Internet y sociedad en América Latina y el Caribe, investigaciones para sustentar el diálogo

Marcelo Bonilla, Gilles Cliche, editores

Internet y sociedad en América Latina y el Caribe, investigaciones para sustentar el diálogo

FLACSO
SEDE ACADÉMICA DE ECUADOR

IDRC CRDI

Páez N19-26 y Patria, Quito – Ecuador
Telf.: (593-2-) 2232030
Fax: (593-2) 2566139

ISBN: 9978-67-065-3
Editores: Marcelo Bonilla y Gilles Cliche
Coordinación editorial: Alicia Torres
Cuidado de la edición: Jesús Pérez de Ciriza
Diseño de portada y páginas interiores: Antonio Mena
Imprenta: RISPERGRAF
Quito, Ecuador, 2001

Índice

Impacto social del Internet en el espacio local

Internet, derecho y sociedad

Políticas públicas para el Internet a inicios del tercer milenio

Internet, derecho y sociedad

Impacto de las nuevas tecnologías de comunicación e información sobre los derechos de intimidad y privacidad

Carlos G. Gregorio, Silvana Greco y Javier Baliosian* [1]

Introducción

Los crecientes niveles de informatización al servicio de los órganos del Estado y al servicio de particulares, así como el incremento exponencial en el acceso a determinadas fuentes de información que se observa a través de Internet, suponen la aparición de situaciones que hasta hace unos años eran impensables. En algunos casos, estas aplicaciones pueden ser aprovechadas por determinados sectores amenazando algunos derechos fundamentales. Por su parte, los sistemas normativos –tanto los instrumentos internacionales como las legislaciones nacionales– corren el riesgo de no dar soluciones, envejecer rápidamente y, en consecuencia, producir peligrosas lagunas normativas.

También se han desarrollado nuevos conceptos sobre la información, de esta forma tanto su contenido como su accesibilidad son utilizados como un instrumento para reforzar la eficacia de políticas públicas, o garantizar intereses de particulares.

Este proceso es tan vertiginoso que los modelos normativos clásicos no parecen surtir resultado; siendo, por otra parte, muy limitado el acceso a la justicia en casos de violación de la privacidad; esto se traduce en una juris-

* Instituto de Investigación para la Justicia. Buenos Aires, Argentina

1. También ha participado en la investigación previa y en la elaboración de este documento Camille Sutton. Los autores agradecen a las siguientes personas por su participación en la revisión del documento y por haber aportado estudios de país: Nuria Castañer, Francina Díaz, Elena Highton y Nelson A. Vaquerano.

Gregorio, Carlos; Greco, Silvana; Baliosian, Javier (2001). **Impacto de las nuevas tecnologías de comunicación e información sobre los derechos de intimidad y privacidad.** En *Internet y sociedad en América Latina y el Caribe, investigaciones para sustentar el diálogo,* ed. Marcelo Bonilla y Guilles Cliche, 375-444. Quito: Serie Foro FLACSO.

prudencia (de hecho una forma de establecer normas más dinámica que la legislativa) muy limitada.

Tanto en Internet como en los sistemas de información del Estado o de particulares, el aumento de la vulnerabilidad de los derechos de intimidad y privacidad se debe a la capacidad creciente de los motores de búsqueda que se suma a la también creciente capacidad de almacenamiento[2]. Como contrapartida los sistemas de información no tienen límites exactos, sino difusos, dados por la conectividad o la interacción entre datos. Ni siquiera se limitan a datos almacenados electrónicamente.

En esta investigación se intenta evaluar el impacto de las Tecnologías de Información y Comunicación (TIC), en particular de los bancos de datos personales sobre los derechos de privacidad e intimidad, para desarrollar mecanismos –legales, judiciales y técnicos– de protección. Se intenta además desarrollar paradigmas de sistemas de información capaces de satisfacer las necesidades para las que fueron creados (principio de finalidad) sin que puedan convertirse en amenazas a la privacidad e intimidad.

Para ello se ha seleccionado un grupo de países *viz:* Argentina, Brasil, Costa Rica, Chile, Jamaica, Ecuador, México, República Dominicana, Trinidad y Tobago, Venezuela y Uruguay, en los que se ha buscado identificar situaciones, legislación y jurisprudencia, si bien no en forma exhaustiva, sí con la finalidad de que el conjunto total de información brinde una clara apreciación de las violaciones y de las formas de garantizar los derechos[3].

---

2 Este proceso puede ser visto como un nuevo salto cualitativo en la ampliación de la memoria humana. Durante siglos los seres humanos necesitaron ampliar y proteger su memoria. Desde las pinturas rupestres, los íconos, 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' pudieron 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 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 significan una ampliación de la memoria. Quizás el salto más interesante en la creación de motores de búsqueda fue el desarrollado por Sigmund Freud. El psicoanálisis puede ser visto en realidad como un motor de búsqueda que le permite al hombre indagar sobre su propia memoria. Son los motores de búsqueda los que transforman el concepto de memoria y los que realmente han cambiado la vulnerabilidad de las personas.

3 También se analizaron algunas situaciones en Canadá, España, EE. UU., Francia y en otros países de América, como El Salvador y Bahamas.

El derecho a la privacidad, intimidad y a los datos personales

Los derechos de intimidad y privacidad han tenido desarrollos diferentes en las tradiciones del *Common Law* —países anglosajones— y en el derecho continental, principalmente España, Francia y América Latina. En la tradición anglosajona los derechos de privacidad abarcan un área más amplia (Shepherd, L. 2001: 251-320):

- Como un derecho de libertad.
- Como una prevención y protección contra los totalitarismos.
- Como el 'derecho a ser dejado solo'[4].

En los EE. UU. 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 diferentes: en *Pierce v. Society of Sisters*[5] se ataca una ley que hacía obligatoria la enseñanza inicial en inglés; en *Skinner v. Oklahoma*[6] se deja sin efecto una ley que establecía la esterilización de ciertos criminales. En *Griswold v. Connecticut*[7] 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'. El concepto de privacidad transitó después situaciones mucho más controvertidas: *Cruzan v. Director, Missouri Department of Health*[8] (rehusar tratamiento médico), *Roe v. Wade*[9] (aborto), y *Washington v. Glucksberg*[10] (suicidio asistido).

La identificación del derecho de privacidad, como un conjunto de prevenciones y protecciones contra los totalitarismos, ha sido señalada por Rubenfeld (1989: 737-752). Esta visión permite advertir que tanto la protección de la privacidad como de los datos personales no son derechos por los

4 La expresión *'right to be let alone'* es usada por Louis Brandeis en *Olmstead v. U.S.*, 277 US 438.

5 268 US 510 (1925).

6 316 US 535 (1942).

7 381 US 479 (1965).

8 497 US 261 (1990).

9 410 US 113 (1973).

10 521 US 702 (1997).

que preocuparse solamente en los países industrializados y con tradiciones democráticas fuertes. En algunos países en desarrollo se han sucedido los totalitarismos más descontrolados; ¿qué sería dotar a estas estructuras estatales de un conocimiento más profundo e individualizado de las personas?, ¿no es la privacidad la mejor protección de grupos minoritarios y disidentes frente a persecuciones estatales?

En la tradición continental, los derechos a la intimidad y a la propia imagen están estrechamente relacionados a la evolución de la defensa del honor. La primera manifestación clara de la protección de la intimidad es el dictado de la *Lex Comelia de iniuris* (81 a.C.). La mayoría de las legislaciones actuales lo consideran un derecho de la personalidad y es un derecho fundamental (Peña González, C. 1996: 545-660). Osvaldo Gozaíni (2001) ha formulado interesantes consideraciones sobre la historia y el proceso de formación de estos derechos: "La preocupación, en los términos actuales, por la intimidad es el resultado de un largo proceso histórico de transformación de la conciencia que comienza con la contrarreforma, pasa por la desvalorización de la conciencia religiosa por los filósofos del siglo XVII (Hobbes, Locke, Descartes, Spinoza) y desemboca en la construcción de la conciencia moral, preparada por Thomasius y concluida por Kant. Con éste la libertad del hombre es la que permite enjuiciar por sí mismo sus acciones y determinar su voluntad a partir de una inclinación a la moralidad que le es innata. Sobre esta concepción del hombre —agrega Juan Manuel Fernández López— adquiere sentido la noción actual de intimidad como atributo necesario de su nuevo *status* de libertad-autonomía. La dualidad de la persona (interioridad y socialidad) se traslada a la intimidad que es bidireccional: *ad se* y *ad alteros*. La intimidad, si bien hace referencia primariamente a un espacio propio, privativo del individuo, éste solo adquiere su pleno sentido frente a los otros, tanto para oponerlo a ellos como para compartirlo con los demás. Así, la intimidad es simultáneamente condición de la personalidad individual y de la personalidad social". Sostiene el autor citado que "mientras Europa persigue la defensa de la persona a través de normas que especifiquen los límites del Estado y de los particulares para el tratamiento de los datos; en Estados Unidos, principalmente, no hay políticas constitucionales sobre el tema, prefiriendo la revisión judicial de aquellos actos que agreden, eventualmente, el derecho a la privacidad (por eso el incluir el aborto dentro de la esfera íntima de la mujer) y que dieron lugar en el año 1974 a la *Privacy Act.* En tér-

minos parecidos, la distinción que hacen los primeros entre derechos personalísimos (titular de los datos) y portadores o administradores de ellos (bancos de datos), busca ampliar el panorama de derechos de las personas y limitar el uso de los datos que tienen las empresas cuando está ausente el consentimiento del titular para la aplicación de ellos a un fin determinado.

La jurisprudencia americana, amplia y generosa en este capítulo de derechos fundamentales, perfila un cuadro sucesivo de protecciones que inician desde el famoso "*right to be alone*" (derecho de ser dejado a solas), atraviesa las relaciones con la prensa y los medios de comunicación, y culmina con la tutela de los datos que se recopilan con medios informáticos.

El trabajo de Alberto Bianchi (1995: 866-878) señala que en los EE. UU. la protección del derecho a la privacidad (*right of privacy*) abarca numerosos casos, así como profusa doctrina, aunque el problema siempre gira sobre el concepto que encierra la conocida cita del juez Louis Dembitz Brandeis según la cual privacidad significa el derecho "de ser dejado a solas". Ahora bien, agrega Bianchi, si queremos remontarnos a los orígenes del derecho a la privacidad advertiremos en primer lugar que se trata de una historia típicamente angloamericana. Asimismo y con fines metodológicos, es susceptible de ser dividida en cuatro períodos. El primero corre desde los orígenes del *common law* hasta el año 1890, fecha en que fue publicado un célebre artículo de Warren y Brandeis (1980: 193), el segundo período que se extiende hasta un ensayo publicado en 1960 por William Prosser, está referido principalmente a los problemas suscitados entre la privacidad y la prensa. El tercer período –donde el eje de la *privacy* se traslada de los Estados Unidos a Inglaterra– comienza con el proyecto de ley elaborado por Lord Mancroft y enfoca los conflictos entre la privacidad y los medios masivos de comunicación (*mass media*). El cuarto período, finalmente, empieza en 1969 con el proyecto de ley de Walden, en el cual aparece por primera vez el problema de la tutela de los datos personales memorizados por ordenadores.

En la jurisprudencia de los EE. UU. el derecho de privacidad está 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[11]. Se ha observado, por ejemplo,

11 Ver 62A *American Jurispudence* 2d Privacy 25. Una excepción en el *common law* sería la Sección 30 de la *Freedom of Information Act* de 1999 de Trinidad y Tobago en la que se protege la privacidad de las personas muertas.

que los registros penales de menores de edad —que están protegidos— pueden ser abiertos, en especial si una persona muere en circunstancias inexplicables. Este punto de vista no es compartido en el sistema continental donde la intimidad y privacidad están ligadas al honor (Cifuentes, S. 1995: 404).

Otro aspecto claro en la tradición continental es que no existe privacidad para las personas jurídicas (morales). En varias oportunidades ha sido declarado por el Tribunal Superior de Justicia de Venezuela, en *Inversora Bohemia II C.A y Valores H.B.* y otros casos similares. Contrariamente, en Trinidad y Tobago, en el caso *Collymore y otro c. General Attorney* el Privy Council sostiene que el derecho se extiende a las sociedades de hecho, como por ejemplo los sindicatos[12].

Estado de la legislación en la Región

Instrumentos internacionales

Tabla I

Instrumentos internacionales relacionados con los Derechos de Privacidad e Intimidad
[1948] Declaración Americana de los Derechos y Deberes del Hombre [artículos ii, iii y xxii].
[1948] Declaración Universal de los Derechos Humanos [preámbulo, artículos 2.1, 16 y 18].
[1948] Convención para la Prevención y la Sanción del Delito de Genocidio [ii].
[1966] Pacto Internacional de Derechos Económicos, Sociales y Culturales [artículos 2.2, 13.1, 13.3 y 17].
[1966] Pacto Internacional de Derechos Civiles y Políticos [artículos 2, 4 y 20].
[1967] Convención Internacional sobre la Eliminación de todas las Formas de Discriminación Racial [artículo 5].
[1969] Convención Americana sobre Derechos Humanos (Pacto de San José de Costa Rica) [artículos 1, 11, 12, 13.5, 16, 22.8, y 27].
[1980] Directrices de la Organización de Cooperación y Desarrollo Económico OCDE para la Protección de la Privacidad y el Flujo Transfronterizo de Datos Personales.

12 12 WIR 5 y 15 WIR 229.

[1989] Convención sobre los Derechos del Niño [preámbulo, artículos 2, 14, 16, 20, 29, 30 y 40.2.vii].
[1990] Directrices de las Naciones Unidas en Relación con los Archivos Computarizados de Datos Personales.
[1995] Directiva 95/46/CE del Parlamento Europeo.
[1998] Declaración Universal sobre el Genoma Humano y los Derechos Humanos [artículos 5 y 7].
[2000] Protocolo facultativo de la Convención sobre los Derechos del Niño relativo a la venta de niños, la prostitución infantil y la utilización de niños en la pornografía [artículo 2.c].

Tendencias legislativas

Algunas legislaciones contemplan diferentes sistemas de acceso —o limitaciones— a los bancos de datos de carácter personal, dependiendo de la clase de archivo de que se trate. Sin embargo, la cuestión es ardua y requiere un debate amplio. Para reconstruir la tendencia actual sobre la protección de datos personales se cita en primer lugar la Directiva 95/46/CE del Parlamento Europeo y del Consejo de Europa, del 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, dice:

Sección I · principios relativos a la calidad de los datos

Artículo 6. 1. Los Estados miembros dispondrán que los datos personales sean:

a. tratados de manera leal y lícita.
b. recogidos con fines determinados, explícitos y legítimos, y no sean tratados posteriormente de manera incompatible con dichos fines; no se considerará incompatible el tratamiento posterior de datos con fines históricos, estadísticos o científicos, siempre y cuando los Estados miembros establezcan las garantías oportunas.
c. adecuados, pertinentes y no excesivos con relación a los fines para los que se recaben y para los que se traten posteriormente.
d. exactos y, cuando sea necesario, actualizados; deberán tomarse todas las me-

didas razonables para que los datos inexactos o incompletos, con respecto a los fines para los que fueron recogidos o para los que fueron tratados posteriormente, sean suprimidos o rectificados.

e. conservados en una forma que permita la identificación de los interesados durante un período no superior al necesario para los fines para los que fueron recogidos o para los que se traten ulteriormente. Los Estados miembros establecerán las garantías apropiadas para los datos personales archivados por un período más largo del mencionado, con fines históricos, estadísticos o científicos.

2. Corresponderá a los responsables del tratamiento garantizar el cumplimiento de lo dispuesto en el apartado 1".

Los derechos de intimidad y privacidad en las Américas

Algunos países americanos poseen legislación de carácter general para la protección de la privacidad y de los datos personales. En Canadá el *Privacy Act* (1983) reemplazó un conjunto de derechos contenidos en la Parte IV del *Canadian Human Rights Act*. El objetivo del *Privacy Act* fue lograr una mejor protección frente al impacto de las nuevas tecnologías y la tendencia creciente del gobierno a crear sistemas de información. Esta norma incrementa la transparencia y les da a los canadienses un mayor control sobre sus datos personales almacenados en sistemas gubernamentales.

Sus regulaciones obligan al gobierno a:

- limitar el almacenamiento de información de carácter personal a los detalles mínimos necesarios para ejecutar los programas o actividades.
- recolectar la información —siempre que sea posible— directamente de la persona concernida.
- informar a las personas por qué se pide información y cómo será usada.
- no utilizar la información para otros propósitos, excepto que la ley lo permita.
- mantener la información en forma tal que la persona concernida tenga una razonable oportunidad de acceso.
- asegurar que la información es precisa, actualizada y tan completa como sea posible.

- no difundir información personal excepto cuando está permitido por el *Privacy Act* u otra legislación.

En los EE. UU. los derechos de privacidad no están enumerados en la Constitución, pero se los considera en 'su penumbra', o sea implícitamente protegidos por los principios constitucionales[13]. En sucesivos fallos la Corte Suprema de Justicia ha sostenido que las Enmiendas Cuarta y Decimocuarta protegen a los individuos de ciertos tipos de intrusiones en su vida privada. En la actualidad el *U.S. Code* contiene dispersas muchas disposiciones sobre privacidad.

Las Constituciones de Colombia, Brasil, Argentina y Perú contienen una protección genérica que en algunos casos siquiera está desarrollada legislativamente o reglamentada.

La Constitución de Brasil de 1988 ha establecido el *habeas data* en el artículo 5º:

Título II Dos Direitos e Garantias Fundamentais
Capítulo I Dos Direitos e Deveres Individuais e Coletivos

Art. 5.º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:

LXXII – conceder-se-á habeas data: a) para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público; b) para a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo.

Prescripciones equivalentes están en la Constitución de Colombia de 1991 (artículo 15), la Constitución del Perú de 1993 (artículo 200.3) y la Constitución de la Nación Argentina de 1994 (artículo 43).

13 *Griswold v. Connecticut*, 381 US 479 (1965).

Varios países cuentan ya con legislaciones específicas para la protección de los derechos de intimidad, privacidad y de los datos personales: Argentina (2000), Brasil (1997), Chile (1999), Ecuador (1997), República Dominicana (1997) y Venezuela (1991), en la mayoría de los casos destinadas a regular el *Habeas data.* En otros, por ejemplo, México, Uruguay hay proyectos o iniciativas parlamentarias que están siendo discutidas.

