, y allí se les castigaba duramente con varas, ellos serían memoria viva, por muchos años del lugar donde se habían acordado los lindes. Son en verdad los mecanismos de búsqueda los que producen una ampliación de la memoria.

3 También debe tenerse en cuenta que simultáneamente se generalizaba el uso de apellidos.

4 Esta decisión del 14 de diciembre de 1890 (*Diário Oficial*, edición del 18 de diciembre, p. 5845) fue muy controvertida. Hay quienes afirman que el objetivo de Rui Barbosa iba más allá de los fundamentos declarados, afirman que buscaba evitar que los ex-propietarios de esclavos demandaran al Estado un indemnización. Se transparenta entonces cierta desconfianza de Rui Barbosa en los Tribunales de Justicia, que le lleva a la eliminación de toda posible prueba; de alguna forma con la quema de los archivos de la esclavitud está afirmando que la abolición de la esclavitud no fue una expropiación sino una reivindicación. Cualquiera sea la interpretación de las motivaciones de Rui Barbosa queda clara la relación entre derechos y registros. *Obras completas de Rui Barbosa*, 1890, vol. XVII, t. II, p. 338; Río de Janeiro, Fundação Casa de Rui Barbosa, 1986.

5 Warren, Samuel y Brandeis, Louis D., “The Right To Privacy”, *Harvard Law Review*, 4, 1890, p. 193.

tion of the person, and for securing to the individual what Judge Cooley calls the right to be let alone”.<sup>6</sup> El propósito de ese artículo era establecer límites jurídicos que vedasen la intromisión de la prensa en la vida privada, motivada por el interés de Warren de frenar las informaciones escandalosas de ciertos periódicos de Boston sobre su vida conyugal.<sup>7</sup> A partir de aquí en los Estados Unidos el derecho de privacidad fue modelado por las decisiones de la Corte Suprema de Justicia, y recién en 1974 se sanciona la *Privacy Act*.

En el siglo XIX y principios del XX en Europa la intimidad fue una preocupación difusa, puesto que los posibles ataques provenían de un entorno cercano y físico (vecinos o familiares). En un segundo término podían proceder del Estado —y su eventual interés en controlar la correspondencia o las comunicaciones— y de la prensa.

Recién con la memoria magnética se generó un cambio sustancial en la acumulación de datos personales, fundamentalmente por la capacidad de duplicación, centralización y búsqueda, en tiempos y costos no significativos.

El objetivo de este trabajo es analizar las diferencias entre los modelos europeos y americanos de la intimidad (*right to privacy* y autodeterminación informativa) y como los argumentos de Warren y Brandeis sobre los inventos recientes y prácticas comerciales son hoy cada vez más vigentes. Se intenta analizar y argumentar cuál es el mejor modelo para América Latina, en función de las historias recientes de totalitarismos y de la capacidad de los Poderes Judiciales para crear garantías caso a caso. También se intenta resaltar que el verdadero problema son las facilidades de búsqueda intensiva (motores de búsqueda). Entre otros dilemas se analizarán

6 Warren y Brandeis citan a McIntyre para introducir el “derecho a ser dejado sólo” (McIntyre Cooley, Thomas, *Treatise of the Law of Torts*, 1888: “Personal immunity. The right to one’s person may be said to be a right of complete immunity: to be let alone. The corresponding duty is, not to inflict an injury, and not, within such proximity as might render it successful, to attempt the infliction of an injury. In this particular the duty goes beyond what is required in most cases; for usually an unexecuted purpose or an unsuccessful attempt is not noticed. But the attempt to commit a battery involves many elements of injury not always present in breaches of duty; it involves usually an insult, a putting in fear, a sudden call upon the energies for prompt and effectual resistance. There is very likely a shock to the nerves, and the peace and quiet of the individual is disturbed for a period of greater or less duration. There is consequently abundant reason in support of the rule of law which makes the assault a legal wrong, even though no battery takes place. Indeed, in this case the law goes still further and makes the attempted blow a criminal offense also”).

7 Véase Eguiguren Praeli, Francisco, “La libertad de información y su relación con los derechos a la intimidad y al honor: el caso peruano”, *Libertad de expresión y democracia desde una perspectiva latinoamericana*, Fundación Konrad Adenauer, 2002.

las recientes tendencias hacia la generación compulsiva de bases de datos, concretamente las actividades de los burós de crédito, que aparecen como los mayores invasores de los datos personales, y al mismo tiempo son una necesidad a raíz de la ineficiencia judicial y de la incapacidad de recobrar deudas.

## II. FICHEROS PÚBLICOS Y PRIVADOS

Existen algunos perfiles que se presentan en la mayoría de los conflictos relacionados con los datos personales, estos son: cuando los registros públicos (gubernamentales) incluyen datos privados; Internet y el problema de determinar la ley aplicable y la jurisdicción competente; y, el creciente interés en acumular datos personales por parte de empresas comerciales —denominadas sociedades de información—. Todos éstos tienen en común la presencia de lagunas normativas y las dificultades de los poderes legislativos para generar normas de carácter general que resulten eficientes.

El tratamiento de la información judicial ofrece uno de los ejemplos más críticos por constituir documentos públicos que contienen datos personales —y en muchos casos— datos sensibles. En Brasil, probablemente el país en el que existe la mayor difusión en Internet de las decisiones judiciales, el artículo 93 (ix)<sup>8</sup> de la Constitución federal ha sido el fundamento para que los Poderes Judiciales estatales y federal hayan desarrollado el acceso en Internet a la jurisprudencia y a los estados procesales. Para analizar este punto, es necesario analizar que valor tiene la palabra “público” y, como en muchos otros campos del derecho, la irrupción de una nueva tecnología puede generar nuevos conflictos o lagunas.<sup>9</sup> Es natural que los constituyentes no imaginaran la existencia y el impacto de Internet, y por tanto es evidente que es un caso de laguna axiológica

8 “...todos os julgamentos dos órgãos do Poder Judiciário sero públicos, e fundamentadas todas as decisões, sob pena de nulidade, podendo a lei, se o interesse público o exigir, limitar a presença, em determinados atos, às próprias partes e a seus advogados, ou somente a estes”.

9 El uso del término “laguna” no es aquí del todo arbitrario: se estima que el legislador no ha tenido en cuenta la propiedad en cuestión *por no haberla previsto*, y que de haberla considerado, hubiera dado una solución diferente. En vez de solucionar el caso en forma genérica, le hubiera dado una solución específica. Es posible definir y distinguir el concepto de laguna axiológica (diferenciándola de la laguna normativa, por ejemplo inexistencia de solución) cuando la solución existente se considera axiológicamente inadecuada porque no toma en cuenta alguna propiedad conceptuada relevante, es decir, porque el sistema no hace un distinción que debe hacerse. Véase Alchourrón, Carlos E., y Bulygin, Eugenio, *Normative Systems*, Springer, 1971.

(presencia de una solución insatisfactoria) y no de laguna normativa (ausencia de una solución). En otros campos del derecho se ha observado que la generalización de Internet —o de otros avances tecnológicos— ha producido una “necesidad” de modificar el derecho, tomando en cuenta una circunstancia que no había sido —porque hasta aquel momento no pudo haber sido— tomada en cuenta por el legislador.