Análisis comparativo de las normas nacionales

Tabla II

Legislación sobre privacidad e intimidad

Argentina

Código Civil [artículo1071 bis].
[1977] Ley de Entidades Financieras [Ley 21.526, artículos 39 y 40].
[1977] Ley de Procedimiento Tributario [Ley 11.683, artículo 101 sobre secreto fiscal].
[1990] Ley de Prevención y Lucha contra el Síndrome de Inmunodeficiencia Adquirida (SIDA) [Ley 23.798].
[1994] Constitución de la Nación Argentina [artículos 18, 19 y 43] y tratados incorporados a la Constitución Nacional con la reforma de 1994 que tienen normas referidas a la protección de la vida privada.
[1995] Ley de Mediación y Conciliación [artículo 11].
[1998] Ley de Tarjetas de Crédito, [Ley 25.065, artículo 53].
[1999] Ley de Ética en el Ejercicio de la Función Pública [Ley 25.188, artículos 10 y 11].
[2000] Ley de Protección de Datos Personales [Ley 25.326].
[2000] Ley del Registro de Deudores Alimentarios de la Provincia de Neuquen.
[2001] Ley de Creación del Registro Nacional de Donantes de Células Progenitoras Hematopoyéticas [Ley 25.392].

Brasil

[1964] Lei nº 4.595 [artículo 38].
[1966] Código Tributário Nacional [Lei nº 5. 172, artículo 198].
[1978] Constituição da República Federativa do Brasil [artículo 5º].
[1990] Código de Proteçao e Defensa do Consumidor [artículos 43, 44 y 45].
[1990] Estatuto da Criança e do Adolescente [artículos 10.I, 17, 240, 241 y

247].
[1996] Lei da Escuta Telefônica [Lei nº 9.296].
[1997] Lei que regula o direito de acceso a informaçoes e disciplina o rito processual do *habeas data*.

Costa Rica
[1949] Constitución Política de la República de Costa Rica (artículos 30 y 24).
[1989] Ley de la Jurisdicción Constitucional [Ley 7135, artículos 2,15, 29, 57 y 66].
[1970] Código Penal [artículo 196].
[1989] Ley de la Jurisdicción Constitucional [artículos 2, 15, 29, 57 y 66].
[1995] Ley contra Hostigamiento o Acoso Sexual en el Empleo y la Docencia [artículo 23].
[1995] Creación del Sistema de Emergencias 911 [Ley 7566 artículo 13].
[1996] Reforma Constitucional (artículos 24 y 46) [Ley 7607, artículo 1].
[1996] Ley de Justicia Penal Juvenil [artículos 20, 21 y 99].
[1996] Ley de Igualdad de Oportunidades para las Personas con Discapacidad [artículo 40].
[1996] Código Procesal Penal [artículos 181, 196 y 295].
[1998] Sistema de Estadística Nacional [Ley 7839 artículo 10].
[1998] Código de la Niñez y la Adolescencia [artículo 25].

Chile
[1928] Decreto 950 de 1928, artículo 10, agregado por decreto 516 de 1988, sobre el Boletín de Informaciones Comerciales.
[1967] Ley 16.643 de Abuso de Publicidad.
[1980] Constitución Política de la República de Chile [artículo 19, Inc. 4].
[1993] Ley 19.223 de Delitos Informáticos.
[1994] Decreto 1.137 - Reglamento del Registro Nacional de Discapacidad. [Ley 19.284].
[1999] Ley 19.628 de Protección de Datos de Carácter Personal

Ecuador
Código Penal [artículos 197 y 213].
[1974] Ley Orgánica de la Función Judicial [artículo 201].
[1992] Ley Especial de Telecomunicaciones (Ley Nro. 184) Artículo 14.
[1996] Código de Menores, [artículo 168].
[1997] Ley de Control Constitucional [artículos 34 al 45 sobre *Habeas data*].
[1998] Constitución Política de la República de Ecuador [Artículo 23.8].
[2000, en *vacatio legis*] Código de Procedimiento Penal [artículo 69.6 sobre los

derechos del ofendido].
[2000] Ley Reformatoria a la Ley de Discapacidades [artículo 14 sobre el Registro Nacional de Discapacidades y Reglamento General de la Ley sobre Discapacidades del 4 de febrero de 1994, artículos 51 y 52].
[2001] Ley General de Instituciones del Sistema Financiero [artículos 88 a 94].
Proyecto de Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.

El Salvador
[1972] Código de Trabajo, artículo 406.
[1983] Constitución de la República de El Salvador [artículo 2 y 6].
[1994] Código de Procedimientos Civiles, artículo 156.
Ley del Ejercicio Notarial de la Jurisdicción Voluntaria y de otras Diligencias, artículo 11.
[1994] Ley del Menor Infractor, artículo 5 y 30.
[1994] Ley Procesal de Familia, artículo 215.
[1995] Ley Transitoria del Registro del Estado Familiar y de los Regímenes Patrimoniales del Matrimonio, artículos 3 y 17.
[1997] Código Penal, "la Calumnia y la Injuria" (artículos 177 al 183) y "Delitos Relativos a la Intimidad" (artículos 184 al 191).

Jamaica
[1962] Constitución de Jamaica [Capítulo III, títulos 19 y 22].
[1992] Ley de Bancos [título 45 y cuarta tabla].

México
[1917] Constitución Federal [artículos 6to. y 7mo.].
[1917] Ley sobre Delitos de Imprenta, (artículos 1ro. y 9no.).
[1990] Ley de Instituciones de Crédito [artículos 112bis, 117 y 118].
[1990] Ley para Regular las Agrupaciones Financieras [artículo 33].
Ley de Protección y Defensa al Usuario de Servicios Financieros [artículos 13,14,15].
[2001] Iniciativa sobre Ley Federal de Protección de Datos Personales del senador Antonio García Torres, PRI.

República Dominicana
[1962] Ley de Expresión y Difusión del Pensamiento [artículos 41 al 45].
[1965] Ley General de Bancos [artículos 31 a 34].
[1994] Constitución Política de la República Dominicana [artículo 8.9 y 8.10].

[1994] Código para la Protección de Niños, Niñas y Adolescentes [artículos 66, 67 y 237].
[1997] Código Penal [artículos 336 a 338-1, reformados por la Ley 24-97].
[1998] Ley General de Telecomunicaciones [artículos 5 y 6].
[2000] Resolución 36 de INDOTEL - Instituto Dominicano de Telecomunicaciones [artículos 1 a 9].
[2001] Ley No. 11-01 sobre Cumplimiento de las Obligaciones Tributarias [artículo 3, párrafo I].

Trinidad y Tobago
[1921] Ley del Registrador General [secciones 4 a 6].
[1925] Ley de Niñez [sección 87].
[1952] Ley de Estadística [secciones 8 y 9].
[1955] Ley de Permisos de Venta de Bebidas Alcohólicas [sección 57].
[1960] Ley de Hospitales Privados [sección 8].
[1960] Ley de Alimentos y Medicamentos [Segunda Tabla].
[1965] Ley de Servicio Policial [secciones 37 y 111].
[1970] Ley de Armas de Fuego [sección 29].
[1980] Constitución de la República de Trinidad y Tobago [sección 4(c)].
[1999] Ley de Libertad de la Información [sección 29] y Ley de Libertad de la Información (Enmienda).
[2000] Ley del Registrador General (Enmienda) [sección 3].
[2000] Ley de Integridad en la Vida Pública [sección 2 y Tabla].
[2000] Ley de Uso Indebido de la Informática [Parte II, secciones 3 a 10].
[2000] Ley de Identificación de ADN [secciones 39 y 40].
[2000] Ley sobre Delitos de Transferencia Electrónica de Dinero [sección 20].
[2000] Proyecto de Ley sobre Telecomunicaciones [secciones 24, 65 y 80].

Uruguay
[1988] Acción de Amparo [Ley 16.011].
[1997] Constitución de la República [artículos 7 y 29].
[2000] Proyecto de Ley sobre Derecho a la Información y acción de *Habeas data.*
[2000] Proyecto de Ley para la creación Registro Nacional de Deudores Alimentarios.
[2000] Proyecto de Ley sobre regulación de los Bancos de Datos de Información de Cumplimiento de Créditos o de Obligaciones de Tracto Sucesivo.
[2000] Proyecto de ley por el que se regula el funcionamiento de los Bancos de Datos.
[2000] Proyecto de Ley por el que se crea un padrón especial para la inscripción cívica de aquellas personas con discapacidades físicas que así lo requieran.

[2000] Proyecto de Ley sobre personas físicas o jurídicas que administren, gestionen u obtengan información de cualquier base de datos.
[2000] Proyecto de Código de la Niñez y Adolescencia, [artículos 11, 22 inc.F, y 211 a 215].

Venezuela
[1999] Constitución de la República Bolivariana de Venezuela [artículos 48, 60, 143 y 283.1].
[1977] Ley de Transfusión y Bancos de Sangre [artículo 44].
[1979] Ley de Registro de Antecedentes Penales [artículos 2 y 6].
[1991] Ley de Protección de la Privacidad de las Comunicaciones.
[1998] Resolución 001-06-98 de la Superintendencia de Bancos.
[2000] Ley Orgánica para la Protección del Niño y del Adolescente [artículos 50, 65 a 68, 139, 227 y 228].
[2000] Ley Orgánica de Telecomunicaciones [artículo 190].
[2001] Decreto con Fuerza de Ley sobre Mensajes de Datos y Firmas Electrónicas
Proyecto de ley Defensoría del Pueblo.

Colisión entre derechos

La mayoría de los casos judiciales en los que se reclama por violaciones a la intimidad o privacidad, son resueltos haciendo una ponderación entre los intereses comprometidos. Existen al menos tres posibilidades:

- colisión entre derechos fundamentales.
- ponderación entre derechos e intereses colectivos.
- ponderación entre derechos e intereses particulares.

Colisión entre derechos fundamentales: libertad de expresión

El ejemplo más interesante sobre colisión de derechos fundamentales ocurre con la libertad de expresión. En una reciente Declaración de Principios la Comisión Interamericana de Derechos Humanos, durante su 108° período ordinario de sesiones, dijo:

> "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 estaban difundiendo noticias falsas o se condujo con manifiesta negligencia en la búsqueda de la verdad o falsedad de las mismas".

Existen varios casos judiciales en los que se ha discutido la cuestión. Quizás el de mayor resonancia es el que resultó de la publicación en Argentina del libro "Impunidad Diplomática" (Martorell, F. 1993). El libro fue prohibido en Chile, decisión que fue 'confirmada' por la Corte Suprema[14]. El caso fue llevado a la Comisión Interamericana de Derechos Humanos, la que finalmente recomendó al gobierno de Chile que debe permitir la circulación y venta del libro[15]. En su fundamentación dice: "[69]. *The Commission considers that it is not for the Commission to examine the content of the book in question or the conduct of Mr. Martorell, because it does not have competence in the matter and because the right to honor is duly protected under Chilean law. Moreover, as the proceedings in the instant case show, those persons who believe that their honor and dignity have been impugned have, in the Chilean courts, adequate remedies to settle that question.* [70]. *For that reason, the Commission cannot accept the Chilean Government's argument that the right to honor would be higher than the right to freedom of expression"* (Fuentes Torrijo, X. 2000: 427).

---

14 *Luksic Craig, Andrónico c. Editorial Planeta.* Corte Suprema, 15 de junio de 1993. "El autor del libro "Impunidad Diplomática" ha incurrido en un acto arbitrario e ilegal que ha significado privación, perturbación y amenaza del artículo 19 nro. 4 de la Constitución, al divulgar hechos que caen en el ámbito de la vida privada e íntima de las personas. Se acogió el recurso de protección y se prohibió la internación y comercialización en Chile del libro". Ver sobre censura artículo 19 nro. 12 y artículo 1 de la Constitución.

15 *Francisco Martorell v. Chile*, Caso 11.230, Report No. 11/96, Inter-Am.C.H.R.,OEA/Ser.L/V/II.95 Doc. 7 rev. at 234 (1997). "The Government of Chile has pointed out that the rights to honor and dignity often conflict with freedom of expression, that the State must endeavor to balance these rights with the guarantees inherent in freedom of expression, and that a right may be sacrificed for the sake of what is considered to be a higher right".

La libertad de expresión ha tenido en los últimos años un matiz diferente. Ello se debe a la actitud que los periódicos han tenido con respecto a Internet. La tendencia actual es que los periódicos colocan diariamente las principales noticia en sus sitios en Internet, y además facilitan el acceso a sus ediciones anteriores con un motor de búsqueda. Estos motores de búsqueda son capaces de buscar noticias en función de nombres personales, por lo que una noticia que incluía nombres personales se torna ahora indefinidamente accesible.

Para analizar esta situación son relevantes algunas decisiones judiciales en los EE. UU. que analizan la pérdida de los derechos de privacidad, en particular de ciertas personas a las que se caracteriza como 'figuras públicas'. También los tribunales de California han sostenido que las figuras públicas retienen cierta 'zona de privacidad'[16].

La Corte Suprema de los EE. UU. ha señalado en dos precedentes el conflicto entre la libertad de prensa y los derechos de privacidad: *Cox Broadcasting Corp. v. Cohn*,[17] y *Florida Star v. BJF*[18]. En ambos casos, la Corte sostiene que la Primera Enmienda no permite a los Estados hacer prevalecer la privacidad cuando la prensa publica información verdadera legítimamente obtenida de documentos públicos o procesos sobres asuntos de interés público. Cuando una figura pública reclama por los daños derivados de una invasión de privacidad, se ha sostenido que quien es famoso ha perdido alguna porción de su privacidad[19].

Williams (1993: 337) sostiene que el estándar de *'newsworthiness'* utilizado por los tribunales para evaluar las acciones de invasión en la privacidad no es suficientemente claro para que los editores estén en condiciones de prevenir reclamos, y considera que debería analizarse: (i) el valor social de los hechos publicados; (ii) en qué medida el artículo incursiona ostensiblemente en asuntos privados; y (iii) el grado en el cual la persona involucrada ha accedido a una posición de notoriedad pública.

Estos conceptos permiten trazar dos categorías de personas públicas: (i) las 'personas voluntariamente públicas' son aquellas que se han ubicado o

16 Ver *Diaz v. Oakland Tribune, Inc.,* 188 Cal. Rptr. 762, 772-73 (Cal. Ct. App. 1983).

17 420 US 469 (1975).

18 491 US 524 (1989).

19 *Carlisle v. Fawcett Publications, Inc.,* 20 Cal. Rptr. 405, 414 (Cal. Ct. App. 1962).

expuesto ante la mirada del público por sus actividades o asumiendo un *rôle* prominente en instituciones o actividades de interés para el público en general. Han sido consideradas personas públicas los actores[20], atletas profesionales[21], políticos[22], músicos, intérpretes y animadores[23]. Se interpreta que el público posee un interés legítimo en obtener información sobre personas voluntariamente públicas, esta información puede llegar a ser tan amplia que incluiría aspectos que para otras personas serían privados. (ii) 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, personas 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[24]. Un caso relevante en la definición de esta categoría es *Kapellas v. Kofman*[25]. 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[26].

Sin duda sería muy difícil establecer quiénes son personas públicas, y entre éstas quiénes son voluntaria o involuntariamente públicas. Las legislaciones latinoamericanas parecen ser más restrictivas con el concepto de per-

---

20 *O'Hilderbrandt v. Columbia Broad. Sys.*, 114 Cal. Rptr. 826, 830 (Cal. Ct. App. 1974).

21 *Cepeda v. Cowles Magazines and Broad.,* 392 F.2d 417, 419 (9th Cir. 1968).

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

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

24 Así fue definido en *Carlisle, supra* nota 29.

25 459 P.2d 912 (Cal. 1969).

26 En *Sidis v. 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.

sonas involuntariamente públicas. La Ley de Ética en el Ejercicio de la Función Pública (1999) de Argentina incluye una lista exhaustiva de personas públicas que están obligadas a revelar su patrimonio[27]. En Trinidad y Tobago parece muy restrictiva la enumeración de 'personas en la vida pública' de la *Integrity in Public Life Act* (2000) sección 2 y tabla final.

En *R.M.F.G. c. D.A.*,[28] se dice que: "Los derechos al honor y a la libertad de expresión se encuentran en el mismo nivel de jerarquía, como derechos fundamentales" y en *H.V.P.*[29], "Cuando se verifica una colisión de derechos (…) entre la libertad de expresión y de información y el derecho al honor y a la intimidad, debe estarse ante una ponderación de intereses. …la injerencia en el honor ajeno encuentra su justificación en la causa del interés público, en el del interés general…"[30].

En el *Common Law,* para establecer responsabilidad por los daños derivados de la divulgación de información privada se requiere que haya sido ampliamente publicada y no confinada a unas pocas personas o en circunstancias limitadas. En 1972 fue reformada la Constitución de California estableciendo que la privacidad es un derecho inalienable de los ciudadanos[31]. Antes de la reforma en *Hill v. National Collegiate Athletic Association*[32], y después en *White v. Davis*[33], la Suprema Corte de California definía los criterios para decidir los reclamos por invasión de la privacidad. De acuerdo a estos criterios los reclamantes deben: (i) identificar un interés específico y protegido legalmente de privacidad, (ii) probar que el reclamante tenía una expectativa razonable de privacidad, y (iii) una invasión grave de la privacidad.

---

27 Ver, por ejemplo, como el ex-vicepresidente de Argentina Carlos Álvarez ha difundido su patrimonio en su sitio en Internet: (www.chachoalvarez.com).

28 Sentencia del 2 de marzo de 1993 del Tribunal de Apelaciones Penal de Uruguay, 107 *La Justicia Uruguaya* nro. 12.338.

29 Sentencia del 13 de marzo de 1999 del Tribunal de Apelaciones Penal de Uruguay, 120 *La Justicia Uruguaya* nro. 13.724.

30 Ver también, *Movimiento al Socialismo M.A.S. v. Gobernador del Estado Apure,* sentencia nro. 1155 del 18 de mayo de 1999 del Superior Tribunal de Justicia de Venezuela.

31 Cal. Const. Art. I, § 1. Article I section 1 dice: *"All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness and privacy".*

32 865 P.2d 633 (Cal. 1994).

33 533 P.2d 222 (Cal. 1975).

La supremacía de la libertad de expresión está en discusión en este momento en relación con el caso *Free Speech Coalition v. Reno*. La *Child Pornography Prevention Act* de 1996 prohíbe la difusión de cualquier imagen que 'aparezca como' una conducta sexualmente explícita de un niño. En el caso se discute si esta ley —cuya finalidad es la protección de la infancia— se aplica cuando se trata de imágenes creadas por software, en las que ningún niño ha participado[34]. Éste es otro interesante ejemplo de la dificultad de las normas jurídicas para adaptarse a los cambios tecnológicos. El caso ha sido admitido el 22 de enero de 2001 por la Corte Suprema para su consideración[35].

Ponderación de intereses colectivos

En *Vernonia School District v. Wayne Aclon et ux.*[36] la Suprema Corte de los Estados Unidos evaluó la *Student Atlete Drug Policy* adoptada por la Escuela Vernonia, motivada por el descubrimiento de que los atletas eran los líderes en la cultura del uso de drogas entre los estudiantes y por la preocupación de que el uso de drogas aumenta los riesgos de lesiones producidas por el deporte. Esta política autoriza la realización de exámenes de orina al azar a estudiantes que participan en los programes atléticos. A James Acton se le negó participar en el programa de fútbol escolar cuando él y sus padres (también partes en el proceso) no dieron su consentimiento para la realización de dicho examen. Ellos iniciaron un proceso judicial buscando una declaración y una orden correctiva sobre la base de que la política violaba la Cuarta y Decimocuarta Enmienda y la Constitución de Oregon.

La Corte Suprema de los Estados Unidos sostuvo que la política es constitucional bajo la Cuarta y Decimocuarta Enmienda. La 'razonabilidad' del examen es juzgada contrapesando la intromisión en los intereses del individuo protegidos por la Cuarta Enmienda contra la promoción de los intereses gubernamentales legítimos. El primer factor a considerar para establecer

---

34 Ver, el *Protocolo facultativo de la Convención sobre los Derechos del Niño relativo a la venta de niños, la prostitución infantil y la utilización de niños en la pornografía*, artículo 2.c.

35 *Cfr.* 'PC Peep Show: computers, privacy, and child pornography', 27 *John Marshall Law Review* (1989) 989-1013.

36 000 US u10263, decidido el 26 de junio de 1995. En términos generales el contenido de este parágrafo está basado en la opinión de Antonin Scalia.

la 'razonabilidad' es la naturaleza del interés de la privacidad, el cual se contrapone con el examen. Los sujetos de la política son niños que han sido sometidos a la custodia temporal del Estado, como autoridad escolar, el Estado puede ejercer cierto grado de supervisión y control mayor que el que podría ejercer sobre los adultos capaces. Los requerimientos de que los niños de una escuela pública se sometan a exámenes físicos y a vacunación indican que ellos tienen una expectativa menor de privacidad con respecto a los exámenes y procedimientos médicos que el resto de la población. Los atletas estudiantiles tienen aun una menor expectativa legítima de privacidad, debido a que en la participación atlética se encuentre implícito un elemento de desnudez colectiva y además los atletas se encuentran sujetos a exámenes físicos pre-temporada y a normas que regulan su conducta. La Suprema Corte sostiene que la cuarta enmienda no exige que se realice el examen 'menos invasivo', de manera que el argumento de que el análisis para establecer el uso de drogas podría basarse en la sospecha de dicho uso, si se comprobase, no sería decisivo; y que dicha alternativa trae aparejadas sus propias 'dificultades sustantivas'[37].

En el caso *CODEPU c. Gendarmería de Chile y otro.* (Corte Suprema 1995) se afirma que la instalación de micrófonos en establecimientos de reclusión se encuadra entre las medidas de seguridad contempladas para el mismo por el Decreto nro. 353, artículo 2, del Ministerio de Justicia. En este caso, indirectamente, se afirma que la seguridad pública prevalece sobre los derechos de privacidad. La decisión ha sido discutida internacionalmente[38].

---

37 Según Traband se invierte la carga de la prueba, se viola la presunción de inocencia, y se crea desconfianza entre alumnos y maestros. Rhett Traband, 'The Acton case: the Supreme Court's Gradual sacrifice of privacy rights on the altar of the war on drugs', 100 *Dickinson Law Review* (1995) 1-28. Ver también, *A.V.P. c. Ministerio de Educación y Cultura y Comité Olímpico Uruguayo,* (Tribunal de Apelaciones Civil –5to. turno– 1998), la doctrina del Tribunal expresa que la información periodística relativa a temas de dopaje, individualizando los autores, contribuye a la erradicación de esa práctica nociva, a la vez que mantiene informada a la opinión pública sobre un asunto de evidente interés, como es la conducta de sus deportistas y las razones por las cuales no han sido llamados a integrar una delegación de la República. 118 *La Justicia Uruguaya*, nro. 13.590.

38 Como es natural el Supremo Tribunal Federal de Brasil en *Paulstein Aureliano de Almeida,* habeas corpus (1996) determinó que "*a violação do sigilo das comunicações telefônicas para fins de investigação criminal ou instrução processual penal, não é auto-aplicável: exige lei que estabeleça as hipóteses e a forma que permitam a autorização judicial. [...] A garantia que a Constituição dá, até que a lei o defina, não distingue o telefone público do particular, ainda que instalado em interior de presídio, pois o bem jurídico protegido é a privacidade das pessoas, prerrogativa dogmática de todos os cidadãos".*

Normalmente, la legislación y la jurisprudencia reconocen la posibilidad de realizar inspecciones personales o de documentos, cuando existen sospechas fundadas de la comisión de un delito. En Jamaica en el caso *King v. The Queen*[39] (Privy Council 1968) se estableció que el título 18 de la *Constabulary Force Act* no tiene previstos términos para la revisión física a una persona, y se decidió que el título 22 no da autorización para revisar a una persona como parte del mandato del juez de paz. Las pruebas contra él (durante la revisión sin consentimiento del Sr. Herman King, se encontró marihuana en un bolsillo de su pantalón), fueron obtenidas ilegalmente, 'habrán de excluirse'. Por el contrario en Trinidad y Tobago, en el caso *D. Davidson c. R. Williams y Fiscal General*[40] (Tribunal Superior 1988) la Policía obtuvo dos órdenes para revisar el local del querellante, y buscar los documentos mencionados en ellas, los cuales evidenciarían la comisión de un delito de falsificación bajo el título 4(2)(a) de la Ley de Falsificación. El querellante inició un proceso reclamando que el procedimiento utilizado fue ilegal e inconstitucional, y solicitó también daños y perjuicios. La sentencia desestimó el reclamo de que los derechos del querellante bajo el título 4(c) de la Constitución fueron afectados.

El secreto bancario es coincidente en algunas legislaciones con el derecho a los datos personales. Es así como en *Douglas and others v. Pindling*[41] se sostiene que el derecho a que no se difunda la información bancaria, sin consentimiento, establecido en la sección 10 de la *Banks and Trust Companies Regulation (Amendement) Act* de Bahamas, debe ceder al interés público. Igual decisión se toma en los casos *Troy Megill v. General Attorney and others* y *George Mayne v. General Attorne and other*[42].

Ponderación de intereses particulares

El acceso al crédito es visto como un interés particular que contribuye al desarrollo de la economía, un interés colectivo. Durante muchos años la ob-

39 10 **JLR** 438.

40 1 **TTLR** 189.

41 Privy Council (1996) 48 **WIR** 1.

42 Court of Appeal, Jamaica, 1994. 31 **JLR** 87.

tención de un crédito, ya sea en metálico o para la compra de bienes, estaba precedida por la obtención de garantías (personales o bienes en hipoteca). Estos requisitos eran especialmente una barrera a la obtención de créditos para el consumo, en particular para personas de pocos recursos. Con la aparición de los sistemas de información centralizados fue posible desarrollar bases de datos sobre antecedentes crediticios. Estas bases de datos contienen datos personales y permiten el acceso al crédito tanto a las personas que no tienen antecedentes negativos como a aquellas que tienen antecedentes positivos. Sus defensores sostienen que la existencia de estos *Bureau* de Crédito resuelve la ineficiencia e ineficacia del sistema judicial en los juicios ejecutivos de cobro de dinero. Es una tendencia generalizada en muchos países que sólo un insignificante número de juicios concluyen con el pago de la deuda (directamente o por remate), mientras que en los restantes la insolvencia del deudor u otras causas hacen que el proceso termine sin una solución. Hoy la inclusión o no de una persona en un *Bureau* de Crédito opera como un incentivo para el pago, pues la 'sanción' es inmediata, permanente y de difusión internacional.

Este panorama es motivo de discusión: algunos opinan que los *Bureau* deben ser administrados por el Estado, otros consideran ésta una actividad del ámbito privado. En los EE. UU., por ejemplo, es necesario que la persona concernida autorice por escrito el pedido de consulta al *Bureau*; por el contrario, en América Latina —en la mayoría de los casos— los comerciantes consultan directamente el *Bureau* sin siquiera informar al interesado que sus datos personales están siendo verificados. En algunos casos se registran deudas que fueron pagadas luego de reclamos, en otros es obligatorio eliminar estos datos[43].

Muchos de estos problemas se resuelven con una legislación específica —prácticamente inexistente en América Latina— y con el recurso de *habeas data*.

---

43 *Cfr. Bravo, Francisco c. Alfaro Standen S.A., Assa S.A.,* Corte de Apelaciones de Santiago, 2000, "Quien repacta su deuda debe ser eliminado de los registros de morosidad" y *Bettenhauser Keim, Francisco c. Congesin Ltda. y DICOM S.A.,* Corte de Apelaciones de Valdivia, 1996, "Incurre en acto arbitrario una entidad de informaciones comerciales que se niega a eliminar a una persona de la lista de deudores no obstante que se acredita por documento fidedigno que la deuda se encuentra pagada de modo íntegro."

Acceso a la información

Un punto relevante al analizar el impacto de las nuevas tecnologías de comunicación e información es el acceso a la información, fundamentalmente si la información es de acceso público o restringido, y si se le garantiza a la persona concernida el derecho de acceso a su propia información, que puede incluir la posibilidad de corregirla y suprimirla. También es relevante para la persona concernida saber que su información está siendo utilizada, y quién y para qué la utiliza. El instituto destinado a proteger estos derechos es el *habeas data.*

Con relación al *habeas data* se distingue el destinado a tutelar el derecho a la autodeterminación informativa y todo el conjunto de principios (igualdad, dignidad, libertad) y derechos (honor, reputación, intimidad, imagen, etc.) que pueden ser vulnerados por el tratamiento de información y se lo denomina 'propio', y se le distingue del impropio destinado a proteger el derecho de acceso a la información pública como derecho a informarse en función a los principios republicanos de la publicidad de los actos de gobierno. Esta distinción es meramente clasificatoria en función de los bienes jurídicos protegidos. Sin embargo, ambos se traducen en ciertas facultades que los sujetos pueden ejercer con una diversidad de objetivos, esgrimiendo derechos subjetivos particulares en cada supuesto. Así se han distinguido en doctrina algunos tipos y subtipos (Sagües, N. 1996: 352)[44].

El *habeas data* informativo, persigue el acceso al registro a fin de indagar sobre la información almacenada y puede limitarse sólo a eso. Está previsto expresamente en Argentina, Brasil, Ecuador, Colombia, Guatemala, Perú y Paraguay, así como en la Constitución de Portugal. Algunos subtipos dentro de esta categoría serían: el 'exhibitorio' con el sólo fin de conocer los datos propios registrados, dentro del que también se incluye el de conocer determinada información pública no propia, generalmente definido como el derecho de libre acceso a las fuentes de información, incluido a veces dentro del derecho de libertad de prensa o expresión. En general, es limitado cuando existe un derecho de seguridad del Estado. Es considerado básico porque de él depende cualquier otra derivación para corregir, suprimir o pe-

44 Ver Sagües (1996: 352) o también *Subtipos de* Habeas data *en el Derecho Argentino: sus posibilidades en el Peruano*, Asociación Argentina de Derecho Constitucional, Argentina, 1996.

dir confidencialidad del dato. Otros subtipos son el 'finalista' que quiere conocer con qué finalidad, para qué y para quién; y el 'autoral' que persigue saber quién obtuvo los datos.

El *habeas data* 'aditivo' tiende a que se incluya un dato que al haberse omitido afecta a su titular, así como a que se aclare alguno que está. Un ejemplo es cuando con relación a bases crediticas, se pide que se aclare en la base que no se es el deudor principal de la obligación sino el garante. Las legislaciones de Argentina, Brasil, Colombia, Ecuador y Paraguay, así como la de Portugal, lo prevén expresamente.

El *habeas data* 'correctivo' persigue corregir datos falsos, inexactos o imprecisos, y cualquier otra forma que por su vaguedad o ambigüedad lleve a interpretar erróneamente al lector. Por ejemplo cuando algunas bases de datos utilizan expresiones con un significado particular en el sistema que no se corresponde con un uso técnico generalizado del término (por ejemplo 'deudor inhabilitado' no en sentido jurídico). Las legislaciones de Argentina, Brasil, Colombia, Ecuador, Guatemala y Paraguay así como la de Portugal lo regulan expresamente.

El *habeas data* 'reservador' pretende asegurar que el dato no sea conocido por cualquiera y se mantenga confidencial. Suele utilizarse para los datos sensibles que deben ser almacenados o para los que integran el secreto de Estado. Argentina, Perú y Portugal los regulan constitucionalmente.

El *habeas data* 'cancelatorio' persigue eliminar el dato del archivo y procede cuando con la reserva o confidencialidad no puede protegerse suficientemente —datos sensibles, fórmulas peligrosas— o cuando ya no tiene sentido el almacenamiento del dato porque a la sociedad no le trae ningún beneficio. Legislaciones como la de Argentina, Ecuador y Paraguay regulan este tipo.

Hasta aquí estos tipos y subtipos tienen reconocimiento constitucional, pero la jurisprudencia ha reconocido otros, como el *habeas data* 'impugnativo', cuando se tiende a cambiar una valoración equivocada de la información o la decisión informatizada. El 'bloqueador' cuando se solicita precautoriamente, hasta tanto se decida si procede el mantenimiento del dato o la cancelación definitiva. El 'disociador' persigue la transformación de un dato para que no se reconozca el sujeto a que se refiere. El derecho de que el dato esté seguro es un principio que rige en esta área, al punto que las regulaciones exigen que se utilicen los procedimientos técnicos para evitar que haya fugas no autorizadas. A veces se ejerce el *habeas data* en función 'ase-

guradora', para que el juez evalúe si se utilizaron los medios técnicos idóneos para evitar la utilización del dato por quienes no están autorizados. Se denomina *habeas data* 'reparador' a la acción que se entabla para que se ordene indemnizar el daño causado, junto con el 'disociador' van siempre acompañados de otras finalidades, como que muestre el dato o se rectifique, o cualquiera de los otros.

Otro punto en el que difieren las regulaciones es respecto de quién es el sujeto activo, si la persona física o individual o también las personas jurídicas. En función a la inclusión de ambas o sólo de los primeros se puede analizar la conveniencia de proteger un derecho u otro. Si se protege la intimidad o privacidad se deja afuera a las personas jurídicas respecto a quienes no se les reconoce. A su vez el aspecto protegido en las personas jurídicas es en general y exclusivamente el económico. Lo cierto es que por ejemplo en España, Alemania, Francia e Irlanda, se excluye de la protección a estas personas. En cambio Suiza, Austria, Dinamarca, Luxemburgo y Noruega lo admiten en lo que se refiere al aspecto económico. Las Naciones Unidas permiten a los Estados contratantes que apliquen la protección a las personas jurídicas (Puccinelli, O. 1999).

¿La protección se brinda a los llamados 'datos sensibles' o a todos? Algunas legislaciones y jurisprudencias entienden que lo que debe protegerse son los datos de la persona que hacen referencia a su ideología, religión, color, creencias, etc., denominados 'sensibles' y que de ser tenidos en cuenta pueden implicar violación de derechos humanos y discriminación. Pero otros entienden que con el cruce de datos y la ausencia de seguridad en su utilización, la información veloz que permite la informática transforma a cualquier dato en sensible y requiere por ende de protección[45]. Algunas legislaciones consagran el derecho a la oposición de la divulgación del dato (Francia), a veces se exige el consentimiento de la persona para su divulgación (España). Si es dato crediticio exigen que la deuda sea cierta, impaga y ya requerida por el acreedor. Si son registros privados deben registrarse y contar con prueba de que los datos almacenados responden a la realidad[46].

---

45 *Lascano Quintana, Guillermo c. Veraz S.A.,* Cámara Nacional de Apelaciones en lo Civil (Argentina), sala D, 23 de febrero 1999 (La Ley,. ADLA XXVI-C, 1491). Nota al fallo por Santos Cifuentes (1999); Rabinovich-Berkman, *Cuestiones actuales en derechos personalísimos*, Dunken, 1997 y *Derecho Civil. Parte General*, Astrea, 1999.

46 LORTAD.

Hay países que cuentan con una ley específica de *habeas data,* como por ejemplo: Argentina, Chile, España, Bolivia. Otros no la tienen, no obstante la doctrina y la jurisprudencia construyen en general un sistema tuitivo a través de la aplicación de otras normas constitucionales y de nivel legislativo o reglamentario. Se utiliza unas veces el recurso de la garantía de amparo y, otras, el de *habeas hábeas* (Pierini, A.; V. Lorences y M. I. Tornabene 1999) (Sosa, R. 2000) (Antik, A. y R. Rammuno 2000) (Slaibe, M. y C. Gabot 2000).