Quizás, para resolver este desacuerdo, sea suficiente aclarar cuál es sentido de la palabra *público* en el texto constitucional. Antes de Internet era común interpretar que los expedientes judiciales eran públicos, y significaba que cualquier persona podía solicitarlo en el juzgado, leerlo, y —salvo unas pocas excepciones legales— darlo a publicidad. Cabe entonces toda una gama de sentidos para la palabra o el carácter *público*: (a) puesto a disposición del público; *i.e.* incluidos en el derecho de acceso a la información; (b) dar a publicidad; *i.e.* forzar el conocimiento por parte de la mayor cantidad de personas posibles, o de determinadas personas. En este contexto resulta —por ejemplo— razonable que los jueces den a publicidad los edictos, cuya finalidad es notificar o crear la presunción de notificación.<sup>10</sup>

Hoy la condición de *público* se vincula a la necesidad de dejar determinado documento accesible a público con la finalidad de facilitar el control ciudadano de los actos de gobierno. Sin embargo la existencia de bases de datos en el ámbito del Estado llamadas por su ubicación *públicas* y bases de datos en manos de personas u organizaciones privadas o no estatales, denominadas, siguiendo el mismo criterio *privadas*, como afirma Cosentino, no necesariamente cambia la condición de los datos personales que puedan contener y no disminuye el nivel de protección que la Ley les asigna.<sup>11</sup>

Se enfoque como una laguna axiológica, un desacuerdo valorativo o como una cuestión semántica, resulta necesario redimensionar el carácter público de la información frente a las nuevas tecnologías; las nuevas finalidades; los riesgos y los conflictos de normas, y restaurar el equilibrio perdido.

10 Salzmann, Victoria S., “Are Public Records Really Public?: the Collision Between the Right to Privacy and the Release of Public Court Records Over the Internet”, *Baylor Law Review*, 52, 2000, pp. 355-379.

11 Cosentino, Guillermo, “La información judicial es pública pero contiene datos privados, cómo enfocar esta dualidad”, *Internet y sistema judicial en América Latina* (en prensa).

### III. EVOLUCIÓN DEL *RIGHT TO PRIVACY* EN LOS ESTADOS UNIDOS

En los Estados Unidos el derecho de privacidad fue acuñado por una serie de decisiones de la Corte Suprema de Justicia en las que se definía una zona de decisión personal en la que el Estado no podía intervenir. Los precedentes jurisprudenciales se refieren a hechos muy diversos.

En *Meyer vs. Nebraska*<sup>12</sup> y *Pierce vs. Society of Sisters*, la Corte Suprema de Estados Unidos declara inconstitucionales leyes estatales que iban demasiado lejos en el adoctrinamiento de niños. En *Meyer*, el Estado de Nebraska prohibía la enseñanza antes del noveno grado en otro lenguaje que no sea el inglés, el señor Meyer había sido condenado por enseñar relatos bíblicos en Alemán a sus estudiantes en una escuela parroquial luterana. Según la Ley de Nebraska sólo las lenguas modernas extranjeras habían sido prohibidas (latín, griego y hebreo estaban permitidas), el objetivo de esta Ley era formar buenos ciudadanos y prevenir a los niños de aprender “ideales y lenguas extranjeras” antes que la lengua y los ideales americanos. La Corte Suprema anula la sentencia en contra del señor Meyer y descalifica la prohibición sobre el lenguaje mostrando la analogía con la práctica que existía en Esparta de encerrar a los niños varones en barracas a la edad de siete años para adoctrinamiento estatal.

En *Pierce vs. Society of Sisters*<sup>13</sup> se ataca una ley que hacía obligatoria la enseñanza inicial en inglés; en *Skinner vs. Oklahoma*<sup>14</sup> se deja sin efecto una ley que establecía la esterilización de ciertos criminales. En *Griswold vs. Connecticut*<sup>15</sup> se ataca una ley en la que se prohibía el uso de anticonceptivos, en este caso es donde la Corte comienza a llamarlo “derecho de privacidad”. De aquí en adelante las principales sentencias de la Corte Suprema relacionadas con la intimidad, han estado vinculadas a temas de sexualidad y la preservación de su intimidad.

El concepto de privacidad transitó después situaciones mucho más controvertidas: *Cruzan vs. Director, Missouri Department of Health*<sup>16</sup> (rehusar tratamiento médico), *Roe vs. Wade*<sup>17</sup> (aborto), y *Washington vs. Glucksberg*<sup>18</sup> (suicidio asistido).

12 262 US 390 (1923).

13 268 US 510 (1925).

14 316 US 535 (1942).

15 381 US 479 (1965).

16 497 US 261 (1990).

17 410 US 113 (1973).

18 521 US 702 (1997).

La mayor peculiaridad de los casos judiciales en los Estados Unidos que construyeron el *privacy right* es que predominantemente se focalizaron sobre la sexualidad (en sentido amplio, o sea decisiones y conductas relacionadas con las condiciones bajo las cuales el sexo es permisible; las instituciones sociales alrededor de las relaciones sexuales; y las consecuencias procreativas del sexo).

Desde este punto de vista el pionero de la privacidad no es Brandeis, sino Sigmund Freud. En su visión, la sexualidad ocupa un estrato psicológico y biológico en la formación de la identidad y, al mismo tiempo, determina el límite interior del área estrictamente personal que el Estado no debe atravesar. Quizás el salto más interesante en la creación de motores de búsqueda fue también desarrollado por Freud, pues el psicoanálisis puede ser visto en realidad como un motor de búsqueda que permite indagar una parte de la memoria.

Para encontrar un factor común en estas decisiones es necesario preguntarse ¿de qué nos protege el *privacy right*? Muchos comentaristas dicen que está relacionado con la autonomía y que llamar a un individuo autónomo es otra forma de llamarlo moralmente libre, en la visión de Freud el individuo que se libera él mismo de la represión socio-sexual. Pero Michel Foucault en su trabajo *Historia de la sexualidad* plantea una hipótesis en la que define la relación entre sexo y poder en términos de represión, según la cual la sexualidad ha sido sistemáticamente reprimida por la sociedad, no permitiendo exteriorizar los verdaderos deseos sexuales, no actuar según ellos, y en consecuencia no conocerlos. Foucault niega que siempre la sociedad haya utilizado su poder para reprimir la sexualidad: la sociedad que emergió en el siglo XIX —burguesa, capitalista, o industrializada— dejó de preocuparse por regular la sexualidad. Foucault piensa que desde entonces la sexualidad no ocupa un *rôle* privilegiado —biológico o psicológico— en nuestra identidad. Toda esta elaboración y las decisiones de la Corte Suprema en la penumbra de la Constitución son vistas por Jed Rubenfeld concibiendo el *privacy right* como un conjunto de limitaciones a un Estado totalitario; en este sentido cita un caso de matrimonio interracial *Loving vs. Virginia*,<sup>19</sup> donde el tema de fondo no es —como el fallo aclara— si una persona tiene derecho a casarse con quien quiera, sino que se discute si el Estado tiene el derecho a intentar

19 388 US 1 (1967).

mantener la raza “pura”. También cita la opinión del juez Jackson en *West Virginia State Board of Education vs. Barnette*,<sup>20</sup> cuando, en medio de la Segunda Guerra Mundial, declara inconstitucional una ley que requería a los niños escolares saludar la bandera y profesar fidelidad a su país.<sup>21</sup>

La Corte Suprema en *Whalen vs. Roe* reconoce el conflicto entre el interés individual para impedir que se difundan datos personales y el interés en disponer de información para tomar cierto tipo de decisiones importantes.<sup>22</sup> En este caso se cuestiona una ley del Estado de Nueva York que creaba un registro centralizado y computarizado para mantener las prescripciones médicas con información completa que permitía identificar al paciente. La Corte estableció que el derecho a recolectar y usar tal información para propósitos públicos está acompañado por la obligación de impedir cualquier diseminación sin garantías.