Riesgos y violaciones

Los conflictos más relevantes se relacionan no tanto con la acumulación de información en papel, como lo han venido haciendo los Registros Civiles de casi todos los países sin que se presentaran violaciones, los problemas se derivan del tratamiento automatizado de estos bancos de datos y de la potencia de los 'motores de búsqueda'. En este sentido las tendencias legislativas más avanzadas son las europeas:

Directiva 95/46/CE del Parlamento Europeo y del Consejo de Europa

Sección ii · Principios relativos a la legitimación del tratamiento de datos

Artículo 7. Los Estados miembros dispondrán que el tratamiento de datos personales sólo pueda efectuarse si:

- *el interesado ha dado su consentimiento de forma inequívoca, o*
- *es necesario para la ejecución de un contrato en el que el interesado sea parte, o para la aplicación de medidas precontractuales adoptadas a petición del interesado, o*
- *es necesario para el cumplimiento de una obligación jurídica a la que esté sujeto el responsable del tratamiento, o*
- *es necesario para proteger el interés vital del interesado, o*
- *es necesario para el cumplimiento de una misión de interés público o inherente al ejercicio del poder público conferido al responsable del tratamiento o a un tercero a quien se comuniquen los datos, o*
- *es necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, siempre*

que no prevalezca el interés o los derechos y libertades fundamentales del interesado que requieran protección con arreglo al apartado 1 del artículo 1 de la presente Directiva.

Sección III · Categorías especiales de tratamientos

Artículo 8. Tratamiento de categorías especiales de datos

1. Los Estados miembros prohibirán el tratamiento de datos personales que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, así como el tratamiento de los datos relativos a la salud o a la sexualidad.

2. Lo dispuesto en el apartado 1 no se aplicará cuando:

a el interesado haya dado su consentimiento explícito a dicho tratamiento, salvo en los casos en los que la legislación del Estado miembro disponga que la prohibición establecida en el apartado 1 no pueda levantarse con el consentimiento del interesado, o

b el tratamiento sea necesario para respetar las obligaciones y derechos específicos del responsable del tratamiento en materia de Derecho laboral en la medida en que esté autorizado por la legislación y ésta prevea garantías adecuadas, o

c el tratamiento sea necesario para salvaguardar el interés vital del interesado o de otra persona, en el supuesto de que el interesado esté física o jurídicamente incapacitado para dar su consentimiento, o

d el tratamiento sea efectuado en el curso de sus actividades legítimas y con las debidas garantías por una fundación, una asociación o cualquier otro organismo sin fin de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que se refiera exclusivamente a sus miembros o a las personas que mantengan contactos regulares con la fundación, la asociación o el organismo por razón de su finalidad y con tal de que los datos no se comuniquen a terceros sin el consentimiento de los interesados, o

e el tratamiento se refiera a datos que el interesado haya hecho manifiestamente públicos o sea necesario para el reconocimiento, ejercicio o defensa de un derecho en un procedimiento judicial.

3 El apartado 1 no se aplicará cuando el tratamiento de datos resulte necesario para la prevención o para el diagnóstico médicos, la prestación de asistencia

sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos sea realizado por un profesional sanitario sujeto al secreto profesional sea en virtud de la legislación nacional, o de las normas establecidas por las autoridades nacionales competentes, o por otra persona sujeta asimismo a una obligación equivalente de secreto.
3 Siempre que dispongan las garantías adecuadas, los Estados miembros podrán, por motivos de interés público importantes, establecer otras excepciones, además de las previstas en el apartado 2, bien mediante su legislación nacional, bien por decisión de la autoridad de control.
5 El tratamiento de datos relativos a infracciones, condenas penales o medidas de seguridad, sólo podrá efectuarse bajo el control de la autoridad pública o si hay previstas garantías específicas en el Derecho nacional, sin perjuicio de las excepciones que podrá establecer el Estado miembro basándose en disposiciones nacionales que prevean garantías apropiadas y específicas. Sin embargo, sólo podrá llevarse un registro completo de condenas penales bajo el control de los poderes públicos. Los Estados miembros podrán establecer que el tratamiento de datos relativos a sanciones administrativas o procesos civiles se realicen asimismo bajo el control de los poderes públicos.
6 Las excepciones a las disposiciones del apartado 1 que establecen los apartados 4 y 5 se notificarán a la Comisión.
Los Estados miembros determinarán las condiciones en las que un número nacional de identificación o cualquier otro medio de identificación de carácter general podrá ser objeto de tratamiento.

Al efecto de la clasificación de los riesgos o violaciones es interesante distinguir cuando éstos se generan como consecuencia de un banco de datos o no.

Generación primaria de bases de datos

Los archivos no automatizados son lentos, tienen permanencia y facilidad para conocer y, eventualmente, corregir los datos. Los sistemas de información —bases de datos con tratamiento informático— tienen rapidez, interconexión y falta de permanencia, por eso no permiten rectificar fácilmente los errores, situación que se complica aun más por la velocidad con que se difunden y duplican.

La generación de bases de datos aporta beneficios muy importantes pero también acarrea riesgos. Para evitar esos riesgos los sistemas de defensa o modelos de protección que se han establecido en los diferentes países son: (i) el judicial (ej. EE. UU.), que repara el daño *ex post facto*, en estos sistemas la actividad de organismos de vigilancia es meramente complementaria; (ii) el administrativo, en el que se le dan funciones jurisdiccionales a la administración pública, se utiliza mucho en Europa (España, Suecia, Alemania), donde se han establecido entidades especializadas con administraciones independientes a las que se les otorgan poderes sancionatorios; y, (iii) el mixto que instaura un equilibrio entre el administrativo y el judicial. Asimismo, los mecanismos de control y protección pueden funcionar en el nivel preventivo o represivo.

Es necesario distinguir los registros públicos de los registros privados. Los bancos de datos públicos son aquellos que obran en organismos del Estado, suelen ser reservados o con carácter secreto. Por ejemplo, en Argentina la ley 11.801 del Registro de la Propiedad Inmueble; la ley 22.617 del Registro de Reincidencia y Estadística Criminal; y la ley 17.622 del INDEC contiene información secreta con fines estadísticos.

En este punto se juega el tema de quiénes son los sujetos obligados al cumplimiento de los requisitos impuestos por las leyes, y respecto de los que se instauran los mecanismos de protección sean preventivos o sancionatorios, es decir los responsables en caso de daño por la utilización del dato. En las regulaciones del área de Brasil y Guatemala se restringe su aplicación a los bancos o registros públicos; en cambio, Colombia, Argentina, Perú y Ecuador incluyen también a los privados.

El principio fundamental al momento de definir y administrar un sistema de información es la 'finalidad'. Todo sistema de información persigue una finalidad, debe diseñarse minimalmente para lograr ese fin y no deberá utilizarse en el futuro para otros fines. La finalidad debe ser explícita, por ejemplo en Trinidad y Tobago la *Liquor Licences Act* de 1980, dice: *"For the purposes of this Act, every holder of a hotel spirit licence or special hotel licence under this Act shall keep a register in which…"*. En base a la finalidad deben, por ejemplo, estar regulados los plazos en relación a los que se permite guardar la información en las bases de datos (5, 7, 10 años).

Los derechos que se protegen con estas regulaciones, a veces mencionados por la ley y en otros casos deducidos en la interpretación doctrinaria y judicial, son amplísimos. En la suma de países, se abarca a todos los personales: derecho a la vida, intimidad, a la privacidad, al nombre, a la dignidad, al honor, a la integridad, a la libertad de conciencia, a la personalidad virtual, a los datos personales, a la autodeterminación informativa. El Consejo de la Unión Europea habla de "protección de las libertades y... del derecho a la intimidad en lo que respecta al tratamiento de los datos personales". También se lo denomina como derecho 'de dominio sobre datos personales' y empieza a considerarse como un derecho personalísimo autónomo. Algunos fallos y doctrinas en Argentina, considerados innovadores, lo consideran como derivado de la dignidad humana, mencionándose que es más que la sola intimidad o imagen el honor o identidad y abarca sus aspectos patrimoniales. Deriva de un fenómeno tecnológico y social"[47]. Se lo puede llamar 'derecho personalísimo a los datos personales', 'derecho a la autodeterminación informativa', 'a la libertad informática', 'derecho personalísimo de dominio de los datos personales'.

Administración de Justicia

El punto de partida es que la administración de justicia debe ser transparente, la publicidad de las actuaciones y de las decisiones es uno de los pilares del sistema y el conocimiento de los precedentes permite el respeto del principio de igualdad ante la justicia (Cadoux, L. 1994: 157-171). En este orden de ideas la información que se origina o procesa judicialmente o administrativamente puede tener diferente entidad y valor. Sin embargo, la información que normalmente es incluida en los sistemas de información podría distinguirse como procesal o jurisprudencial.

Los sistemas de seguimiento de causas son estrictamente necesarios para una eficiente administración de justicia. Paulatinamente se han reemplazado los Libros de Registro de los juzgados por sistemas computarizados que están cada vez más centralizados. En estos sistemas no sólo se registran una

47 *Lazcano Quintana, Guillermo c. Veraz S.A.,* Cámara Nacional Civil, sala D, 23 de febrero de 1999; *Urteaga, Facundo R. c. Estado Mayor Conjunto de las Fuerzas Armadas,* Corte Suprema, 15 de octubre 1998. Ver Santos Cifuentes (1999).

gran cantidad de datos personales sino que es posible relacionar a esas personas con hechos, conflictos de intereses o con delitos. También es creciente la tendencia a crear expedientes electrónicos en los que está registrada prácticamente la totalidad de la información que se relaciona con un caso (incluidos víctimas, testigos, abogados, peritos). Esta tendencia es sin duda la forma de lograr que la administración de justicia sea rápida y eficiente, sin duda un derecho ampliamente reclamado. Todos los datos judiciales en soporte informático (excepto la sentencia) deberían ser considerados confidenciales y su finalidad debe restringirse a la Administración de Justicia; por ello, los sistemas de justicia deberían garantizar con la mayor seguridad que los datos no puedan ser manipulados ni sustraídos. El acceso a la inspección visual de los expedientes y documentos en papel no debería ser restringido salvo que la ley lo disponga.

Se presentan varios tipos de violaciones:

i) Las empresas que venden información sobre antecedentes crediticios obtienen y utilizan los registros de los juzgados en materia comercial.

ii) En los juzgados en materia laboral se reciben pedidos de empresas que seleccionan personal interesadas en conocer la existencia de demandas laborales iniciadas por un potencial candidato a cubrir un puesto.

iii) En los juzgados en materia civil se han presentado pedidos con las mismas características, por ejemplo, para averiguar si una persona, potencial arrendataria, ha sido desalojada en el pasado.

En todos estos casos se intenta predecir la conducta futura, pensando que quien fue parte en un conflicto o ejerció sus derechos en el pasado mantendrá en el futuro esa actitud (Cappelletti, M. y B. Garth 1988). Si bien la información judicial es pública, los sistemas de información creados con la finalidad de agilitar la administración de justicia no deberían estar al servicio de intereses de terceros no relacionados con la justicia del caso.

La situación con las sentencias judiciales y los sistemas de acceso a la jurisprudencia es distinta. La publicidad de los precedentes es la garantía del principio de igualdad de todos los ciudadanos ante la ley. Por esta razón, y salvo que la ley determine lo contrario, las decisiones judiciales deben ser

públicas y deben instrumentarse todos los medios posibles para que sean accesibles (Rotunda, R. 1995: 119-127).

El problema presenta algunas dificultades. Las sentencias judiciales contienen muchos datos personales y revelan hechos que caen dentro de la esfera privada. La finalidad de garantizar la igualdad ante la ley no requiere que estos datos puedan encontrarse utilizando un motor de búsqueda, pero sí es deseable que las decisiones estén expuestas al escrutinio público —por ejemplo la prensa— y que puedan ser elogiadas o criticadas. Muchas revistas y proveedores de jurisprudencia en Internet han comenzado a tomar algunos recaudos. Se suprimen selectivamente algunos datos personales (generalmente los nombres de las partes en el conflicto, de los testigos, de los abogados y en algunos casos también el nombre del juez); se parte del concepto de que es necesario divulgar la lógica y los fundamentos de la decisión, y no el conflicto personal y particular. Finalmente, una vez identificada una sentencia por su contenido jurídico (sea sobre los hechos o sobre el derecho) el acceso a los datos personales es casi siempre posible concurriendo al juzgado y pidiendo el libro de sentencias. La búsqueda que se quiere evitar es la que persigue identificar casos judiciales en los que una persona determinada esté envuelta.

La tendencia a suprimir datos personales es el resultado de un equilibrio entre los derechos de intimidad y privacidad y los de igualdad ante la ley, en algunos casos los nombres personales se reemplazan por iniciales, en otros casos se suprimen partes de la sentencia que no hacen a la decisión de fondo (por ejemplo: la regulación de honorarios de los abogados y peritos). Sin embargo, la operación de suprimir datos personales tiene un costo adicional significativo. Este tema divide a las revistas y proveedores de jurisprudencia. Algunos sólo eliminan los nombres en algunos casos, otros en todos los casos (por ejemplo: Aranzadi en España). También existen proveedores que no los eliminan, salvo que la ley específicamente prohíba la difusión, y permiten el uso de nombres en el buscador (por ejemplo: en Brasil el Tribunal de Justiça do Distrito Federal e Territorios, el Sistema Costarricense de Información Jurídica y en EE. UU. los proveedores Lexis y West Law). El 8 de marzo de 2001 se interpuso un recurso de protección ante la Corte de Apelaciones de Santiago, el motivo se relaciona con el 'buscador' del sitio en Internet (www.poderjudicial.cl), recientemente inaugurado, en el que una persona al introducir su nombre en el sistema de búsquedas —estado de

causas de Santiago— comprobó que aparecían los datos de una demanda que tenía interpuesta por la reclamación de paternidad de su hija[48].

Salud

En el ámbito de la salud, la creación de bases de datos o sistemas de información que contengan las recetas o prescripciones médicas, o que faciliten el acceso a datos clínicos personales, podría considerarse como un riesgo. El acceso a esta información es otro tema que ha suscitado controversias, en particular porque puede ser el fundamento de preconceptos o actitudes discriminatorias. W. Brennan (miembro de la Corte Suprema de los Estados Unidos) opinó en el caso *Whalen vs. Roe,* 429 US 589, 607 (1977), en el que se cuestionaba la constitucionalidad de una ley de Nueva York que establecía el registro obligatorio de todas las recetas médicas en una base de datos centralizada: "*The central storage and easy accessibility of computerized data vastly increase the potential for abuse of that information, and I am not prepared to say that future developments will not demonstrate the necessity of some curb on such technology".* La situación no ha cambiado mucho. La reciente *Health Security Act* en los EE. UU. reconoce la necesidad de reglas estrictas para administrar la información sin vulnerar la privacidad. En ella se enuncian algunos 'principios': (i) es necesario definir y limitar cuando una consulta está autorizada; (ii) se requiere que sólo la 'mínima cantidad de información necesaria' sea recuperada; (iii) se reconoce el 'derecho a conocer' quién tiene información sobre una persona, y (iv) el 'derecho de acceso' a tal información, a copiarla y a ser notificado de todas las correcciones o modificaciones (Shapiro, R. y G. Annas 1994: 10-36). También se ha detectado que empresas que se dedican al marketing compran a las farmacias las prescripciones médicas ya utilizadas y las ingresan a bases de datos, estos datos se usan para realizar análisis estadísticos sobre las tendencias en el uso de medicamentos; si bien no se estarían registrando los nombres de los pacientes, sí se registran los nombres de los médicos y se determinan sus preferen-

48 El recurso fue presentado por la Red Latinoamericana de Mujeres Transformando la Economía (REMTE-Chile) y la Red Nacional Género, Comercio y Derechos Humanos contra la Corporación Administrativa del Poder Judicial. Ver Germán J. Bidart Campos (1992: 415).

cias al efecto de enviarles visitadores médicos. Los destinatarios de estos estudios serían los grandes laboratorios farmacéuticos.

La existencia de bases de datos con historias clínicas, donantes de sangre[49], vacunaciones se ha generalizado en los últimos años, la información es sensible y debería estar protegida. También muchas instituciones hospitalarias han comenzado a colocar las historias clínicas en Internet.

La condición de portador del virus HIV-SIDA puede requerir una protección especial de la privacidad. En Argentina, la Ley de Prevención y Lucha contra el Síndrome de Inmunodeficiencia Adquirida (SIDA) (ley 23.798 de 1990) establece que en ningún caso se podrá "individualizar a las personas a través de fichas, registros o almacenamiento de datos, los cuales, a tales efectos, deberán llevarse en forma codificada" a tal efecto "se utilizará, exclusivamente, un sistema que combine las iniciales del nombre y del apellido, día y año de nacimiento. Los días y meses de un sólo dígito serán antepuestos del número cero (0)". Por ejemplo, en los expedientes judiciales al mencionar un portador de HIV, su nombre es reemplazado por un número, también en los documentos en papel. Por aplicación de la misma ley la revista El Derecho publica los casos judiciales sin utilizar las iniciales de los nombres del portador de HIV, se utiliza en su lugar las letras 'N.N.'. El Supremo Tribunal de Justicia de Venezuela en "NA y otros" ha definido su posición sobre la privacidad y el SIDA[50].

En *N.N. c. Estado*[51], se concede una indemnización por el daño moral causado por la discriminación de un funcionario afectado de HIV-SIDA, aun cuando no hubo difusión de los resultados del examen, no parece que el Estado empleador hubiere cumplido con la obligación de confidencialidad. Se fija el daño moral en 14.000 USD ciertamente el valor más alto observado en América Latina durante la presente investigación.

En Chile se ha presentado un caso difícil de remediar legal o judicial-

---

49 Por ejemplo en Argentina la Ley 22.990 del Sistema Nacional de Sangre, y en Venezuela la Ley de Transfusión y Bancos de Sangre (1977).

50 "La garantía del derecho a la no discriminación no se logrará si ellos mismos —resguardándose en la privacidad— se aislasen, se apartasen de sus actividades, ocultasen sus propios padecimientos o se sintiesen culpables cuando en realidad no hay razón para ello. La privacidad es un derecho de todos, y siempre que sea solicitado el carácter reservado de las actuaciones que se lleven a cabo en casos similares, la Sala tomará en cuenta las razones que se le expongan".

51 Juzgado Contencioso Administrativo de Montevideo –1er. turno– 1997, 1 *Lex* (1997) 17-27.

mente. Vivo Positivo es una asociación de autoayuda de los portadores de HIV. Los registros de los miembros de esa asociación llegaron a manos de una empresa que ofrece servicios funerarios, que envió a cada uno de los asociados una carta invitándolo a contratar sus servicios. Para establecer una violación sería necesario demostrar que la empresa envió ese tipo de cartas a portadores de HIV con mayor frecuencia que a otro tipo de personas. Este tipo de prueba estadística es inexistente en los tribunales latinoamericanos.

En el ámbito de los seguros, la información sobre salud permite establecer inferencias sobre riesgo de contraer enfermedades, o sobre la esperanza de vida. Por esta razón esta información podría ser utilizada por las compañías de seguros para negarse a dar cobertura ya sea de seguros de vida, de asistencia médica o de retiro[52].

Las bases de datos genéticos son sin duda el problema del futuro (Annas, G. J. 1999: 9-11) (Roche, P. 1996: 1-11). En Trinidad y Tobago se ha sancionado el año 2000 la *Deoxyribonucleic Acid (DNA) Identification Act*, por la que se crea una base de datos genéticos personales, compulsiva para personas que hayan sido declaradas culpables por una corte de apelaciones y para aquellas personas que presten su conformidad[53].

Infancia

Existe una fuerte tradición en las legislaciones americanas de proteger los nombres y las imágenes de niños y adolescentes en las publicaciones de la prensa, en especial cuando se trata de víctimas o adolescentes infractores de la ley penal[54]. Sin embargo, en algunos países los sistemas nacionales de pro-

52 La Corte Suprema de Costa Rica en *M. J. J. c. Instituto Nacional de Seguros* ha denegado un amparo sosteniendo que: "En efecto, no se trata de una discriminación ilegítima, sino de una diferenciación razonable, si se establecen condiciones distintas –en cuanto a primas o beneficios– para personas con ciertas limitaciones funcionales, como cuando así se actúa con motivo de la edad de un solicitante del servicio. El trato desigual, en estos casos, obedece a razones obvias, por manera que no es dable aceptar la tesis del recurrente de que él está en igualdad de condiciones que otras personas sin su problema físico y que como tal debe tratársele". Este punto de vista le resta al sistema asegurador su función eminentemente social. Por otra parte, el número de variables a discriminar en el cálculo de las primas debe ser limitado, pues de otra forma el tamaño de las sub-poblaciones se reduciría significativamente y el mismo concepto de 'seguro' perdería eficacia.

53 La sección 39 subsección 2 incluye también a quienes han sido condenados dentro de los cinco últimos años o a quienes tengan una causa pendiente.

54 *Privacy and Juvenile Justice Records: a mid-decade status report*, Bureau of Justice Statistics, EE.UU., 1997.

tección a la infancia entendieron ventajoso el desarrollo de sistemas de información en los que se almacenan datos personales, de salud, infracciones o situaciones de riesgo de niños que estuvieron en programas de atención. Este tipo de registros tuvo su fundamentación en la posibilidad de realizar un seguimiento individualizado –que en definitiva redunda en beneficio de los niños– y en la realización de estudios estadísticos e investigación que incidirían directamente en las tareas de planificación y diseño de políticas[55]. Sin embargo, no parece haber un adecuado equilibrio entre los objetivos de estos sistemas y las tendencias sobre protección de datos personales (Gregorio, C. 1999). Tampoco las normas de seguridad alrededor de estos sistemas han sido consideradas siempre prioritarias, ni están claras las sanciones penales para quienes violen la seguridad y confidencialidad de los datos[56].

En *S., V. v. M., D. A.*[57] se afirma que cuando están en conflicto el derecho a la intimidad de un niño y el de expresión cabe entenderse que la protección judicial del interés superior del niño debe estar estrictamente ceñida a lo que resulta indispensable, para evitar así una injustificada restricción de la libertad de prensa, ya que el derecho de prensa, reconocido como derecho de crónica en cuanto a la difusión de noticias que conciernen a la comunidad como cuerpo social y cultural, requiere para su ejercicio que las restricciones, sanciones o limitaciones deban imponerse únicamente por ley y su interpretación deba ser restrictiva.

Los procedimientos de adopción son generalmente secretos y en algunos países inclusive se destruyen los documentos relativos a la filiación biológica, sin embargo existen en Internet sitios destinados a recuperar los vínculos biológicos[58].

Los registros escolares presentan también una posibilidad de discriminación. En los EE. UU. las acciones disciplinarias por violación de las reglas escolares son consideradas registros escolares y están protegidos por la *Family Educational Right to Privacy Act (FERPA)*[59].

---

55 En América Latina y el Caribe estos sistemas fueron promovidos por el programa SIPI del Instituto Interamericano del Niño de la Organización de Estados Americanos (www.iin.org.uy).

56 Algunas normas de seguridad han sido incluidas en el nuevo Proyecto de Código de la Niñez y Adolescencia del Uruguay, artículos 11, 22 inc.F, y 211 a 215.

57 *S., V. v. M., D. A.* medidas precautorias, filiación. Corte Suprema de Justicia de Argentina, 3 de abril de 2001.

58 Adoption Records Database (http://www.skylace.net/adoption).

59 20 US Code section 1232g.

Se presentan, en general, pocos conflictos sobre violaciones de la privacidad de los niños por sus padres, sin embargo la compañía estatal de teléfonos de Uruguay (ANTEL) difundió una publicidad en la que resaltaba, entre los usos del identificador de llamadas telefónicas, la posibilidad de "controlar las amistades de un hijo adolescente". Varias legislaciones, por ejemplo en Francia, establecen una edad a partir de la cual los niños tienen cierta privacidad con respecto a sus padres, y la Ley de Protección de Niños y Adolescentes de Venezuela establece normas sobre la confidencialidad de la correspondencia. En los EE. UU. se ofrece en Internet la posibilidad de detectar el consumo de drogas en un adolescente a partir de una muestra de cabello, que generalmente es tomada por sus padres sin su consentimiento[60].

Otras bases de datos acumulan información sobre adultos pero están relacionadas con los niños. En los EE. UU. se han desarrollado bases de datos nacionales con los datos personales de los padres que han incumplido sus obligaciones alimentarias. Estas bases de datos interactúan con las instituciones bancarias para restringir sus operaciones. El procedimiento ha recibido una crítica considerable (Schwartz, P. 1992: 1321-1389). En Argentina existe un proyecto de ley para crear un Registro Nacional de Deudores Alimentarios, que ya existe en algunas provincias[61]. También en los EE. UU. varios estados mantienen bases de datos de personas con sospechas de abuso infantil[62].

Otros registros estatales

Los Registros Civiles –quizás los registros más antiguos– se basaron generalmente en 'índices' que se anexaban a cada libro de registro, que generalmente se correspondían con el año calendario. Este sistema ofrecía un mecanismo de búsqueda eficiente pero limitado en la medida en que eran necesa-

60 Algunos sitios son (www.drugtestwithhair.com) y (www.drugfreeteenagers.com).

61 La leyes de Neuquen y la ciudad de Buenos Aires prevén la prohibición de salir del país hasta tanto el deudor satisfaga la prestación alimentaria. Otros ordenamientos han adoptado también esta restricción, por ejemplo: artículo 90 de la Ley Orgánica de Defensa del Niño de Colombia, artículo 220 del Código del Niño del Uruguay.

62 Ver *Hodge v. Jones*, 31 F3d 157, *cert. denied* 115 S.Ct. 581 (1994) y Joni JONES, 'Maintaining Unsubstantiated Recors of "Suspected" Child Abuse: much ado about nothing or a violation of the right of privacy?', 1995 *Utah Law Review* (1995) 887-912.

rios datos sobre el año y el lugar del hecho (por ejemplo: nacimiento, matrimonio, defunción, etc.). La transformación de los Registros Civiles en bases de datos automatizadas y centralizadas permitiría hacer búsquedas sobre filiación, homónimos y otras que pueden dar lugar a violaciones a la intimidad o generar riesgos.

Los registros electorales contienen datos personales y algunos extremadamente sensibles como son la afiliación a un determinado partido político (ejemplo: Argentina). También se ha observado que algunos países (por ejemplo: República Dominicana y Venezuela) han creado sitios en Internet capaces de desplegar información personal correspondiente a un determinado número de cédula de identidad.

Los Registros de Antecedentes Penales almacenan sentencias judiciales firmes y están en la mayoría de los países regulados por normas específicas, son confidenciales y administrados por el Estado. Sin embargo, la información es muy sensible y existe el riesgo de que estos registros sean reemplazados por registros policiales de aprehensiones. En El Salvador la Ley del Menor Infractor le prohíbe a la policía mantener este tipo de registros sobre niños y adolescentes.

Los movimientos migratorios entre países son cada vez más registrados. Los antiguos formularios en papel están siendo reemplazados por nuevos de reconocimiento óptico y también se está generalizando la lectura automática de los documentos de identificación personal. Estos registros migratorios contienen información sensible sobre datos personales y la vida privada. No resulta claro cuál es la 'finalidad' para la que se generan estas bases de datos.

En Ecuador existe una base de datos que lleva el Consejo Nacional de Control de Sustancias Estupefacientes y Psicotrópicas (CONSEP) en la que se registran infracciones tipificadas en la Ley de Sustancias Estupefacientes y Psicotrópicas[63].

La decisión del Superior Tribunal de Justicia de Venezuela en el caso *R.C.M. y otros v. Consejo Nacional Electoral* (2000) es muy significativa, pues establece un límite al concepto de transparencia de la información estatal y al concepto de *Habeas data*: "...lo solicitado por las pretensiones no es el ac-

63 En *P.M.D.J. c. CONSEP,* un recurso de *Habeas data* presentado ante el Tribunal Constitucional de Ecuador, se acordó suprimir al accionante del listado por haber sido derogado el artículo de la ley que tipificaba y sancionaba el delito por tenencia de pequeñas dosis.

ceso a los archivos y registros administrativos, sino que se les otorgue información electoral digitalizada relacionada con los resultados obtenidos en todas y cada una de las mesas de votación que funcionaron en las respectivas jurisdicciones electorales y de manera [sic] discriminada; mesa por mesa". Esta decisión permite distinguir que transparencia y derecho a la información no implican el acceso (o búsquedas) a registros informatizados del Estado, ya que la finalidad con que fueron desarrollados se corresponde solamente con funciones estatales. No existe por tanto un derecho a obtener copias de los registros públicos. En Trinidad y Tobago la *Freedom of Information Act* de 1999 y en los EE. UU. la *Freedom of Information Act* de 1996 le dan a los ciudadanos el derecho (con excepciones) de acceder a documentos oficiales. En la sección 30 de la ley de Trinidad y Tobago se excluyen los documentos que pudieran afectar la privacidad personal, también se excluyen otros documentos por razones de Estado. Igualmente en *Bruno F. Villaseñor*[64], se entiende que el derecho a la información consagrado en la última parte del artículo 6° de la Constitución Federal no es absoluto, su ejercicio se encuentra limitado tanto por los intereses nacionales y de la sociedad, como por los derechos de terceros (por ejemplo, a la privacidad).

Personas con discapacidad y sus familias

En varios países (por ejemplo: Chile, Ecuador, México, Uruguay) existen registros de las personas con algún tipo de discapacidad, en algunos casos son oficiales y en otros son generados por asociaciones de autoayuda (por ejemplo: la Asociación Down del Uruguay). La inclusión o no en estos registros facilita la obtención de ciertos beneficios sociales o subsidios. Pero también estas bases pueden ser motivo de discriminación o, por ejemplo, dificultades para acceder a seguros de vida o realizar aportes a sistemas jubilatorios privados (ejemplo: El Salvador).

64 Amparo en revisión ante la Corte Suprema de México, 2000. *Semanario Judicial de la Federación y su Gaceta*, tomo XI, Abril de 2000, tesis P. LX/2000, pag. 74.

Identificación personal

Los sistemas de identificación personal comienzan a tener la posibilidad de almacenar gran cantidad de información innecesaria a los efectos de la identificación y en muchos casos desconocida para el propietario del documento. En Venezuela está a punto de introducirse un nuevo sistema de documentos de identificación. Si bien no se conocen aún los detalles de la implementación, el pliego de la licitación realizada por el gobierno venezolano incluía la existencia de una enorme base de datos biométrica de huellas dactilares y un *chip* inserto en el documento con información aún no especificada y legible por proximidad (es decir desde un dispositivo que no necesita contacto con el documento). Este tipo de documento será asignado a los recién nacidos en Malasia, con la aprobación de los padres les será asignada una tarjeta con un *chip* de memoria que incluirá número, nombre, nombre de los padres y *status* de ciudadanía[65].

Información ilegible para el propietario del documento se encuentra en forma de códigos de barras en los documentos de identidad de Costa Rica y República Dominicana. En Filipinas, además de información como código de barras (incluida la biométrica de huellas), el documento llamado SS-ID (Social Security ID), tiene una barra magnética que permite leer, en los 'kioscos de información', las contribuciones al Servicio de Seguridad Social del propietario y en el futuro permitirá realizar operaciones en ATM[66].

Sistemas de información sobre riesgo crediticio

Ciertamente, la falta de una legislación clara que regule esta actividad se traduce en violaciones a los derechos de privacidad e intimidad. La regla ideal es que sea obligatoria para el *Bureau* la verificación de cada dato que ingresa a la base, pero normalmente esta información es recibida informalmente de sus clientes y no está respaldada documentalmente. En este punto es interesante analizar el caso *Hoffman Fuenzalida, Luis c. Boletín de Informaciones Comerciales* pues trata un punto de singular importan-

65 'Govt to issue identity cards to newborn babies'. *The Star*, Malasia, 16 de marzo de 2001.

66 http://www.sss.gov.ph/other/othe5001.htm.

cia[67]. Al margen de la fundamentación en este caso, liberar al *Bureau* de todo tipo de responsabilidad civil por información errónea y trasladarla a la institución que originó el dato, es liberar al *Bureau* de todo incentivo para la calidad de información. Parece ciertamente contradictorio que la Corte Suprema de Costa Rica exija en *Félix Przedborski v. Mauricio Herrera y La Nación* (2001) verificar la veracidad de una fuente en Bélgica y hasta eliminar los *links* a un sitio en ese país —mediando la libertad de expresión— y por el contrario no sea requisito para un *Bureau* verificar la veracidad de la información, mediando derechos a la privacidad e intimidad. Ciertamente, la situación debería ser la contraria.

Otra situación de riesgo se debe a la falta y a las dificultades de controlar la información contenida en las bases de datos de los *Bureau*. Se ha observado que algunos de ellos no sólo contienen información crediticia sino también otros tipos de datos no necesariamente obtenidos en forma lícita (antecedentes penales, juicios laborales, infracciones de tránsito, perfiles de compra, etc.) y también han existido casos de venganzas personales instrumentadas ingresando información falsa en las bases de datos para perjudicar una persona (del Villar, R.; A. Díaz de León y J Gil Hubert 2000) (Miller, M. 2000).

Empleo

En el ambiente de trabajo el empleador puede monitorear las llamadas telefónicas de sus empleados con sus clientes por razones de control de calidad. En algunos casos debe advertirse con un mensaje grabado o un tono agudo que la comunicación está siendo grabada o monitoreada. En los EE. UU. la *Electronic Communications Privacy Act*, 18 *U.S. Code* 2510, et. seq. —la ley federal que regula las comunicaciones entre estados— permite el monitoreo no advertido de llamadas. También las llamadas internas entre empleados pueden ser monitoreadas. El empleador puede tener acceso al registro de teléfonos discados desde una extensión en particular. También pueden ser monitoreados discos magnéticos, el correo electrónico, el correo de voz y se

67 Corte Suprema de Chile, 1996, "Debe dirigirse el recurso de protección contra la Entidad Bancaria que informó sobre protestos aclarados mantenidos en el Boletín Histórico, y no contra este último, que actuó conforme a derecho".

colocan cámaras de vídeo en determinados lugares[68]. La privacidad en el ambiente laboral es bastante reducida, y el fundamento se relaciona con los procedimientos para aumentar la productividad, la prevención de robos, evitar la responsabilidad civil por actos de los empleados y prevenir el espionaje industrial o comercial. Unas de las pocas excepciones está en la *Employee Polygraph Protection Act* de 1988 que impide las pruebas con polígrafo.

Es difícil establecer un límite claro entre la información privada del empleado y la del empleador, pero en algunos extremos se tratarían de violaciones a la intimidad y privacidad. Para evitar estos conflictos algunos empleadores crean reglas internas.

También se ha discutido si el empleador puede obligar al empleado a someterse a exámenes médicos (ejemplo: HIV) o psicológicos. En muchos casos el empleador fundamenta su derecho por razones de seguridad.

Sin embargo la Suprema Corte de la República Dominicana en *Agromán Empresa Constructora S.A. v. B.P.*[69] entiende que pueden existir hechos de carácter personal y relacionados exclusivamente con su vida privada y no con su trabajo.

Bases de datos subproducto

Servicios telefónicos

Las empresas telefónicas guardan en sus bases de datos la relación de las llamadas recibidas y realizadas desde un teléfono. Estos datos pueden ser procesados y dar información sobre aspectos de la vida íntima de las personas. Si bien no se han detectado violaciones o demandas relacionadas con estas bases de datos, sí se han utilizado con orden judicial en investigaciones de

68 Existe software que es capaz de registrar toda la actividad realizada en una computadora, incluyendo, además de correo entrante y saliente, sitios web visitados, muestras periódicas de la pantalla y todo lo digitado en el teclado (*keystroke monitoring)*. Esta información es enviada secretamente a la computadora de quien espía de forma que el usuario no pueda borrar sus pasos.

69 Sentencia del 9 de septiembre de 1974, Boletín Judicial Nro. 766, páginas 2437-2444.

hechos delictivos (por ejemplo, en Argentina en la investigación del homicidio de José Luis Cabezas).

Los identificadores de llamadas no representan directamente una violación a la privacidad. Sin embargo, si son utilizados para que el propietario del teléfono establezca las llamadas que recibe otra persona (por ejemplo en hoteles, o los padres respecto de sus hijos) esto podría eventualmente ser considerado una violación. También se ha observado que algunas empresas que reciben solicitudes de servicio a través del teléfono utilizan los identificadores de llamadas para generar bases de datos de clientes. Por ejemplo, las empresas de radio-taxi disponen de archivos históricos sobre día, hora y lugar de destino de sus usuarios.

En algunos países (por ejemplo: Jamaica, Uruguay) es posible obtener el estado de la deuda (facturación de servicios) con la compañía telefónica sólo disponiendo del número telefónico. En Jamaica (Roxborouh, P. 1999) es un servicio automático que se obtiene discando el número 1-919-1919; en Uruguay se obtiene también el nombre del propietario de la línea telefónica en terminales públicas ubicadas en los locales de la compañía telefónica.