Tradicionalmente, el derecho a la privacidad ha sido relacionado con la Decimocuarta Enmienda, y algunas decisiones judiciales le han colocado en una “penumbra” cercana a las Primera, Cuarta y Novena Enmiendas y finalmente el modelo americano de privacidad descansa sobre la fuerza de la ley y en la capacidad de la judicatura para limitar las acciones de un Estado que pudiera resultar invasor y totalitario. Esta construcción de la privacidad es una limitación sucesiva para impedir que leyes —dictadas dentro de los procedimientos constitucionales— terminen asignado al Estado poderes que no debe tener, pero nunca estas decisiones han enfrentado casos de terrorismo de Estado.

En Estados Unidos existe legislación federal para proteger la privacidad en sectores determinados: informes crediticios (*Fair Credit Reporting Act*, Public Law 91-508, modificada varias veces entre 1996 y 2001); archivos de televisión por cable (*Cable Communications Policy Act*, 47 USC 521-611, 1994); comunicaciones electrónicas (*Electronic Communications Privacy Act*, de 1986, 18 USC 2510-2520, 1994 & Supp. 1997); escucha de comunicaciones en una investigación criminal (*Omnibus Safe Streets and Crime Control Act* de 1967, 18 USC 2510-2520, 1968); registros de alquiler de videos (*Video Privacy Protection Act*, 18 USC 2710, 1994); registros telefónicos (*Telephone Consumer Privacy Act*, 47 USC 227, 1994); registros bancarios (*Bank Secrecy Act*, 31 USC

20 319 US 624 (1943).

21 Rubenfel, Jed, “The Right to Privacy”, *Harvard Law Review*, 102, 1989, pp. 737-807.

22 429 US 589 (1977).

5313, 1994); archivos de permisos de conducir (Drivers Privacy Protection Act, 18 USC 2721-25 1994); control parental de los niños en sus actividades en Internet (Children's Online Privacy Protection Act, 15 USCA 6501-6506, 1998). También existe legislación a nivel estatal, el problema es entonces el enfoque fragmentado que requiere una nueva legislación cada vez que aparece una nueva posibilidad tecnológica.

La *Privacy Act* de 1974 fue una de las primeras protecciones contra un uso inadecuado de los datos personales por parte del gobierno, pero su alcance es limitado, ya que sólo se aplica al procesamiento de datos por parte del gobierno federal, y no se aplica a los gobiernos estatales ni al sector privado. Si bien la Ley requiere el consentimiento previo por escrito para la cesión de los datos, existen varias excepciones, entre ellas la transmisión de datos a otra agencia del gobierno dentro del concepto de "uso rutinario".<sup>23</sup>

#### IV. PROTECCIÓN DE DATOS EN EUROPA

Las primeras formas de protección de la intimidad se encuentran en las prevenciones para evitar la inspección de personas y propiedades sin una autorización judicial. También existen normas penales dirigidas inicialmente a proteger la correspondencia. Estas normas fueron luego ampliadas a otras formas de comunicación. Un ejemplo son los artículos 13 y 14 (registro personal), 15 (secreto de la correspondencia y de cualquier otra forma de comunicación) de la Constitución italiana de 1947.

La Declaración Universal de los Derechos Humanos de 1948 ya recoge expresiones muy claras garantizando que: (artículo 12) "Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques". Inmediatamente en Europa la Convención para la Protección de los Derechos Humanos y Libertades Fundamentales de 1950 incluye estos derechos en los artículos 8 y 10.

En Alemania la historia no es tan lineal, pues el pasado del país hace a los alemanes especialmente sensibles con respecto a la información que puede ser manejada por la policía. En la década de los cuarenta los nazis pudieron ejercer el control de la población con los datos del censo y los

23 Privacy Act (1974) 5 USC 552a(b)(3).

archivos del gobierno, que fueron utilizados para identificar a los judíos y a otros grupos víctimas de genocidios. Estos hechos motivaron que el derecho de privacidad fuera incluido en la Constitución alemana de la posguerra y que luego las raíces de la teoría europea de protección de datos esté relacionada directamente con estas experiencias horribles ocurridas durante la Segunda Guerra Mundial.<sup>24</sup>

Aun así en 1970, la policía alemana fue pionera en el uso de perfiles computados para capturar a los miembros de la organización terrorista *Rote Armee Fraktion*. Pero esa forma de investigación generó muchas protestas y fue uno de los argumentos que llevó a Alemania a sancionar probablemente una de las leyes más duras del mundo en materia de protección de datos. La primera Ley de Protección de Datos (*Datenschutz*) fue sancionada el 7 de octubre de 1970 en el estado de Hesse. En 1977 el Parlamento Federal alemán aprueba la Ley Federal *Bundesdatenschutzgesetz* (BDSG). Estas leyes impiden, con muy pocas excepciones, a cualquier institución transmitir cualquier dato personal sin el consentimiento de la persona interesada.

Como una protección contra la intromisión del gobierno en la vida privada, la Ley alemana requiere que cualquier compañía con cinco o más empleados que haga algún tratamiento de datos personales, deberá designar una persona como responsable de la protección de datos. Los gobiernos federales y estatales deben designar también un *ombudsman* de protección de datos. Los Estados Unidos y los otros países de la Unión Europea no tienen una regulación comparable.

Otras naciones europeas comienzan luego a desarrollar Leyes sobre Protección de Datos que regulan tanto al sector público como privado, crean autoridades de vigilancia y le prohíben al gobierno y a particulares procesar datos personales sin consentimiento previo del interesado: entre ellas Suecia en 1973 y Francia en 1978. Otros hitos son también el proyecto de ley elaborado en el Reino Unido por Lord Mancroft en 1961 —donde el eje de la *privacy* se traslada de los Estados Unidos a Inglaterra— y enfoca los conflictos entre intimidad y los medios masivos de comunicación (*mass media*). En 1969 con el proyecto de ley de Brian Walden, aparece

24 Los artículos 1o. y 2o. de la Constitución de 1949 son el marco para el derecho a la vida privada (artículo 2o.). “Cada uno tendrá derecho al libre desenvolvimiento de su personalidad, en tanto no vulnere los derechos de otro y no atente al orden constitucional (*verfassungsmässige Ordnung*) o a la ley moral (*Sittengesetz*).” Los artículos 10 y 13 introducen garantías sobre el secreto de las comunicaciones, inviolabilidad del domicilio y de la persona (*Durchsuchungen*).

el problema de la tutela de los datos personales memorizados por ordenadores.

En Europa varios movimientos de protección de datos convergen hacia una directiva común ya en la Europa unificada. Una de las primeras normas en Europa son las que surgen del Convenio 108 del Consejo de Europa para la Protección de las Personas con Respecto al Tratamiento Automatizado de Datos de Carácter Personal, aprobado en Estrasburgo el 28 de Enero de 1981.