En base al *Communications Assistance for Law Enforcement Act* (CALEA) las compañías de telecomunicaciones estadounidenses deberán incluir en sus equipos de telefonía móvil la capacidad de conocer su posición con una precisión de 50 metros a los efectos de inteligencia (FBI) y de localizar llamadas a los servicios de emergencias (911). Incluso sin la existencia de estos dispositivos, en zonas densamente pobladas, es posible conocer, con una cierta precisión, la ubicación de un celular, esto se debe a que se sabe cual es la antena más cercana a él y en las ciudades hay antenas cada algunas decenas o cientos de metros.

Tarjetas de crédito

Las entidades emisoras de tarjetas de crédito disponen de bases de datos que no sólo permiten conocer el perfil de compras de una persona, sino también ubicarla en el tiempo y el espacio. Algunas de ellas utilizan esta información en tiempo real para prevenir fraudes. No se han detectado violaciones en relación con estas bases de datos, presumiblemente por los criterios de seguridad y reserva que aplican estas empresas. En términos de legislación pue-

de citarse en la Argentina la Ley de Tarjetas de Crédito (ley 25.065 de 1998), que les prohíbe dar información a los *Bureau* de crédito[70].

Perfil de consumidores

En muchos comercios se acostumbra a solicitar ciertos datos personales para almacenar el 'perfil del cliente', esta información en muchos casos se realiza también cuando la operación es al contado. Estas bases de datos se comparten y acumulan con otras generadas por otros comercios y dan lugar a invasiones a la privacidad, que generalmente consisten en ofrecer nuevos productos por correo, teléfono, e-mail, etc.

También se ha generalizado la realización de sorteos o concursos en los que los interesados en participar deben completar un cupón con datos personales. Estos datos son almacenados y relacionados, generalmente son utilizados o vendidos para la oferta telefónica de nuevos productos.

Riesgos no relacionados con bases de datos

Comunicaciones

La posibilidad de realizar intercepciones telefónicas es en muchos países una violación a los derechos de privacidad e intimidad. Existe aquí una importante distinción, si la intercepción se realiza con la orden de un juez o si la realiza la policía u otras fuerzas de seguridad, o particulares en forma generalizada.

---

70 Artículo 53. "Las entidades emisoras de Tarjetas de Crédito, bancarias o crediticias tienen prohibido informar a las 'bases de datos de antecedentes financieros personales' sobre los titulares y beneficiarios de extensiones de Tarjetas de Crédito u opciones cuando el titular no haya cancelado sus obligaciones, se encuentre en mora o en etapa de refinanciación. Sin perjuicio de la obligación de informar lo que correspondiere al Banco Central de la República Argentina. Las entidades informantes serán solidarias e ilimitadamente responsables por los daños y perjuicios ocasionados a los beneficiarios de las extensiones u opciones de Tarjetas de Crédito por las consecuencias de la información provista".

Este tipo de violaciones ha sido legislada en: Ecuador, Ley Especial de Telecomunicaciones (ley 184 de 1992) artículo 14; Venezuela, Ley Orgánica de Telecomunicaciones (2000) artículo 190. En República Dominicana por Resolución 80 del 2001 de la Suprema Corte de Justicia se instruye a los jueces sobre la Resolución 36-00 del Instituto Dominicano de las Telecomunicaciones (INDOTEL) que "considera interceptación ilegal de las telecomunicaciones toda participación directa e indirecta en la injerencia, interceptación, intervención, recepción, encomienda, permisión, espionaje, escuchas y provisión de medios, por su propia cuenta o por encargo de otro, sin autorización previa de un Juez del Poder judicial". En México la Corte Suprema en el caso *Fernando Karam Valle y otro, amparo directo*[71], estableció que "si la intercepción telefónica no estuvo precedida de una orden judicial, se trata de un acto inconstitucional y, por ende, nulo de pleno derecho en sí mismo y en sus frutos". En Jamaica[72] la legalidad de una intercepción telefónica hecha por la policía en la investigación de un delito se considera regulada por el precedente *Malone v. Commissioner for the Metropolitan Police (no.2)*[73].

También la jurisprudencia tiende a rechazar las pruebas (escuchas telefónicas) obtenidas ilegalmente: *In re Sergio F. Lezica*[74], se dice que no reviste va-

---

71 Semanario Judicial de la Federación, (1987) tomo 217-228 (7) pag. 75.

72 La Constitución de Jamaica no lo prohíbe expresamente, pero da un punto de partida para analizar las implicaciones legales [*cf.* section 22]. Al analizar los delitos bajo la *Telephone Act* of 1893, sección 20 es interesante ver cómo las lagunas axiológicas son comunes frente a nuevos delitos, y resultado de la aplicación de nuevas tecnologías; difícilmente están incluidos en los textos legislativos y –por lo general– son incluidos como violaciones a los derechos constitucionales.

73 [1979] Chancery Division 344, y [1979] 2 All ER 620. Ver Margaret Demeriex (1992: 306-313).

74 Cámara Nacional de Apelaciones en lo Criminal y Correccional (Argentina), sala VI, 1997. También es relevante la decisión *In re Manuel Gaggero*, (Cámara Nacional de Apelaciones en lo Criminal y Correccional Federal, 1999) en la que se reitera el criterio sentado por el tribunal en numerosos precedentes, en el sentido de que la prueba obtenida por un particular, aun sin el consentimiento de quien resulta involucrado, no contraviene norma constitucional o procesal alguna, sin perjuicio del valor probatorio, no es aplicable cuando quien así la obtiene es el propio Estado por intermedio de uno de sus órganos administrativos, por el cual trazó pautas investigativas y tomó una iniciativa que no le era propia. Esta irregular actividad investigativa desplegada por el Estado mediante la utilización de subterfugios tendientes a obtener información y pruebas de cargo de parte de las personas de las que se sospechaban comportamientos delictivos, es violatoria de principios constitucionales que determinan pautas mínimas del debido proceso legal y que son condición de validez de un eventual juicio de reproche. En el mismo sentido, la sentencia RHC10534 del Superior Tribunal de Justicia de Brasil "*a gravação de conversa por um dos interlocutores não configura interceptação telefônica, sendo lícita como prova no processo penal*", DJ 11/12/2000 pag. 218.

lidez ni eficacia probatoria la transcripción de la conversación telefónica, pues conforma una pieza espuria al haber sido obtenida de un modo subrepticio y, por lo tanto, en directa violación a la garantía de resguardo a la intimidad, que consagran los artículos 18 y 19 de la Constitución de la Nación Argentina.

Cuando la escucha se realiza a las comunicaciones efectuadas por personas privadas de libertad las soluciones son muy diferentes, en Brasil son consideradas ilegítimas y violatorias también del derecho de defensa, mientras que en Chile es considerado legal colocar micrófonos en las celdas atendiendo a temas de seguridad.

Internet

En el contexto de Internet existen algunas técnicas y prácticas que violentan la privacidad aunque en principio parezcan inofensivas (Vives, F. 2000: 1011-1024). El *spam* consiste en enviar correos electrónicos a una gran lista de personas, por lo general con fines publicitarios, pero también incluyen 'cadenas', peticiones, etc. Algunos proveedores de e-mail implementan filtros de *spam* aunque esto podría llegar a verse como otra intromisión.

Las *cookies* consisten en piezas de información que un servidor web puede almacenar en la computadora del usuario con el fin de 'recordar', por ejemplo, preferencias de éste. Sin embargo dichas *cookies* suelen pasar inadvertidas al usuario quien puede sufrir una especie de rastreo de sus visitas a un determinado sitio o, valiéndose de errores en los navegadores, de su actividad en la Red.

No existen reglas claras ni universales en lo que refiere a la asignación de 'nombres de dominio', por lo que se dan casos de personas dedicadas a registrar nombres de celebridades o empresas ya existentes como nombres de dominio con el fin de venderlos o desprestigiar a la persona o compañía. En algunos países estas situaciones las resuelve la justicia caso por caso y en otros la empresa que asigna los nombres de dominio se reserva el derecho de retirarlo si considera que se trata de una de estas situaciones (por ejemplo en Uruguay).

Algunos sitios de organismos del Estado permiten el acceso a información de carácter personal con sólo ingresar un número de documento de identidad. Sitios de este tipo son, por ejemplo: (www.bcra.gov.ar/esefaaaa.htm) del Banco Central de la República Argentina; (www.sri.go-

v.ec/html/ruc_consulta.html) del Servicio de Rentas Internas de Ecuador; (www.cne.ve/donde.asp) del Consejo Nacional Electoral de Venezuela; y, (www.jce.do/consultas/index.asp) de la Junta Central Electoral de República Dominicana. Estos sitios permiten el acceso público a datos personales.

Matrículas de los automóviles

En muchos países se ha observado que la información contenida en las placas de identificación de los automóviles no guarda estrictamente relación con la finalidad para la que fueron creadas. La inclusión del lugar de residencia del propietario es una información excesiva y revela un dato personal que puede eventualmente generar un riesgo adicional (por ejemplo, ser elegido para un robo). Se observa este problema en Brasil, México y Uruguay.

Existen también otras violaciones que muestran que el concepto de intimidad y privacidad es algo más amplio. En *Szewc, Andrés v. Carrefour Argentina S.A.*[75] se estableció que Carrefour S. A. había violado la intimidad del actor al permitir que éste fuera molestado en su domicilio por llamadas telefónicas de personas que pretendían comunicarse con el hipermercado, ya que en sus tiques y facturas figuraba erróneamente el teléfono del actor, y se acordó un daño moral de 3.500 USD. En *João Rodríguez v. Viernes Entretenimiento C.A.*[76] se afirma que "un ambiente con una marcada perturbación sónica, perjudica la salud y perturba la intimidad". En *Julia Vanessa Castro Sánchez v. Tercera Comisaría y otros*[77], se dice que "el hecho de fotografiar a una persona que transita por la vía pública, aun sin su consentimiento, no constituye delito; aunque la Sala estima que, conforme a los artículos 29 y 30 del Código Civil y 24 de la Constitución, sería una violación de sus derechos constitucionales a la personalidad y a la privacidad si la fotografía es publicada, reproducida, expuesta o vendida sin el consentimiento de la persona, salvo los casos allí enumerados relativos a la notoriedad pública de la persona o necesidades de justicia o policía". En *Rischmaui Grinblatt, Francisca c. Consorcio Periodístico de Chile S.A.*[78], se establece que:

75 Cámara Nacional Civil, sala E (1997), 1999-II *Jurisprudencia Argentina* (1999) 339-42.

76 Ver *Viernes Entretenimiento C.A. amparo*, Supremo Tribunal de Justicia de Venezuela, 2000.

77 Recurso de *Hábeas corpus,* Corte Suprema de Costa Rica, 1991.

78 Corte Suprema de Chile, recurso de protección, 1997. 468 *Fallos del Mes* 2055-2058

"El hecho de asistir a un lugar público, no implica el consentimiento para la divulgación de una fotografía tomada en dicho lugar".

Dispositivos y tecnologías que atentan contra la privacidad

La tecnología actual, soportada en gran parte por el aumento constante de la capacidad de cómputo y almacenamiento de información, está permitiendo elaborar dispositivos y procedimientos de vigilancia extremadamente poderosos. Los siguientes son algunos de los más conocidos.

El FBI admitió estar utilizando un producto llamado *Carnivore*[79] desarrollado con el fin de 'escuchar' el tráfico de correo electrónico dentro de EE. UU. (incluyendo el entrante y saliente) y seleccionar aquéllos que parecen sospechosos automáticamente.

Las herramientas de localización global (GPS, GLONASS) permiten conocer con una precisión de algunos metros la posición de algo o alguien sobre el planeta[80]. De esta forma se puede tanto arar un campo a la perfección como determinar la posición exacta de un presidiario prófugo o de un niño perdido. Actualmente se utilizan brazaletes que integran un GPS con la red de telefonía celular o receptores de radio para delatar su posición. Así es posible perseguir a un posible prófugo o controlar si un arresto domiciliario o una orden de restricción están siendo cumplidos. La empresa *Digital Angel* (http://www.digitalangel.net) desarrolló tecnología para implantar un dispositivo de este tipo en el cuerpo humano que genera la electricidad necesaria con el propio calor corporal y además de informar su posición monitorea el pulso y la temperatura del portador. Aunque la empresa lo presentaba como una excelente forma de cuidar niños y ancianos, sus estudios de mercado revelaron que el público 'aún' ve con desconfianza este tipo de im-

---

79 (http://www.fbi.gov/congress/congress00/kerr072400.htm) *Internet and Data Interception Capabilities Developed by FBI*, Federal Bureau of Investigations, EE. UU.

80 Este tipo de equipos utiliza la señal proveniente de un grupo de satélites a partir de los cuales triangula su posición. Uno de estos grupos de satélites es mantenido por el gobierno de EE. UU. (GPS) y otro por el gobierno Ruso (GLONASS). Ambos se encuentran disponibles para el uso civil (investigaciones, aviación, automóviles, etc.) aunque el primero de ellos introduce un corrimiento en la señal de forma que degrada la precisión de los equipos civiles, aun así se pueden obtener hasta unos 10 m. de precisión.

plantes, por lo que la empresa decidió posponer su lanzamiento hasta que el mercado sea más receptivo. A cambio, está dedicada a desarrollar versiones externas del dispositivo.

El 12 de marzo de 2001 se celebraron elecciones en Uganda. El gobierno de este país decidió utilizar tecnología de reconocimiento de rostros con el fin reducir el fraude electoral. Esta tarea se realizó por la compañía estadounidense Viisage Technology, Inc. (http://www.viisage.com) que fue contratada por el gobierno ugandés para registrar los rostros de los aproximadamente 10 millones de ugandeses habilitados para votar. Este registro de rostros implica convertir sus fotografías en 128 vectores que representan las características faciales, incluyendo el perfil de la nariz, el grosor de los labios y la distancia entre los ojos. Esta tarea se realizará durante el proceso de votación.

El gobierno estadounidense pagará unos 500 millones USD[81] a la industria de telefonía digital para que introduzca en sus desarrollos 'puertas traseras' para facilitar sus tareas de inteligencia. Ésta y algún otro tipo de iniciativas, como agregar funcionalidades de rastreo a los teléfonos celulares, se realizan según una ley aprobada en 1994 por el congreso de EE. UU. conocida como *Communications Assistance for Law Enforcement Act (CALEA)*[82].

Recientemente, el gobierno holandés realizó una investigación que le confirmó al parlamento europeo la existencia de *Echelon.* Se trata de una organización de espionaje masivo organizada por EE. UU., Gran Bretaña y otros países del Commonwealth que es capaz de escuchar y filtrar comunicaciones de todo tipo (voz, datos, etc.) interceptando las emisiones de microondas y satelitales y utilizando poderosas herramientas de extracción de información y una vasta red de satélites y antenas en, al menos, El Reino Unido y EE. UU. El parlamento europeo formó una comisión especial para estudiar este caso a raíz de numerosas denuncias y pruebas de su existencia. Aparentemente esta organización ha sido usada, al menos, para realizar espionaje industrial contra países de la Unión Europea[83].

---

81 (http://www.fbi.gov/congress/congress97/calea2.htm*), Implementation of the Communications Assistance for Law Enforcement Act (CALEA)*, FBI, EE. UU.

82 (http://www.epic.org/privacy/wiretap/calea/calea_law.html), [H.R.4922*] 'Communications Assistance for Law Enforcement Act'*, EE. UU.

83 (http://www.europarl.eu.int/committees/echelon_home.htm).

Un estudio[84], publicado en abril de 2000 por la American Management Association, encontró que la cantidad de compañías estadounidenses que realizan algún tipo de vigilancia activa sobre sus empleados subió del 45% en 1998 al 74% en 1999. El 'monitoreo' de correo electrónico creció del 27% al 38% en el mismo período.

La International Data Corporation (http://www.idc.com) estima que, en el mundo, las corporaciones gastan unos 62 millones USD en software de monitoreo y filtrado de Internet. Un estudio de la misma IDC predice que este gasto subirá a los 561 millones USD en 2005.

Reordenamiento de ideas

La evolución de los derechos (legislación) ha tenido muchas veces a los desarrollos tecnológicos como contrapartida. La invención del automóvil y su difusión e incremento en su potencia ha tenido un crecimiento exponencial. Ya desde su invención (y la del ferrocarril) se planteó el conflicto entre los beneficios que ofrecían estos medios de transporte y las consecuencias o riesgos que se presentaban. Si bien los derechos a la vida y a la integridad personal estaban suficientemente desarrollados antes de la invención del automóvil, los accidentes comenzaron a incrementarse significativamente.

Es importante ver que pese a las críticas y pronósticos apocalípticos que se hicieron sobre los riesgos que significaría el automóvil, las primeras modificaciones hechas a las legislaciones fueron para ajustar y ampliar el alcance de la legislación sobre daños; de esta forma se entendía que se compensaban económicamente las violaciones a los derechos a la vida y a la integridad personal. Si bien se fueron desarrollando normas legales para ordenar la circulación, no necesariamente fueron estas políticas las que tuvieron la capacidad de revertir el número de accidentes ni el número de muertes o lesiones. En este punto la legislatura fue quizás la que agregó la cuota de optimización y seguridad. Más que los textos legislativos y las ordenanzas de tránsito fueron las demandas contra los fabricantes (por ejemplo: el ca-

84 (http://www.amanet.org/research/pdfs/monitr_surv.pdf), "Workplace Testing, Monitoring y Surveillance", AMA, EE. UU.

so del *Ford Pinto*) las que obligaron a desarrollar diseños de automóviles más seguros[85].

Esta analogía muestra una vez más la lentitud (incapacidad) de la legislación para crear protecciones efectivas para los derechos y su incapacidad de ordenar o frenar los desarrollos tecnológicos. Puede decirse que el incremento en la seguridad fue más el resultado de soluciones tecnológicas (diseños más seguros) que el resultado de normas dirigidas a la protección de derechos. La adaptación rápida de la legislación sobre daños y la capacidad de la judicatura de encausar situaciones nuevas, fueron fuertes incentivos para la regulación del mercado automotor.