Después de 1990 la Unión Europea asumió la responsabilidad de la protección de datos por medio del Consejo de Europa para asegurar el adecuado funcionamiento de un mercado unificado, la protección uniforme de los datos personales fue considerada entonces una meta comercial necesaria para la consolidación de la Comunidad Económica Europea. Fundamentalmente se entendió que las diferencias entre las Leyes de Protección de Datos de los Estados miembros serían un obstáculo para el flujo interno de datos personales. Los dos Estados miembros con Leyes más fuertes, Francia y Alemania, estaban en condiciones de poner barreras a la transferencia de datos a otros Estados con Leyes más débiles como Italia. La política seguida por la Unión Europea fue evitar los inconvenientes de muchas Leyes nacionales de Protección de Datos Personales y lograr una norma común, la Directiva 95/46/CE,<sup>25</sup> transformando la información personal en una mercancía de alto valor. La estrategia para forzar Leyes de Protección más fuertes fue mantenida en la Directiva como la cláusula “de terceros países”.<sup>26</sup>

Ajustándose a la Directiva, los Estados miembros deben asegurar que los datos serán “tratados de manera leal y lícita” y sólo recogidos “con fines determinados, explícitos y legítimos”. Los datos deberán ser “adecuados, pertinentes y no excesivos con relación a los fines para los que se recaben” y “exactos”. Serán “conservados... durante un periodo no superior al necesario para los fines para los que fueron recogidos”. La Directi-

25 Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

26 El capítulo IV de la Directiva limita y regula la transferencia de datos a países terceros cuando “el país tercero de que se trate garantice un nivel de protección adecuado... El carácter adecuado del nivel de protección que ofrece un país tercero se evaluará atendiendo a todas las circunstancias...”. Ver, Kramer, Lynn Chuang, “Private Eyes are Watching You: Consumer Online Privacy Protection Lessons from Home and Abroad”, *Texas International Law Journal*, 37, 2002, pp. 387-419.

va también contienen protecciones tales como el “derecho de acceso del interesado a los datos”, derecho de oposición al tratamiento y a recurrir judicialmente en caso de violación de esos derechos (responsabilidad y sanciones). Merecen destacarse el concepto de “finalidad” que luego fue recogido por otras legislaciones no europeas, pues es el eje interpretativo de un tratamiento leal y lícito,<sup>27</sup> y la prohibición del tratamiento de datos sensibles, *i.e.* aquellos que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, así como los datos relativos a la salud o a la sexualidad.

El concepto de autodeterminación informativa aparece formalmente en Europa en la sentencia del Tribunal Constitucional alemán del 15 de diciembre de 1983 en relación con la Ley del Censo prohibiendo explícitamente al gobierno generar “un inventario de datos personales de los individuos por medio de censos gubernamentales de carácter confidencial”. Luego de esta decisión el derecho a la privacidad incluye el derecho a controlar la información sobre sí mismo y la capacidad para determinar si esa información puede ser recogida y cómo puede ser usada.

La tendencia actual supone el principio de uso mínimo de los datos personales y, consistente con la finalidad, con preferencia por la anonimización en la recolección y transferencia, cuando sea posible.

## V. LA PROTECCIÓN DE LOS DATOS PERSONALES EN AMÉRICA LATINA

En América Latina la protección de datos fue vista como una necesidad resultado de la explosión tecnológica, pero inevitablemente todos los procesos legislativos en la región han sufrido los avatares de una fuerte carga histórica y de la presión de los intereses económicos en la generación de bases de datos.

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 5o.- X, XII y LXXII; artículo 105 I b); Colombia (1991) artículo 15; Paraguay (1992) artículos 33, 36 y 135;

27 Entre ellas, algunas latinoamericanas y la Ley Relativa al Marco Jurídico de las Tecnologías de la Información (de Québec, Canadá), por ejemplo el artículo 24: “La utilización de funciones de investigación extensiva en un documento tecnológico que contiene informaciones personales y que, por una finalidad particular, se rinde público, debe ser restringida a esta finalidad”. Las Leyes de Transparencia de Michoacán y Sinaloa (México) obligan a hacer una definición explícita de la finalidad.

Perú (1993) artículos 2o., 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 los riesgos de la informática. Son el caso de la Constitución Política del Perú: “artículo 2o. 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 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”.<sup>28</sup>

Las Leyes Generales de Protección de Datos Personales tienen todas cierta semejanza con la legislación europea, existen en Argentina (2000), Chile (1999), Panamá (2002), Brasil (1997)<sup>29</sup> y Paraguay (2000). Otros países tienen muy avanzados sus proyectos de Ley de Datos Personales: Costa Rica, Colombia, Ecuador, México, Uruguay.

Algunos países han desarrollado leyes sectoriales: Venezuela (1991): Ley sobre Protección a la Privacidad de las Comunicaciones, Panamá (2002): Ley sobre el Servicio de Información sobre el Historial de Crédito; y, México (2002): Ley para Regular las Sociedades de Información Crediticia.

Sigue también una importante jurisprudencia, que fundamentalmente viene a llenar las imprecisiones o 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

<sup>28</sup> Cfr., 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”.

<sup>29</sup> Lei que Regula o Direito de Acesso a Informações e Disciplina o Rito Processual do Habeas Data.

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).

Varios países han sancionado Leyes de Transparencia y Acceso a la Información Gubernamental: Colombia (1985), Perú (2002), Panamá (2002) y México (2002).

## VI. LAS DIFERENCIAS MÁS VISIBLES ENTRE LAS POSTURAS

En términos generales la privacidad aparece en los Estados Unidos como un concepto más amplio que está relacionado con la libertad dentro de una esfera íntima. Su construcción es fundamentalmente jurisprudencial hasta que en 1974 comienzan a sancionarse algunas normas. El enfoque legislativo está relacionado con la presión y preocupación de los ciudadanos por los abusos y las exigencias del mercado. Por eso el enfoque es sectorial y fragmentado. También la construcción del *right to privacy* por parte de la judicatura se ha traducido en un proceso de auto-regulación.<sup>30</sup>

En Europa gravita singularmente la experiencia histórica de persecución asistida por la disponibilidad de datos personales, percepción que produce una conciencia pública a favor de la protección de datos. Cada país europeo en su medida buscó leyes de protección, pero el impacto comercial de las diferencias entre estas leyes es el que produce un proceso

30 Varias empresas y asociaciones han creado un grupo —la *Online Privacy Alliance*— para conducir el proceso de auto-regulación, crear un ambiente de confianza y promover la protección de la privacidad de los clientes específicamente en el comercio electrónico.

de homogenización que converge a una regulación unificada sobre la base del criterio más proteccionista.

Existen en la práctica algunas diferencias más sutiles. En la jurisprudencia de los Estados Unidos el derecho de privacidad esta destinado a proteger los sentimientos y la sensibilidad de las personas y no su propiedad, o intereses pecuniarios, por ello es que se sostiene que es un derecho personal que termina con la muerte.<sup>31</sup> Se ha observado, por ejemplo, que los registros penales de menores de edad —que están protegidos— pueden ser abiertos cuando una persona muere en circunstancias inexplicables y así permitir la investigación sobre las causas de su muerte.

Este punto de vista no es compartido en el sistema continental europeo donde la intimidad y privacidad están ligadas al honor.<sup>32</sup> Por ejemplo el artículo 185 del Código Penal portugués establece una pena por “ofender gravemente la memoria de una persona fallecida” y establece que “la ofensa no será punible cuando hayan transcurrido más de 50 años del fallecimiento”. En España la exposición de motivos de la Ley Orgánica de 5 de mayo 1982, de Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar, y a la Propia Imagen dice: “Aunque la muerte del sujeto de derecho extingue los derechos de la personalidad, la memoria de aquél constituye una prolongación de esta última que debe también ser tutelada por el Derecho”.<sup>33</sup>

Otro aspecto es que en la tradición continental no existe privacidad para las personas jurídicas (morales). Por ejemplo así ha sido declarado por el Tribunal Superior de Justicia de Venezuela en *In re P. H. S. e Inversora Bohemia*. El extremo de este principio puede verse en Trinidad y Tobago, en el caso *Collymore* y otro *vs. General Attorney* donde el Privacy Council sostiene que el derecho de privacidad se extiende a las sociedades de hecho, como por ejemplo, en este caso, un sindicato.<sup>34</sup>

En Estados Unidos existe la costumbre judicial de proteger a las partes que así lo soliciten por medio de pseudónimos. La concesión de esta pro-

31 Véase 62A American Jurisprudence 2d Privacy 25, además el derecho de privacidad es de carácter personal y la acción le cabe sólo a la persona ofendida, en *Nelson vs. Maine Times* (Me) 373 A2d 1221 se estableció que la privacidad de la madre no fue invadida por la publicación no autorizadas de la fotografía de su hijo. Una excepción en el *common law* sería la Sección 30 de la Freedom of Information Act de 1999 de Trinidad y Tobago y la Sección 27 de la Freedom of Information Act de 1994 de Belice en las que se protege la privacidad de las personas muertas.

32 Véase Cifuentes, Santos, “La intimidad y el honor de los vivos y de los muertos”, *El Derecho*, 162, 1994, pp. 404-408.

33 Véanse artículos 4o. y 6o. de la Ley.

34 12 WIR 5 y 15 WIR 229.

tección fue inicialmente limitada casi exclusivamente a aquellos casos involucrando menores, divorcios, custodia de un hijo, manutención de los hijos o paternidad, pero en los últimos años se ha aplicado también a personas morales: en *United States vs. Microsoft Corp.*,<sup>35</sup> se permitió a tres compañías participar como *amici curiae* en forma anónima como *Doe Companies* y al Federal Bureau of Investigation (F.B.I.) como *John Doe Government Agency*, en *John Doe Agency et al. vs. John Doe Corp.*<sup>36</sup>

Según la jurisprudencia de los Estados Unidos, es posible perder en parte el derecho de privacidad. Para ello se han establecido las categorías de personas voluntariamente públicas y las involuntariamente públicas. Estos conceptos permiten trazar dos categorías de personas: (a) las “personas voluntariamente públicas” son aquellas que se han ubicado o expuesto ante la mirada del público por sus actividad o asumiendo un *rôle* prominente en instituciones o actividades de interés para el público en general. Han sido consideradas personas públicas los actores,<sup>37</sup> atletas profesionales,<sup>38</sup> políticos,<sup>39</sup> músicos, intérpretes y animadores.<sup>40</sup> Se interpreta que el público posee un interés legítimo en obtener información sobre personas voluntariamente públicas, esta información puede llegar ser tan amplia que incluiría aspectos que para otras personas serían privados. (b) En contraste las “personas involuntariamente públicas” son aquellas que no han buscado la atención del público, pero que han sido *noticia* como resultado de su participación o asociación con algún hecho notorio. Esta categoría incluye —por ejemplo— víctimas de delitos o accidentes, per-

35 56 F3d 1448 (1995).

36 493 US 146 (1989). Ver Milani, Adam A., “Doe vs. Roe: an Argument for Defendant Anonymity when a Pseudonymous Plaintiff Alleges a Stigmatizing Intentional Tort”, *Wayne Law Review*, 41, 1995, pp. 1659-712. Un aspecto similar es la protección de secretos comerciales; en México la Ley Federal de Transparencia y Acceso a la Información Pública incluye (artículo 14.) “También se considerará como información reservada:... II. Los secretos comercial, industrial, fiscal, bancario, fiduciario u otro considerado como tal por una disposición legal...”. También en Estados Unidos la Ley de Libertad de Información (FOIA) establece (Sección 552): “Información pública... (a) Toda división del gobierno deberá poner a disposición del público su información del modo que se estipula a continuación:... (b) La presente Sección no se aplicará a cuestiones que fuesen o estuviesen:... (4) secretos comerciales e información comercial o financiera obtenida de una persona que se considera información privilegiada y confidencial;”. En Europa la Directiva 95 protege sólo a las personas físicas aun cuando las Leyes de Austria, Dinamarca, Italia y Luxemburgo han extendido la protección a las personas morales.

37 O’Hilderbrandt vs. Columbia Broad. Sys., 114 Cal. Rptr. 826, 830 (Cal. Ct. App. 1974).

38 Cepeda vs. Cowles Magazines and Broad., 392 F.2d 417, 419 (9th Cir. 1968).

39 Miller vs. Bakersfield News-Bulletin, 119 Cal. Rptr. 92, 94 (Cal. Ct. App. 1975); Yorty vs. Chandler, 91 Cal. Rptr. 709, 712 (Cal. Ct. App. 1970).

40 Star Editorial vs. United States District Court, 7 F.3d 856, 861 (9th Cir. 1993); Montandon vs. Triangle Publications, 120 Cal. Rptr. 186, 191 (Cal. Ct. App. 1975).

sonas procesadas por delitos o personas que han realizado actos heroicos. Una persona puede tornarse involuntariamente pública —y por tanto perder parte de su privacidad— simplemente por el hecho de estar relacionada con una persona voluntariamente pública.<sup>41</sup> Un caso relevante en la definición de esta categoría es *Kapellas vs. Kofman*.<sup>42</sup> En este caso un periódico publicó un editorial criticando a Ines Kapellas, una candidata a un cargo electivo, el artículo se refería a que su hijo había sido arrestado y que su hija fue encontrada varias veces vagando por las calles. La Corte Suprema de California sostuvo que los niños habían perdido su privacidad como resultado de la candidatura de su madre. También los tribunales han sostenido que quienes han perdido su privacidad nunca podrán recuperarla.<sup>43</sup>

La tradición europea y latinoamericana sólo considera a la personas voluntariamente públicas y que éstas pierden su privacidad solamente en relación con la razón de su notoriedad y mediando una manifestación clara de renuncia a un área determinada de su intimidad. Las legislaciones latinoamericanas también parecen ser más restrictivas con el concepto de personas involuntariamente públicas. En Trinidad y Tobago se denominan “personas en la vida pública” según la *Integrity in Public Life Act* (2000) sección 2 y tabla final, pero se trata de una enumeración de funcionarios públicos muy restrictiva.

Mientras en Europa se persigue la defensa de la persona a través de normas generales y uniformes que especifiquen los límites del Estado y de los particulares para el tratamiento de los datos; en Estados Unidos no hay políticas constitucionales sobre el tema, sólo existen algunas normas sectoriales, y se prefiere la revisión judicial de aquellos actos que agreden eventualmente el derecho a la privacidad, y que esta revisión opere como un incentivo para la autoregulación.

## VII. RIESGOS ACTUALES PARA LOS DATOS PERSONALES

Por tratarse de datos está implícito un proceso de almacenamiento y comunicación, un emisor y un receptor. De aquí surge la pregunta ¿hasta

41 Así fue definido en *Carlisle vs. Fawcett Publications, Inc.*, 20 Cal. Rptr. 405, 414 (Cal. Ct. App. 1962).

42 459 P.2d 912 (Cal. 1969).