Quizás exista cierta analogía con la protección de los derechos de privacidad e intimidad. Pero, ¿es en este caso suficiente dejar en el ámbito de la responsabilidad civil el conjunto de incentivos para el ordenamiento de las nuevas tecnologías de información y comunicación? No debería tenerse en cuenta que la industria automotriz se desarrolló en países que tenían sistemas de responsabilidad civil muy fuertes. Hoy el desarrollo de sistemas informáticos ocurre con mayor velocidad en países en vías de desarrollo, donde prácticamente no existen sistemas difundidos de responsabilidad civil ni la costumbre de litigar por daños, más aun en los casos que si llegan al sistema judicial los montos indemnizatorios son insignificantes al compararlos con las ganancias de comercializar datos personales. Solo debería mencionarse que en América Latina no existen –o no están contemplados en el derecho positivo vigente– los daños punitivos, mientras que en los EE. UU. éstos pueden alcanzar cuantías millonarias (Alterini, A. y A. Filippini 1986: 406-418).

Re-conceptualización del dato personal

Al analizar la finalidad de un sistema de información y para evaluar los riesgos de invasión a la intimidad y privacidad es conveniente precisar categorías de datos:

---

85 *The Ford Pinto Case: A Study in Applied Ethics, Business and Technology,* Douglas Birsch and John H. Fielder, eds., 1994, State University of New York Press.

Dato estadístico: la inclusión de la información sólo está justificada para la realización de estadísticas, investigación o monitoreo; por lo que el nombre de las partes no será necesario identificarlo (quizás con la excepción del Estado o partes que mantienen múltiples casos). La consecuencia más importante es que la información que sólo se incluye a estos fines puede ampararse en el 'secreto estadístico'. Las normas sobre información estadística suelen incluir cierta obligación para las personas físicas y jurídicas de brindar datos. Como contrapartida se les garantiza cierta confidencialidad, que consiste en que no se publicará ni divulgará ningún dato individual que permita identificar quién brindó la información. La forma en que se divulgarán los datos, queda limitada a las técnicas estadísticas tradicionales.

Dato referencial: la información contenida en el sistema facilita el acceso o el proceso de identificación de documentos o personas necesarios para la gestión.

Dato documental: la información que tiene valor documental habilita para la toma racional de decisiones. Si las partes, por ejemplo, pueden informarse sobre una decisión del juez o una notificación por medio de una consulta al sistema de información, ese dato debe tener valor documental. En todos los datos clasificados como documentales debe garantizarse que la información no pueda ser modificada o, en su caso, deberá dejar rastros sobre el contenido anterior, quién los modificó y cuándo.

Dato registral: la característica más importante son sus efectos legales y su completitud; en un sistema registral, la no existencia de información pertinente tiene valor documental. Los principios que rigen la registración y la actividad de los Registros son: (i) rogación: el Registro no procede de oficio, sino a solicitud de la parte interesada, por intervención de autoridad administrativa o mandato de la autoridad judicial; (ii) todo documento inscripto puede dar lugar a oponibilidad; (iii) existe presunción de veracidad de los asientos registrales; (iv) el Registro debe examinar y comprobar fehacientemente que los documentos que se pretenden inscribir reúnen los recaudos legales del caso.

Poco se ha dicho sobre el papel que juega la información en la toma de decisiones. En el ámbito público y privado debe destacarse en Francia la Ley sobre la Informática, los Archivos y las Libertades[86]:

86 J.O. du 7 jan.1978 et rectificatif au J.O. du 25 jan.1978.

Loi 78-17 du 6 janvier 1978 relative a l'informatique, aux fichiers et aux libertés

Article 1er. L'informatique doit être au service de chaque citoyen. Son développement doit s'opérer dans le cadre de la coopération internationale. Elle ne doit porter atteinte ni a l'identité humaine, ni aux droits de l'homme, ni a la vie privée, ni aux libertés individuelles ou publiques.

Article 2. Aucune décision de justice impliquant une appréciation sur un comportement humain ne peut avoir pour fondement un traitement automatise d'informations donnant une définition du profil ou de la personnalité de l'intéressé. Aucune décision administrative ou privée impliquant une appréciation sur un comportement humain ne peut avoir pour seul fondement un traitement automatise d'informations donnant une définition du profil ou de la personnalité de l'intéressé.

Políticas gubernamentales

Históricamente, el derecho ha creado mecanismos, no para limitar los desarrollos tecnológicos sino para regularlos, para establecer un sistema de incentivos, y crear responsabilidades penales y civiles. Ese fue el caso del automóvil, que ha dado lugar a la aceptación del riesgo social que significa y la cantidad de daños personales que generan los transportes. Las soluciones a este tipo de conflictos rara vez son legislativas. En la mayoría de los casos se crean normas jurisprudenciales.

Sin embargo, es necesario un conjunto coordinado de políticas públicas para ordenar la generación de sistemas de información y la protección de los datos personales. La legislación general debería establecer que cada sistema de información que almacene datos personales esté precedido por una evaluación de necesidades, un análisis de riesgos y se establezca explícitamente su finalidad. La información personal almacenada debe ser mínima en función de esa finalidad.

También es necesario que las políticas públicas prevean un control del procesamiento de datos personales tanto en el ámbito público como privado. Esta tarea como autoridad de control puede ser ejercida por un funcio-

nario específico como, por ejemplo, en España la Agencia de Protección de Datos, sino puede ser una de las responsabilidades del Defensor del Pueblo u *Ombudsman*[87].

Es necesario que se definan políticas públicas explícitas sobre necesidad, almacenamiento, transferencia, y acceso a los sistemas de información con datos personales. Estas políticas deben ser dinámicas y ser el resultado del análisis de nuevos desarrollos y nuevas violaciones. El objetivo de estas políticas debería ser resolver la incapacidad de la legislación general para resolver situaciones imprevistas.

El órgano de control debería, además de investigar las denuncias y violaciones, verificar que los sistemas de información que se creen tengan una finalidad explícita, y sean minimales con relación a esa finalidad, que guarden normas de seguridad proporcionales a los riesgos evaluados y en el caso de sistemas privados dispongan de un seguro de responsabilidad civil.

Los servicios ofrecidos en Internet deben ser especialmente analizados y se debería promover la investigación y desarrollo de buscadores capaces de omitir los datos personales.

Soluciones tecnológicas

Seguridad en el ambiente de Internet

La construcción de la Internet como un sistema abierto de comunicaciones, a la vez que la hace inter-operable, la hace también vulnerable a ciertos riesgos incluyendo intrusiones subrepticias tales como el '*hacking*' y los errores humanos. Se pueden identificar tres tipos de riesgos que pueden superponerse:

Errores de programación ('*bugs*') y problemas provocados por errores de configuración en los servidores web, permiten a usuarios remotos no autorizados robar documentos y lograr información acerca del computador que realiza las tareas de servidor web lo que permite a continuación irrumpir en

87 Véase por ejemplo el veto del Poder Ejecutivo de Argentina al artículo 29 de la Ley de Protección de los Datos Personales (ley 25.326 de 2000) presumiblemente tratando de evitar el costo de la creación de una estructura administrativa.

el sistema. También existen riesgos del lado del navegador o '*browser'* que pueden resultar en el uso inadecuado de información personal provista con o sin conocimiento del usuario. Utilizando técnicas de 'escucha' del tráfico de la Red es posible interceptar datos enviados desde el *browser* al servidor o viceversa.

Estas vulnerabilidades vienen siendo explotadas inocente o deliberadamente. Algunos incidentes recientes incluyen el ingreso a las bases de una compañía de comercio electrónico y robo de miles de números de tarjetas de crédito (Ward, B. 1997). Una encuesta reciente publicada en EE. UU. indica que se realizan cinco ataques serios por mes a sitios web de comercio electrónico[88].

El Departamento de Defensa de EE. UU. reportó que el 80% de sus sitios fue penetrado, solo en 1996 sufrieron 250.000 intentos de intromisión en sus computadoras[89]. Este tipo de vulnerabilidades hace pensar que lo más indicado es no exponer información crítica en el contexto de la www. Es decir se debe minimizar el tipo de información que se brinda o almacena en equipos accesibles desde Internet separando aquella data crítica de la que no lo es. Esto puede incluir cortes transversales de información, como extraer un determinado tipo de casos de una base de jurisprudencia; o cortes longitudinales tales como extraer los nombres de las partes de todos los casos o de alguna clase de ellos.

Algunas técnicas desarrolladas con el fin de respetar la privacidad en la www[90]

Tecnologías de etiquetado y licenciamiento

Se trata de licenciar el uso de símbolos llamados *trustmarks* a los sitios 'en línea' a través de un programa de certificación y auditoría. Estas auditorías

88 (http://www.techweb.com/wire/news/1997/11/1120hack.html), (Yasin, R. 1997).

89 (http://www.gao.gov/AIndexFY96/abstracts/ ai96084.htm), "Information Security: Computer Attacks at Department of Defense Pose Increasing Risks" , U.S., General Accounting Office, May 22, 1996.

90 *'Privacy: The Key to Electronic Commerce'*, Information and Privacy Commissioner, Ontario, Canada. (http://www.ipc.on.ca/english/pubpres/sum_pap/papers/e-comm.htm).

se realizan por firmas de buena reputación que aseguran la integridad de las *trustmarks*. Con un 'clic' sobre la *trustmark* el usuario puede leer la política de privacidad del sitio web. Al menos el sitio debe revelar qué tipo de información recoge, como usa los datos, con quién comparte el sitio esa información, cómo el usuario puede evitar que sus datos sean utilizados por el sitio o terceros, cómo pueden realizarse cambios sobre los datos propios y cómo uno puede borrarse de la base de datos del sitio web. Un ejemplo de este tipo de empresas es TRUSTE (http://www.truste.com).

Tecnología de bloqueo

Una tecnología conocida como PICS (*Platform for Internet Content Selection*) desarrollada por el World Wide Web Consortium (W3C) del MIT, adjuntará etiquetas a las páginas web. En el momento de navegar en la Red estas etiquetas previenen el ingreso a aquellos sitios que el usuario haya configurado como indeseables. Además del etiquetado de material ofensivo, esta tecnología puede describir también las prácticas del sitio web sobre la información, tales como la información personal que recoge y qué información es re-usada o vendida[91].

Tecnologías de intercambio de información

Un ejemplo de este tipo de encares es el proyecto desarrollado por W3C llamado P3P (Plataforma para Preferencias de Privacidad)[92]. Una vez implementado P3P permitirá a los sitios web informar sus políticas de privacidad basándose en un conjunto específico de sentencias acerca de cómo ellos usarán, transferirán, negarán o aceptarán el acceso a los datos personales colectados. El usuario podrá a su vez configurar el conjunto de sus preferencias

---

91 (http://www.sciam.com/0397issue/0397resnick.html) , Paul RESNICK, 'Filtering Information on the Internet', *Scientific American.*

92 (http://www.w3.org/TR/WD-P3P-grammar.html), "Grammatical Model and Data Design Model,", World Wide Web Consortium, P3P Vocabulary Working Group y (http://www-.w3.org/TR/WD-P3P-arch.html), "General Overview of the P3P Architecture", P3P Architecture Working Group.

en privacidad. Si las configuraciones del sitio web y del usuario coinciden, se permite el acceso a dicho sitio sin advertencia alguna. De lo contrario un usuario puede negociar (asistido por herramientas simples) con el sitio (incluyendo la posibilidad de que le sea negado el acceso).

Perfil anónimo

Un acercamiento alternativo a la recolección de datos personales sobre la Red es el de los perfiles anónimos. Es decir la información demográfica recabada no es relacionada con un nombre en particular.

Criptografía

Muchas de las tecnologías de encriptación se encuentran aún en desarrollo. Aun así existe consenso en que las firmas digitales y la encriptación serán las herramientas básicas de todas las transacciones electrónicas. La encriptación se hace necesaria para la seguridad informática, incluyendo autenticación[93], confidencialidad, integridad y no-repudiación[94]. Existen varias formas de encriptación electrónica, pero actualmente prevalece sobre todas el esquema de clave pública-privada combinado con métodos muy fuertes de encriptación de clave única. El ejemplo más extendido de este esquema es PGP que en inglés es la sigla de Privacidad Bastante Buena (http://www.pgp.com). Este esquema encripta el mensaje con un mecanismo de clave única la que es generada aleatoriamente para cada procedimiento y ésta es a su vez encriptada con un mecanismo de clave pública-privada. Esto es, la clave pública únicamente sirve para encriptar y la privada sólo para des-encriptar. De esta forma la clave utilizada para desencriptar sólo está en posesión del destinatario de la información. Este tipo de encriptación utiliza claves de hasta 2.056 caracteres y hasta ahora quebrarlas implica tiempos de procesamiento del orden de miles de años.

---

93 En este contexto 'autenticación' significa que tanto el remitente como el receptor pueden confirmar la identidad de su contraparte y el origen y destino de la información.

94 'No-repudiación' implica que el creador-remitente de la información no puede negar la autoría del envío o de la información.

Firma digital

Las firmas digitales se utilizan para autenticar las partes en una comunicación en línea, de la misma forma que una firma escrita en un documento de papel autentica la identidad de los individuos involucrados. Sin embargo, a diferencia de las firmas de 'puño y letra', las firmas digitales son transferibles, esa posibilidad de transferencia debe ser manejada correctamente para garantizar la confiabilidad de este sistema. Una firma digital es una pieza de información secreta que un individuo posee y que está relacionada con su nombre. Esto deja lugar a dos riesgos centrales asociados con el uso de las firmas digitales: (1) identificación falsa en el momento de certificación de la firma digital, y (2) la información secreta, es decir la firma digital, es duplicada fuera del control de su propietario. La existencia de estos riesgos ha impulsado el desarrollo de nuevas tecnologías de autenticación, como lo son las técnicas de autenticación biométrica (huellas dactilares, 'huella' de voz, reconocimiento del iris, geometría de la mano, geometría facial, etc.). Paradójicamente este tipo de técnicas crea un nuevo mundo de posibles violaciones a la privacidad.

Transmisión segura

Estas aplicaciones proveen transferencias seguras de información entre un navegador y un servidor utilizando criptología del tipo clave pública-privada. Existen dos estándares en competencia: *Secure HTTP* y *Secure Sockets Layer* (SSL). Ambos poseen el mismo problema: el servidor web está habilitado para des-encriptar la información enviada por el usuario abriendo una puerta a su posible uso fraudulento.

Protocolos para transacciones con tarjetas de crédito

El protocolo de Transacciones Electrónicas Seguras (SET) desarrollado por Visa y Master Card imita el sistema normal de procesamiento de tarjetas de crédito utilizando técnicas de criptografía de clave pública y privada y firmas digitales. Su ventaja es que no permite que el comerciante al que se le

está realizando un pago lea la información de la tarjeta de crédito. De todas formas la entidad emisora de la tarjeta conoce y certifica los movimientos.

Dinero electrónico o virtual

El dinero electrónico (*e-cash*) se basa en una estrategia diferente a los efectos de ser usado en una red abierta como Internet. Dicha estrategia es evitar enviar información personal, en el caso del comercio electrónico, información acerca de la tarjeta de crédito utilizada. En su lugar se envía el 'dinero electrónico' es decir un mensaje que certifica la existencia del pago pero que no posee ninguna información personal de quien lo realiza. Esta tecnología fue diseñada por David Chaum (Chaum, D.; A. Fiat y M. Naor S/f.: 319-327) con el fin expreso de proteger la privacidad de los individuos. Existen varias implementaciones de esta idea, pero básicamente algunas de ellas están basadas en hardware (*smart cards*) y otras almacenan 'dinero' basándose en software a los efectos de realizar pagos sobre redes abiertas. En el caso de las basadas en hardware, se trata de sistemas que les permiten a los individuos usar tarjetas con memoria electrónica (bandas magnéticas o *chips* de memoria). En el caso de las basadas en software, se trata de una aplicación instalada en una computadora en la Red.Hay dos formas básicas de representar la cantidad de fondos almacenados: 'basados en balance', donde un balance simple es almacenado y actualizado en cada transacción o 'basado en notas', donde notas electrónicas, cada una con un valor fijo y un número de serie (tal como un billete real), es transferida de un dispositivo a otro. Estos valores son encriptados en el momento de las transmisiones para asegurar confidencialidad e integridad. La implementación basada en notas de *eCash Technologies, Inc* (www.digicash.com) usa un proceso de 'firma ciega' que asegura la imposibilidad de seguir la pista del dinero hasta el individuo.

Seguridad en los centros de cómputo, y otros elementos físicos

Normalmente se pone un gran énfasis en proteger las comunicaciones entre computadoras remotas, sin embargo, gran parte de los robos de informa-

ción se realizan 'a la antigua', es decir, accediendo localmente a los equipos que almacenan los registros. Esto implica considerar la forma de evitar irrupciones, robos y alteraciones, etc., en equipos, instalaciones y actividades tales como centros de cómputo, transporte de información, respaldo de información, dispositivos de almacenamiento extraíbles (discos blandos, CD-ROM, etc.), *notebooks*, impresoras, escritorios.

Pueden encontrarse buenos criterios de seguridad de elementos físicos, clasificados por niveles de seguridad en el Real Decreto 994/1999[95] del gobierno español.

Herramientas tecnológicas para control y prevención en el uso y manejo de la data

Sistemas de información dispersos

Un sistema de información disperso está constituido por dos o más sub-sistemas de información distintos que cooperan. Cada sub-sistema es capaz de procesar *data* almacenada localmente. La información almacenada para ser accedida remotamente o para propósitos de mantenimiento centralizado, debe estar almacenada de acuerdo a un esquema conceptual global. Sobre el cual se diseña un esquema común de base de datos. De acuerdo a Date es útil pensar un sistema distribuido como una relación de colaboración entre un conjunto de sistemas centralizados independientes pero cooperantes[96].

Los sistemas distribuidos aportan a la protección de la privacidad, la capacidad de aplicar diferentes niveles de seguridad a información personal de un mismo individuo. De esta forma puede, por ejemplo, cortarse longitudinalmente una base con datos demográficos e identificatorios, separar físicamente las partes resultantes, de forma que los datos de identidad se almacenen bajo medidas de seguridad extremadamente estrictas; y los datos demográficos, con un menor nivel de seguridad, estén disponibles, por ejemplo, para investigación.

---

95 (http://www.agenciaprotecciondatos.org/datd8.html), "Real Decreto 994/1999, Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal", España.

96 (http://www.adb.gu.se/~nickolas/papers/IRIS18.pdf), Nickolas Makrygiannis, *'Dispersed Information System Structures'*, Department of Informatics, Göteborg University, Sweden.