43 En *Sidís vs. F-R Publishing Corp.*, 113 F.2d. 806 (2d Cir. 1940), el reclamante era un niño prodigio que ganó notoriedad al graduarse en la universidad a los 17 años. Veinte años más tarde, una revista publicó un artículo contrastando sus logros con su vida actual. El tribunal sostuvo que el artículo no violó su privacidad porque él seguía siendo una figura pública.

dónde una persona puede controlar la comunicación de su información privada e historia personal? y por el contrario ¿hasta dónde y cómo puede limitarse un proceso de búsqueda de información? Tomando como paradigma del *privacy right* la sexualidad, se podría equiparar como privado cualquier otro aspecto que socialmente no sea admisible de ser observado. Pero toda persona está permanentemente comunicando datos de su vida privada, en algunos casos puede controlar esa comunicación y evitar que otros reciban esos datos, pero el proceso tiene sus límites (en este sentido no parece útil el paradigma de la “sexualidad entre cuatro paredes”).<sup>44</sup>

Un ejemplo interesante se puede establecer con el nombre y apellido de las personas. El sólo nombre esta informando sobre el sexo y sobre cierta inserción lingüística. Resulta además que 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 transcripción de los Registros Civiles estarían mostrando además datos migratorios. También si un apellido es frecuente o raro estaría marcando una vulnerabilidad diferencial para los procesos de búsqueda e identificación, pues una forma de conservar la intimidad es también caer dentro de la saturación de una búsqueda.<sup>45</sup> Así las leyes que restringen o facilitan los cambios de nombres o apellidos pueden limitar o facilitar la intimidad.<sup>46</sup> La tendencia europea y latinoamericana es a restringir el cambio de apellidos, mientras que en los Estados Unidos puede ser un procedimiento sencillo.

44 En *Vernonia School District 47J vs. Wayne Acton et ux.*, US (1995) la Suprema Corte de Estados Unidos afirma que los atletas tienen una menor expectativa de privacidad —entre otros argumentos— por la “desnudez” en la desarrollan su actividad, porque en los vestuarios es común que no existan cortinas entre las duchas, y los escusados no tienen puertas.

45 Por ejemplo, una búsqueda por los nombres “Juan Pérez” produciría tantos resultados que haría prácticamente imposible cualquier proceso de identificación, por el contrario nombres originales o apellidos raros no pasarían inadvertidos. También los apellidos que tienen significado en un lenguaje nacional son menos vulnerables que aquellos que no son palabras de uso corriente.

46 En Chile la Ley 17.344 permite el cambio de nombre y apellido una sola vez en la vida justificando menoscabo moral o uso continuado de otro nombre. Contrariamente otras legislaciones, en la Argentina por ejemplo, es muchísimo más restrictiva y en muy pocos casos es autorizado un cambio de nombre o apellido. Si bien en Chile la reforma legislativa se fundamentó en el derecho de las personas de reflejar en sus apellidos su pertenencia étnica, los resultados prácticos fueron que muchos mapuches cambiaron sus apellidos por apellidos españoles aduciendo que sus apellidos originales eran motivo de discriminación, ver: Millaray Llanquileo Romero, María Cristina, “Un análisis de los cambios de nombres en sujetos mapuches, 1970 a 1990”, *Revista Proposiciones*, Santiago de Chile, 27, 1996, pp. 148-160.

Hoy se considera incluido en la libertad de expresión el acceso a la información gubernamental. No existe una solución de carácter general para balancear libertad de expresión con derechos de intimidad y privacidad. Pero no es ésta la principal fuente de problemas sino la creciente tendencia a generar bases de datos.

Las más generalizadas son los burós de crédito, que son utilizadas para determinar si una persona ha fallado en el pasado en algún pago. El segundo gran conflicto es con los registros públicos (entendido como aquellos que se generan en alguna institución pública) que contienen datos personales y particularmente aquellos que contienen datos sensibles. Entre estos los más delicados son los registros judiciales, ya que contienen información personal relacionada con conflictos entre personas que son confiados al sistema de administración de justicia para obtener una solución. En algunos países el expediente judicial es público, en otros es reservado, pero no existe duda que una sentencia judicial que ha causado estado es un documento público. Sin embargo la difusión indiscriminada de sentencias judiciales y la capacidad de un motor de búsqueda en Internet pueden llegar a un nivel de exposición de los datos personales desproporcionado con la finalidad de difundir la jurisprudencia.

### 1. Información judicial: Reglas de Heredia

En los Estados Unidos la regla general es el acceso y la publicidad, sin embargo existen reglas que restringen o prohíben el acceso a la información judicial. La reserva es absoluta en asuntos de adopción, custodia, patria potestad, salud mental y reproductiva. Complementariamente existen reglas para restringir el acceso a algunas partes del expediente, que operan a instancia de parte o de oficio.<sup>47</sup> También las partes pueden solicitar al juez litigar bajo pseudónimo, situación que en los últimos años ha generado un creciente número de casos judiciales en los que se autoriza el uso de pseudónimos.<sup>48</sup>

47 Véase Juan Luis González Alcántara, “Transparencia y acceso a la información judicial”, *Reforma Judicial. Revista Mexicana de Justicia* 2, 2003, pp. 67-82. Recientemente se ha regresado a la práctica de los expedientes duplicados en casos sobre drogas o terrorismo (llamados *dual dockets*, uno secreto y otro para el público y la prensa) que había sido declarada inconstitucional dentro de la Primera Enmienda en *US vs. Valenti*, 987 F 2d 708, 713 (11th Cir. 1993), véase Dan Christensen, “Federal Court in Florida hides Cases From Public”, *Miami Daily Business Review*, 12 de mayo de 2003.

48 Véase Milani, *supra*, nota 36.

Recientemente se han propuesto algunas soluciones para la difusión de información judicial; en Francia la Recomendación 01-057 del 29 de noviembre de 2001 de la Comisión Nacional Informática y Libertades:

(1) Los editores de bases de datos de decisiones judiciales, libremente accesibles en sitios de Internet, se abstengan de hacer figurar los nombres y los domicilios de las partes y de los testigos.

(2) Los editores de bases de datos de decisiones judiciales accesibles en Internet, mediando pago en concepto de abono, se abstengan de hacer figurar los domicilios de las partes y de los testigos.

En Italia el *Codice in Materia di Protezione dei Dati Personali* incluye entre las categorías de datos especiales los datos judiciales (artículo 21) y el título I de la segunda Parte regula específicamente el tratamiento de datos en el ámbito judicial.<sup>49</sup> En Canadá, en todas las provincias existe legislación que asegura el acceso público a documentos e información en manos del gobierno y, al mismo tiempo, leyes que protegen ciertos derechos de privacidad; pero el Canadian Judicial Council ha concluido que en términos generales el derecho de acceso tiene mayor peso que el derecho de intimidad.<sup>50</sup>

En México, y como consecuencia de la aprobación de las Leyes estatales y federal de Acceso a la Información Pública la Ley Federal establece que (artículo 8o.) “El Poder Judicial de la Federación deberá hacer públicas las sentencias que hayan causado estado o ejecutoria, las partes podrán oponerse a la publicación de sus datos personales” y (Artículo 14) “se considerará como información reservada:... IV. Los expedientes judiciales o de los procedimientos administrativos seguidos en forma de juicio en tanto no hayan causado estado”.

Los tribunales han visto la necesidad de definir algunos criterios, por ejemplo, en el Acuerdo del Pleno de la Suprema Corte de Justicia de México 9/2003 del 27 de mayo de 2003 se dice (artículo 42) “los expedientes relativos a los asuntos de naturaleza penal o familiar constituyen información reservada, por lo que en los medios en que se hagan públicas las sentencias respectivas se deberán suprimir los datos personales de las partes” y el Acuerdo del Supremo Tribunal de Justicia de Sinaloa (México, del 8 de marzo de 2003) “Se clasifica como reservada la información

49 El Código fue aprobado el 30 de junio de 2003 y entrará en vigor el 1 de enero de 2004 sustituyendo a la Ley 675/1996.

50 Véase “Judges Technology Advisory Committee for the Canadian Judicial Council”, *Open Courts, Electronic Access to Court Records, and Privacy*, 2003, 55 pp.

contenida en los expedientes de procesos jurisdiccionales... hasta en tanto no causen legalmente estado” y “la información contenida en expedientes de procesos jurisdiccionales de divorcio, alimentos, paternidad, filiación, adopción, tutela de menores y violencia familiar, aun cuando hayan causado o causen, legalmente estado”.

Existen muy pocas normas que regulen específicamente el equilibrio entre acceso a la información (difusión de la jurisprudencia) y protección de datos personales. El concepto que parece clave en este proceso es el de “finalidad” que se encuentra definido en la normativa europea. Este parece ser el eje de las *Reglas Mínimas para la Difusión de Información Judicial en Internet* (Reglas de Heredia) aprobadas en 2003.<sup>51</sup> La primera consecuencia que se puede deducir de la aprobación de las Reglas de Heredia es que sus redactores han puesto en el mismo plano los derechos de intimidad y privacidad que los derechos de acceso a la información pública. Este punto marca una diferencia con las soluciones dadas en otras regiones. Podría decirse, a grandes rasgos, que la tradición en los Estados Unidos es a dar cierta preferencia al derecho de acceso a la información pública (situación bastante evidente por la forma en que se difunde la jurisprudencia por parte de empresas comerciales y la forma en que organizaciones de la sociedad civil y empresas comerciales pueden obtener bases de datos judiciales completas).<sup>52</sup> En Europa —por el contrario— parece que existe una preferencia por la protección de datos personales, esta situación es clara en la Recomendación 01-057 del 29 de noviembre de 2001 de la Comisión Nacional de la Informática y de las Libertades de Francia.

Las Reglas de Heredia parecen ser el primer instrumento que ha propuesto una definición de finalidad de la acumulación y diseminación de la información judicial. Quizás el único precedente es la Recomendación núm. R(95)11 del Comité de Ministros de la Unión Europea. En México

51 Recomendaciones aprobadas durante el seminario *Internet y Sistema Judicial* realizado en la ciudad de Heredia (Costa Rica), los días 8 y 9 de julio de 2003 con la participación de Poderes Judiciales, organizaciones de la sociedad civil y académicos de Argentina, Brasil, Canadá, Colombia, Costa Rica, Ecuador, El Salvador, México, República Dominicana y Uruguay.

52 La práctica en los Estados Unidos es que las partes pueden solicitar litigar bajo pseudónimo para proteger su identidad durante el proceso y en la difusión de la sentencia. Esta posibilidad debe solicitarse y fundamentarse, y el juez debe decidir si la autoriza o no. Varios autores han señalado que el número de casos en los que alguna de las partes litiga bajo pseudónimo se ha incrementado en los últimos tiempos. Ver Steinman, Joan, “Public Trial, Pseudonymous Parties: when Should Litigants be Permitted to keep their Identities Confidential?”, *Hastings Law Journal*, 37, 1985, pp. 1-89; y Milani, Adam A., *op. cit.*, nota 36.

las Leyes de Transparencia de Michoacán y Sinaloa (México) obligan a definir la finalidad, pero aún ninguno de estos tribunales ha realizado tal definición. La finalidad así definida (Reglas 1 y 2) está siempre orientada hacia la administración de justicia, incluyendo la transparencia en la medida que contribuye a mejorar el desempeño judicial. Para definir la finalidad utiliza tres categorías: sentencias, información procesal y edictos, para estos últimos se sobreentiende que la publicidad es máxima y sólo se espera que los jueces se limiten a revelar en su texto la información estrictamente necesaria.

La definición dada para la categoría de personas voluntariamente públicas se relaciona directamente con el punto 10 de la Declaración de Principios sobre Libertad de Expresión, de la Comisión Interamericana de Derechos Humanos de la O.E.A. y con algunos códigos de ética periodística.<sup>53</sup> También parece alejarse de la jurisprudencia de California, que considera también que las personas involuntariamente públicas pierden parte de su privacidad.<sup>54</sup>

La adecuación de los motores de búsqueda a la finalidad (Regla 4) tiene un antecedente en la Ley Relativa al Marco Jurídico de las Tecnologías de la Información (de Québec, Canadá), el artículo 24 dice: “La utilización de funciones de investigación extensiva en un documento tecnológico que contiene informaciones personales y que, por una finalidad particular, se rinde público, debe ser restringida a esta finalidad.”

Sin embargo indirectamente la Regla de Heredia número 8 impediría una difusión indiscriminada de los datos personales de acusados o condenados por delitos, en la medida que —a partir de esa difusión— cualquier particular podría construir bases de datos de antecedentes penales. La difusión del inicio de casos penales (por ejemplo los sorteos de juzgados) parece ser la que representa mayor vulnerabilidad por dos razones: (a) las estadísticas señalan que gran parte de las acciones penales concluyen sin sentencia definitiva; y, (b) que difundir acciones penales obligaría a difundir luego la decisión judicial que da por terminado el caso (sea una

53 Véanse, por ejemplo, las decisiones del Consejo de Ética de los Medios de Comunicación de Chile ([www.anp.cl/site/pags/consejo/index.html](http://www.anp.cl/site/pags/consejo/index.html)). Este Consejo es un mecanismo de autorregulación ética emanada de los propios medios de comunicación. Su misión es promover la ética periodística en el ámbito de la información y representar, dentro de sus atribuciones, las infracciones que contra ella se cometan.

54 Véase Gary Williams, “On the QT and Very Hush Hush: a Proposal to Extend California’s Constitutional Right to Privacy to Protect Public Figures from Publication of Confidential Personal Information”, *Loyola of Los Angeles Entertainment Law Journal*, 19, 1999, pp. 337-361.

absolución, condena, sobreseimiento, o archivo), si no fuera así se estaría difundiendo información incompleta y no se ofrecería a los imputados la posibilidad de establecer con el mismo nivel de publicidad que la acción no prosperó (situación en la que se violaría la presunción de inocencia).

## 2. *Generación de nuevos registros públicos y privados (sociedades de información)*

Aparte de los Registros Civiles y de capacidad de las personas y los de propiedad, existen otros registros públicos en casi todos los países como los registros de antecedentes penales y carcelarios. También las escuelas y hospitales tienden a llevar registros con datos personales. En los últimos años se han aprobado leyes que crean nuevas bases de datos personales, algunos ejemplos son:

- Ley de Creación del Registro Nacional de Donantes de Células Progenitoras Hematopoyéticas, (Ley 25.392 de Argentina);
- Ley 6.879 de la Provincia de Mendoza (Argentina) sobre el Registro de Deudores Alimentarios Morosos;
- Ley Reformatoria a la Ley de Discapacidades de Ecuador (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);
- Proyecto de Ley en Uruguay por el que se crea un padrón especial para la inscripción cívica de aquellas personas con discapacidades físicas que así lo requieran;
- Ley de Transfusión y Bancos de Sangre (artículo 44) de Venezuela;
- DNA Identification Act (sections 39 & 40) de Trinidad y Tobago;

Los sistemas de registro de antecedentes crediticios (burós o *bureaux* de crédito),<sup>55</sup> han desarrollado un mecanismo de acceso al crédito (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

55 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.

del comercio obviando las garantías personales. 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.<sup>56</sup>

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. También vulneran el derecho de defensa, pues la inclusión de una persona en una base de datos como mal pagador se realiza sin mediar una notificación al interesado.