Por otra parte, es en la alta integración de los sistemas de información existente hoy en día donde reside, en buena parte, el riesgo a la privacidad de los individuos. Es decir la posibilidad de seguir el comportamiento de un individuo en diferentes áreas, se da gracias a la capacidad de cruzar información de todo tipo: qué está comprando, a quién está llamando o escribiendo, qué debe, qué no debe, de qué está enfermo, etc. Es la alta integración de toda esa información la que le da verdadero poder. Su dispersión efectiva ayuda a establecer trabas a qué sub-sistemas pueden colaborar y qué información se puede cruzar a los efectos de proteger la privacidad.

Tecnologías de autenticación

Un principio clave, que debe ser cuidado por cualquier política de seguridad, es el de responsabilidad. Es decir, poder definir quién es responsable por cada acción realizada en el espacio digital. En consecuencia, es necesaria una correcta identificación y para esto se debe realizar una correcta autenticación. Hay tres tipos clásicos de autenticación: (i) algo que el usuario sabe (una *password*), (ii) algo que el usuario tiene (una llave, una *smartcard*, etc.), (iii) algo que el usuario 'es' o 'hace' (biométricas). A pesar de gozar de simplicidad y alta aceptación, la autenticación basada en conocimiento es vulnerable a ataques basados en diccionarios y en 'fuerza bruta', en los que se intenta con cada combinación posible de caracteres.

La biométrica estrecha la línea que separa los métodos de identificación de los métodos de autenticación. Existen dos fases principales en la autenticación biométrica. En la fase de enrolamiento, cierta característica del usuario es medida. Ésta puede ser una característica física tal como sus huellas dactilares, la geometría de su mano, la configuración de las venas de la retina, el diseño del iris, la geometría de la cara o el ADN, o una característica de comportamiento tal como la voz o la dinámica del acto de firmar. En cualquiera de estos casos la tecnología actual permite analizarlos y extraer una representación numérica (en forma de vectores por ejemplo) de la característica. Esta puede ser tan afinada que, por ejemplo, exprese las diferencias entre dos rostros cualquiera. Para autenticar a una persona, la característica considerada debe ser medida nuevamente y el resultado numérico comparado con el almacenado en la primera fase. La perso-

na es entonces autenticada según lo cerca que se encuentre el valor calculado del almacenado.

Si bien se trata de sistemas muy avanzados y precisos de autenticación, debe notarse que las biométricas no son llaves. Por ejemplo, no pueden ocultarse, cambiarse o destruirse. La unicidad de los identificadores biométricos, el hecho de no ser transferibles y de no poder ser perdidos u olvidados les da una ventaja interesante sobre los sistemas basados en conocimiento. Pero como se dijo anteriormente, crean un nuevo riesgo a la privacidad y deben ser manejados y almacenados con sumo cuidado y su uso debe ser restringido al esperado por el usuario.

Manejo de notificaciones

Después de tomadas todas las medidas de seguridad que se consideren adecuadas y de aplicar políticas de autorizaciones y autenticación que correspondan con la clasificación de la información manejada, debe considerarse la posibilidad de que sean burladas. Es muy importante entonces minimizar el tiempo durante el cual la intrusión no es detectada a los efectos de minimizar sus perjuicios. Para lograr esto se deben mantener registros de todas las actividades realizadas sobre el sistema por cualquiera de los usuarios que poseen algún derecho sobre la información. Estos registros, además de dar una pista de los perjuicios ocasionados, deben ser inspeccionados automáticamente de forma que detecten patrones que sugieran una posible irrupción en el sistema, por ejemplo sucesivos intentos fallidos de autenticación. Estas aplicaciones deben realizar una notificación al administrador del sistema o al encargado de la seguridad para que éste investigue la situación potencialmente peligrosa. Así mismo, el sistema debe notificar sobre operaciones especialmente delicadas o sospechosas, tales como copias, bajas o modificaciones masivas de información.

Conclusiones

Cada vez que se sacrifica la intimidad y la protección de los datos personales, la justificación se basa en la solución de un conflicto de intereses: la se-

guridad pública, la lucha contra las drogas, la libertad de prensa (Budano Roig, A. 1998: 181-217), etc. en el que se establece una preferencia en contra de la privacidad e intimidad. Es claro que no hay reglas generales que puedan establecerse por la vía legislativa, este es el terreno propio de las decisiones judiciales que pueden resolver con justicia las situaciones particulares.

Atento, pues, a la disparidad de criterios existentes dentro de los órganos del Estado con respecto a la publicidad de la información recogida en sus actuaciones, o en los bancos de datos privados y ante la certeza de que tanto el volumen como las facilidades de acceso seguirán creciendo, mientras, que la demanda de información, con un interés legítimo o sin él, irá en aumento, se considera altamente recomendable proponer legislación que contemple las situaciones anotadas y, fundamentalmente, defina principios generales aplicables durante el desarrollo de procesos de informatización.

Esta legislación debería ser compatible y complementarse con la ley que determine los alcances del *habeas data*, aún no reglamentado en algunos países, puesto que, en principio, la publicidad rige para casi toda información que se maneja en la esfera pública. Con todo, deberían establecerse lineamientos que atiendan al ciudadano en su situación de indefensión frente al uso que de esa información pueda hacerse. Será necesario, pues, establecer límites en los procesos de recolección de datos mediante normas sustantivas que exijan la identificación previa de la necesidad de contar con el dato y su finalidad de uso, así como quiénes podrán requerir tal información.

La creación de sistemas de procesamiento de datos debería ser transparente y accesible a todas las personas. Es necesario que las agencias gubernamentales que trabajen con bancos de datos tengan contactos con instituciones independientes y organizaciones no gubernamentales que ofrezcan el servicio de sus expertos y representen la opinión de sectores específicos. Se deberían estudiar, como análisis de riesgo, los efectos y consecuencias que los sistemas de procesamiento de datos puedan producir en la sociedad.

La legislación debería evitar que la información almacenada genere o permita cualquier forma de discriminación o preconcepto, por ejemplo mediante la recopilación y conservación de datos sobre creencias religiosas, opiniones políticas, actitudes sexuales, origen étnico, discapacidad, etc. A su vez, se deberían identificar y estipular los plazos en que el mantenimiento de los datos fuera necesario, definiendo los procedimientos mediante los

cuales serán eliminados. La publicidad no protege la indiscriminada divulgación de los datos, ni significa convertir a la administración pública en un servicio de informes. La legislación debería establecer en qué casos la información referente a un individuo puede ser proporcionada a terceros.

Resulta, necesaria, pues, la definición de políticas en esta área, sea abriendo la información del Estado a cualquier usuario y admitiendo el recurso individual de reserva de la información, o, por el contrario, restringiendo el acceso solamente a quienes ostenten un interés legítimo debidamente acreditado. Las definiciones en este campo son un requerimiento sustancial para el desarrollo y la eficacia de los sistemas de información, así como de los servicios públicos de información y de los registros estatales, y, en especial, del procesamiento estadístico de los datos.

Los 'motores de búsqueda' facilitan la tarea de obtener información y es por ello que se les reconoce una marcada utilidad, sin embargo también son el principal instrumento informático en contra de los derechos de privacidad. Es difícil, pero deberían 'saltar' sobre los datos personales; esto llevaría a diferenciar dentro de un registro automatizado (sea de texto o estructurado) la información que pueda relacionarse unívocamente con una persona determinada.

La auto-regulación ha sido exitosa en áreas similares, por eso de acuerdo con los antecedentes expuestos, el diseño de los sistemas de información debería –mientras no existan normas o políticas explícitas– buscar no romper el equilibrio entre:

- publicidad y transparencia de las actuaciones del Estado
- legitimidad de las actividades privadas que supongan la acumulación de datos personales

y la protección de la privacidad y la intimidad de las personas (prevalentemente la de los grupos más vulnerables).

Hoy, este equilibrio se garantiza con las más recientes tendencias sobre la protección de datos personales:

- principio de finalidad
- principio de proporcionalidad (los datos deben ser adecuados, pertinentes y no excesivos)

- los datos se obtendrán y tratarán legal y legítimamente
- derecho de acceso a la información (a saber, antes de iniciarse cualquier tratamiento informático, qué datos personales y cómo dichos datos van a ser tratados, transmitidos y transferidos a otras personas)
- derecho a saber a quién se han transferido sus datos personales
- derecho de oponerse por motivos legítimos a que los datos sean objeto de tratamiento informático
- derecho de rectificación
- acciones específicas para la garantía del *habeas data*
- cancelación de los registros cuando hayan dejado de ser necesarios o pertinentes para su finalidad
- secreto estadístico
- existencia de una autoridad de control y protección de datos personales.
- control estricto de la organizaciones que comercializan datos personales
- penas severas para quienes violen las normas y para quienes roben información

La forma de alcanzar el equilibro supone varias políticas diferenciadas:

Muchas de las violaciones surgen de la creciente tendencia del Estado a crear bases de datos o registros. En muchos casos son las legislaturas las que los crean. Debería existir una normativa que establezca requisitos para su creación y las condiciones necesarias para su operación, incluyendo medidas de confidencialidad y seguridad. En palabras de Leggiere, muchos riesgos o violaciones son la consecuencia de la 'ignorancia' sobre el potencial de las nuevas tecnologías[97]. Tampoco debe olvidarse que la protección de la privacidad es una protección frente a los sistemas totalitarios[98].

La iniciativa privada requiere leyes que regulen actividades específicas, por ejemplo: bureau de crédito, tarjetas de crédito, bancos, teléfonos, historias clínicas, etc. Estas leyes deben buscar equilibrar los intereses económicos con los derechos de privacidad e intimidad, algunos elementos claves son: la asignación de responsabilidad civil debe estar direccionada como un

97 (http://www.upenn.edu/gazette/1198/leggiere.html) Phill Leggiere, Constitutionalist in cyberspace, *The Pennsylvania Gazette,* 1998.

98 Ver nota 12 y texto acompañante.

incentivo hacia la protección de los derechos fundamentales; deben crearse autoridades de control y vigilancia; y, obligar a los responsables de las bases de datos a adoptar severas, medidas de seguridad. Es fundamental para regular estas actividades que los jueces estén informados sobre los nuevos desarrollos tecnológicos y un recurso accesible y efectivo de *habeas data.*

El problema más arduo se relaciona con Internet y más aun cuando está por medio la libertad de expresión, por ejemplo: periódicos *on line*. Hoy las leyes de Internet son las leyes del mercado[99], más aun Internet ha modificado algunas de las leyes clásicas del mercado. Por eso es actualmente difícil lograr garantías para los Derechos Humanos en Internet. Es importante analizar la evolución del derecho a la libertad de expresión[100], en particular la decisión que tome la Suprema Corte de los EE. UU. en *Free Speech Coalition v. Reno.* Si bien existe en Internet una creciente auto-regulación, los sitios de mayor riesgo son los que evaden todo marco de regulación.

Bibliografía

Alterini, A. y A. Filippini
1986 Responsabilidad civil derivada de la difusión de noticias inexactas: acto ilícito o acto abusivo. En: 1986-c *La Ley,* pp.: 406-18.

Annas, G. J.
1999 Genetic Privacy: there ought to be a law. En: 4 *Texas Review of Law y Politics,* pp.: 9-15.

Antik, A. y L. Ramunno
2000 *Habeas Data*: comentarios sobre los bancos de datos privados destinados a proveer informes. En: 2000-b *La Ley,* p.: 1.164.

99 The end of Privacy: the surveillance society, *The Economist* (May 1st, 1999) 21-23.

100 Algunos ordenamientos reconocen limitaciones al derecho de prensa. Así, por ejemplo, en el derecho alemán, se establecen "límites en las disposiciones de las leyes generales, en las disposiciones legales adoptadas para la protección de la juventud y en el derecho al honor personal" (artículo 5 inciso 2 de la Constitución alemana).

Bianchi, A.
1995 *Habeas data* y derecho a la privacidad. En: 161 *El Derecho,* pp.: 866-878.
Bidart Campos, G. J.
1992 Identidad, filiación y privacidad de una menor en su juicio de filiación paterna: nada de vedettismo informativo. En: 145 *El Derecho,* p.: 415.
Birsch, D. y J. H. Fielder (eds.)
1994 *The Ford Pinto Case: A Study in Applied Ethics, Business and Technology.* State University of New York Press.
Budano Roig, A.
1998 La libertad de prensa, la censura previa y el derecho a la intimidad de una menor. En: 177 *El Derecho,* pp.: 181-217.
Cadoux, L.
1994 L'experience française en protection des données personnelles dans le domaine des banques de données judiciares. En *Informática Judicial y Protección de Datos Personales.* Departamento de Justicia, Gobierno Vasco, pp.: 157-171.
Cappelletti, M. y B. Garth
1988 *Acesso à Justiça.* Fabris Editor.
Cifuentes, S.
1995 La intimidad y el honor de los vivos y de los muertos. En: 162 *El Derecho,* p.: 404.
Cifuentes, S.
1999 Reconocimiento Jurisprudencial del derecho a los datos personales informáticos y del *habeas data* en su verdadero fin tutelar. En: 1999-e *La Ley*, p.: 151.
Cifuentes, S.
1999 Nota al fallo: "Reconocimiento del derecho a los datos personales informáticos y del *habeas data* en su verdadero fin tutelar". En: *La Ley* (diario del 15 de septiembre).
Chaum, D.; A. Fiat y M. Naor
S/f. Untraceable Electronic Cash. En: *Advances in Cryptology crypto '88.* S. Goldwasser. (Ed.) Springer-Verlag.

del Villar, R.; A. Díaz de León y J. Gil Hubert
2000 La regulación de protección de datos personales y burós de crédito en América Latina. En: *International Conference on Credit Reporting Systems*, World Bank Institute.

Demeriex, M.
1992 *Fundamental Rights in Commonwealth Caribbean Countries.* University of West Indies.

Fuentes Torrijo, X.
2000 Criterios para solucionar el conflicto entre la libertad de expresión y la protección de la honra de las personas: dos métodos distintos de razonamiento jurídico. En: 6 (1) *Ius et Praxis,* pp.: 427-41.

Gozaíni, O.
2001 *Habeas Data. Derecho Procesal Constitucional.* Rubinzal Culzoni eds.

Gregorio, C. G.
1999 *Información, Privacidad y Derechos del Niño.* XVII Congreso Panamericano del Niño. OEA/SER.K/XXIV.18.1/CPN-/DOC.12/99.

Jones, J.
1995 Maintaining Unsubstantiated Recors of 'Suspected' Child Abuse: much ado about nothing or a violation of the right of privacy?. En: *Utah Law Review,* pp.: 887-912.

Leggiere, P.
1998 Constitutionalist in cyberspace. En: *The Pennsylvania Gazette.*

Makrygiannis, N.
S/f. *Dispersed Information System Structures.* Department of Informatics, Göteborg University, Sweden.
1989 PC Peep Show: computers, privacy, and child pornography. En: 27 *John Marshall Law Review,* pp.: 989-1013.

Martorell, F.
1993 *Impunidad diplomática.* Buenos Aires: Editorial Planeta.

Miller, M.
2000 Credit reporting systems arround the globe: the state of the art in public and private credit registries. En: *Interna-*

tional Conference on Credit Reporting Systems, World Bank Institute.

Peña González, C.
1996 El derecho civil en su relación con el derecho internacional de los derechos humanos. En: *Sistema Jurídico y Derechos Humanos* (Medina, C. y J. Mera Figueroa, eds.) Universidad Diego Portales, Chile, pp.: 545-660.

Pierini, A.; V. Lorences y M. I. Tornabene
1999 *Habeas data: derecho a la intimidad.* Editorial Universidad.

Prosser, W.
1960 *Handbook of the Law of Torts.*

Puccinelli, O.
1999 *El* Habeas data *en Indoiberoamérica.* Santa Fe de Bogotá: Editorial Themis.

Resnick, P. Filtering
1997 Information on the Internet. En: *Scientific American*, marzo.

Roche, P. y L. Glantz
1996 The Genetic Privacy Act: a proposal for national legislation. En: *Jurimetrics Journal* 37, pp.: 1-11.

Rotunda, R.
1995 Computerized highways and the search for privacy in the case law. En: *Computer y High Technology Law Review,* pp.: 119-27.

Roxborouh, P.
1999 Invasion of privacy: telephone customers upset with billing system. En: *The Jamaica Gleaner*, 8 de marzo.

Rubenfeld, J.
1989 The Right of Privacy. En: *Harvard Law Review,* pp.: 737-752.

Sagüés, N. P.
1995 Subtipos de *Habeas data.* En: 1995-iv *Jurisprudencia Argentina,* pp.: 352-5.

Schwartz, P.
1992 Data processing and government administration: the failure of the American legal response to the computer. En: 43 *Hasting Law Review,* pp.: 1321-1389.

Shapiro, R. y G. Annas
1994 Who sees your medical records? En: *Human Rights: Journal of Individual Rights,* pp.: 10-36.
Shepherd, L.
2001 Looking forward with the Right of Privacy. En: *Kansas Law Review* 49*,* pp.: 251-320.
Slaibe, M. y C. Gabot
2000b *Habeas data:* su alcance en la legislación comparada y en nuestra jurisprudencia. En: *La Ley,* p.: 27.
Sosa, R.
2000 El *habeas data* y el amparo al derecho a la intimidad. En: *Gaceta Judicial* 74 (República Dominicana).
Traband, R.
1995 The Acton case: the Supreme Court's Gradual sacrifice of privacy rights on the altar of the war on drugs. En: *Dickinson Law Review* 100*,* pp.: 1-28.
Vibes, F.
2000d Internet y Privacidad: la difusión en Internet de imágenes lesivas de la intimidad, el honor y otros derechos personalísimos. En: *La Ley,* pp.: 1011-1024.
Ward, B.
1997 Hackers find theft at fingertips. En: *Windsor Star*, Oct. 21.
Warren, S. y L. D. Brandeis
1890 The Right To Privacy. En: *Harvard Law Review* 4*,* p.: 193.
Williams, G.
1999 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. En: *Loyola of Los Angeles Entertainment Law Journal 19,* pp.: 337-61.
Yasin, R.
1997 E-Commerce Sites Top Hacker Hit List. En: *Internet Week* reported in Tech Web News, 20 Nov.