En varios países de la región se han intentado proyectos legislativos que regularan esta actividad. Los ejemplos de Argentina y Brasil son los más significativos. Luego de los debates parlamentarios se incluyeron algunas normas en las Leyes de Datos Personales y *habeas data*, las que resultan insuficientes para regular la actividad a la luz de los conflictos observados en la jurisprudencia. Aprovechando este vacío legal las empresas de riesgo crediticio ocuparon un importante lugar en el mercado, que fue seguido por una creciente litigiosidad.

Recientemente se han sancionado leyes para esta actividad en forma específica: Paraguay (diciembre de 2000),<sup>57</sup> México (enero de 2002), Panamá (mayo de 2002),<sup>58</sup> Chile (junio de 2002),<sup>59</sup> y en Argentina y Brasil se encuentran tangencialmente reguladas dentro de las Leyes de Protección de Datos Personales.

Uno de los problemas más delicados de estos sistemas de información es su incidencia en el acceso al empleo. Durante el último año la Sala Constitucional de la Corte Suprema de Costa Rica ha recibido varias demandas laborales vinculadas con esta actividad en las que 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 no es informado sobre el pedido de informes y puede ser discriminado sin percibirlo. El tema es aun más crítico cuando se discrimina a un candidato a un empleo por haber realizado en el pasado ac-

56 Villar, Rafael del, Díaz de León, Alejandro y Gil Hubert, Johanna, *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.

57 [www.ulpiano.com/habeasdaata\\_paraguay\\_Ley.htm](http://www.ulpiano.com/habeasdaata_paraguay_Ley.htm)

58 [www.condusef.gob.mx/informacion\\_sobre/buro\\_credito/leyregularlassociedades.htm](http://www.condusef.gob.mx/informacion_sobre/buro_credito/leyregularlassociedades.htm)

59 <http://lac.derechos.apc.org/legislacion/completo.shtml?x=8540>

ciones laborales contra su empleador (esto es posible por la disponibilidad en Internet de los juicios laborales iniciados).<sup>60</sup>

Un punto a regular es cómo las empresas de historial crediticio generan sus bases de datos. Hace algunos años estas empresas eran muy pequeñas e incipientes, por eso tenían por costumbre obtener bases de datos de organismos públicos y privados en forma irregular. Hoy la mayoría de ellas han sido adquiridas por empresas multinacionales, situación que ha generado alguna transparencia sobre el contenido de las bases de datos y la forma en que los datos son obtenidos. La dificultad reside en que el organismo de control debe cerciorarse que los datos 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.

### 3. Libertad de expresión en Internet

Colocar información en Internet es “difusión indiscriminada” (siguiendo la terminología europea) y además con una persistencia que no podría cumplir con el requisito europeo de “caducidad del dato”. Simultáneamente Internet es la más grande expectativa para garantizar la libertad de expresión de las minorías, pues facilita la más amplia difusión a costos insignificantes. El vacío legislativo existente sobre la cuantía de las penas civiles (limitadas a la indemnización del daño moral) frente a los abusos de la libertad de expresión y la imposibilidad de borrar definitivamente cualquier información que alguna vez fue colocada en Internet, configuran un conflicto difícil de resolver.

Las nuevas tecnologías de información y comunicación son un catalizador preponderante para la vigencia de ciertos derechos, como la libertad de expresión. Para preservar esta expectativa la Comisión Interamericana de Derechos Humanos reiteró el principio en la *Declaración de Principios sobre Libertad de Expresión*.<sup>61</sup>

60 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 Lobato de Paiva, Mário Antônio, *A difusão de informações judiciais na Internet e seus efeitos na esfera trabalhista*.

61 [www.cidh.oas.org/relatoria/spanish/Declaracion.htm](http://www.cidh.oas.org/relatoria/spanish/Declaracion.htm)

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 maniobra negligencia en la búsqueda de la verdad o falsedad de las mismas.

Aun así, parece cada vez más necesario generar un marco regulatorio adecuado y eficaz para evitar que estos avances se transformen en riesgos o violaciones para otros derechos. En América Latina, los sistemas de responsabilidad civil —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.<sup>62</sup>

## VIII. CONCLUSIÓN

Los usos más cuestionables de las bases de datos personales (antecedentes crediticios, laborales, arrendamientos) se relacionan con el prejuicio de que alguien, que actuó en el pasado de alguna forma, volverá a actuar de esa forma en el futuro; ya sea si no pago una deuda, no pago un arrendamiento, accionó judicialmente contra su empleador por un conflicto laboral, o si fue víctima, testigo, o autor de un delito. En todo estos casos se supone “cierto riesgo” y las decisiones apuntan a discriminar a estas personas.

Paradójicamente la prevención europea, más fuerte al momento de proteger los datos personales, se funda en una experiencia también histórica. Se estima que si en el pasado los regímenes autoritarios utilizaron las bases de datos para perseguir y exterminar personas por su pertenencia étnica o su forma de pensar, no existe ninguna garantía de que esto no ocurrirá en el futuro. Por esta razón se pretende una solución de raíz: evitar que existan tales bases de datos, particularmente en manos del Estado.

62 Véase *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/legislacion.shtml?x=9471>).

Frente a la polaridad manifiesta entre Estados Unidos y Europa, probablemente el enfoque de protección de datos personales que mejor se ajusta a la realidad latinoamericana, aun muy frágil en sus instituciones democráticas, es la experiencia europea. El conflicto radica en que una protección así, parece insostenible con las demandas de desarrollo económico; puesto que las economías latinoamericanas necesitar agilizar el comercio con un acceso dinámico al crédito —sólo posible con la generalización de los sistemas de riesgo crediticio— y los exiguos presupuestos de los Estados no están en condiciones de soportar los costos de los procesos de anonimización o encriptación de la información estatal ni de sostener sistemas eficaces de control estatal de la bases de datos en manos privadas.

En concordancia con el enfoque de los Estados Unidos las Leyes de Acceso a la Información Pública Gubernamental son un instrumento para el control ciudadano de la administración pública que eventualmente puede prevalecer frente al interés por la privacidad. En América Latina también resulta difícil compatibilizar los niveles europeos de protección de datos personales con la necesidad de combatir la corrupción de los funcionarios estatales facilitando el acceso público a la información gubernamental.

Probablemente sea un error pensar que hoy la protección de datos personales es sólo una cuestión de derechos fundamentales. Para América Latina y otros países puede tener implicaciones comerciales, ya que no les resulta conveniente quedar fuera del área de transmisión segura de datos, incluyendo éstos los del comercio electrónico. En este sentido, la reciente certificación que la Unión Europea ha otorgado a la Argentina como país cuya legislación es adecuada dentro de la Directiva 95/46/CE marca una ventaja comercial significativa, consecuencia de la una legislación orientada hacia la tradición europea.<sup>63</sup> En los próximos años será posible ver cuáles son los criterios e intereses que prevalecen.

63 Argentina es el primer país de América Latina que recibe esa certificación (Decisión 2003/490/CE del 30 de junio de 2003), que también ha sido conferida a Suiza, Hungría y a la Bailía de Guernsey. El principio de *safe harbor* es aplicado a los Estados Unidos y Canadá.