EL DERECHO A LA INTIMIDAD Y EL TRATAMIENTO DE DATOS PERSONALES EN EL DERECHO INTERNACIONAL PRIVADO ARGENTINO

MARIO J. A. OYARZÁBAL*

I. ACTUALIDAD Y DIMENSIÓN INTERNACIONAL DEL PROBLEMA

La noción de los derechos de la personalidad —que abarca aspectos tan diversos como el derecho al nombre, a la integridad física, al respeto a la vida privada, a la imagen, al honor, y aun el derecho moral del autor a su obra— ha cobrado particular importancia en las últimas décadas con el advenimiento de la sociedad tecno-científica, que multiplica las posibilidades de lesiones de los derechos que la integran a través de su utilización económica muchas veces allende las fronteras del país de residencia de la persona afectada. Me refiero principalmente a los daños cometidos a través de la prensa u otros medios de difusión internacionales, como la reproducción de fotografías personales, la difusión de correspondencia y el plagio, que constituyen ilícitos; pero también a los problemas creados en el ámbito internacional por la investigación genética y el trasplante de órganos, que tienen al cuerpo humano mismo como objeto de actos jurídicos.

Un problema acuciante y relativamente novedoso que plantea el avance de la informática y de la tecnología de las telecomunicaciones se relaciona con el tráfico de datos personales, que incide sobre uno de los atributos más caros de la persona humana: su *derecho a la intimidad*, una de cuyas proyecciones consiste precisamente en "preservar en la confidencialidad y la reserva bienes personales como los que hacen al honor, la dignidad, la información 'sensible' [por ejemplo, la referida a orientación sexual, identidad étnica o racial, religión, ciertas enfermedades, e ideas

* Cónsul Adjunto de Argentina en Nueva York, Jefe de la Sección Consular, desde 2005. Profesor Adjunto de Derecho Internacional Privado, Facultad de Ciencias Jurídicas y Sociales, Universidad Nacional de La Plata.

políticas], la privacidad, la verdad, la autodeterminación informativa [y] la igualdad [que incluye el derecho a la identidad personal y el derecho a ser diferente]"[1].

Las actividades relacionadas con el tratamiento automatizado de datos personales poseen necesariamente una dimensión internacional que es consecuencia de la naturaleza global (o internacional, o transnacional) de los medios informáticos. En primer lugar, porque la tecnología que se utiliza en el tratamiento automatizado de datos es generalmente importada, lo que ocasiona una dependencia sustancial de los proveedores extranjeros, principalmente de los Estados Unidos y el Japón. En segundo lugar, por la desmaterialización del soporte de los circuitos automatizados y la facilidad con que los datos pueden ser consultados desde cualquier parte del mundo. Finalmente, por la falta de controles eficaces a la transmisión de datos personales desde un país a otro (*transborder flow of data*) a través de una cooperación e instrumentos internacionales adecuados[2].

Efectivamente, con excepción de la Unión Europea y de algunas otras iniciativas internacionales de las que doy cuenta más abajo, el "régimen de los datos informatizados" —que incluye tanto el funcionamiento doméstico de la red informática y los controles a los cuales los Estados someten los flujos transfronterizos, como los efectos que el tratamiento de datos personales puede tener sobre los derechos individuales de las personas[3]— está sometido exclusivamente al derecho nacional de cada país. Así las cosas, cuando los datos atraviesan una frontera y las diversas fases del tratamiento se realizan en el territorio de Estados diferentes, como ocurre en gran parte de las operaciones automatizadas, es de prever el surgimiento de conflictos entre las leyes potencialmente aplicables a la controversia, que son esencialmente cuatro: la ley del lugar de la sede del banco de datos, la ley del lugar de la sede o residencia del responsable del tratamiento, la ley personal del titular de los datos y la ley del Estado donde tiene lugar la principal actividad del tratamiento[4]. La solución de esos conflictos corresponde, por esencia, al derecho internacional privado.

[1] Bidart Campos, Germán J., *Manual de la Constitución reformada*, Ediar, Buenos Aires, 1998, t. II, p. 389, y t. I, ps. 529 y 532.

[2] Ver Rigaux, François, "La loi applicable à la protection des individus à l'égard du traitement automatisé des données à caractère personnel", *Rev. Crit. Dr. Int. Pr.*, 1980, p. 444.

[3] Según definición de Rigaux, François, "Le Régime des données informatisées en droit international privé", *Clunet*, vol. 113, 1986-2-314.

[4] Ver Saravalle, Alberto, "Brevi osservazioni critiche sull'ambito d'applicazione territoriale della legge n. 675/96 sul trattamento dei dati personali", *Riv. dir. int. pr. proc.*, 1999-I, ps. 46 y 47 y la bibliografía citada en nota 11.

II. La ley 25.326 de Protección de Datos Personales y la garantía constitucional del *habeas data*. Aspectos regulados y lagunas

En la Argentina, la ley 25.326 de Protección de los Datos Personales del 4 de octubre de 2000[5] vino a cubrir el vacío legal existente desde la reforma de la Constitución Nacional de 1994, que instituyó el *habeas data* como acción destinada a preservar la intimidad o privacidad de las personas (art. 43, párr. 3°)[6]. Asimismo, aunque los tratados de derechos humanos con jerarquía constitucional no contienen disposiciones expresas sobre el *habeas data*, se ha sostenido con autoridad que cuando en alguna disposición de los mismos se hace referencia a derechos que se identifican con los que el *habeas data* protege, se les debe dispensar el "recurso sencillo y rápido" que, innominadamente, aparece en el Pacto de San José de Costa Rica (art. 25) y el Pacto Internacional de los Derechos Civiles y Políticos (art. 2, inc. 3) (*habeas data* implícito)[7].

La Ley de Protección de los Datos Personales contiene dos disposiciones de interés desde la perspectiva del derecho internacional privado: el art. 2°, que determina las personas (cuyos derechos individuales son) objeto de la protección; y el art. 12, que protege los datos tratados a través del control de las transferencias al exterior. Otros aspectos no han tenido una definición legal, como en qué casos los tribunales argentinos poseen jurisdicción internacional y a la luz de qué derecho se resolverán las controversias que un tratamiento de datos suscite, por ejemplo, entre el titular de los datos y el responsable del banco de datos o un usuario de los datos, entre otras cuestiones relevantes; presumiblemente porque el legislador ha juzgado que las cuestiones no reguladas deben quedar sometidas a los principios generales.

En los parágrafos que siguen procuraré dar solución a los aspectos más fundamentales de este fenómeno, a la luz de las normas argentinas de derecho internacional privado, para lo que tendré en consideración las orientaciones más recientes y que cuentan con mayor aceptación en el derecho comparado. Especial cuidado pondré en identificar las normas imperativas de la ley 25.326 que, por la defensa de la intimidad de las personas que persiguen, son aplicables aun cuando los casos presenten carácter multinacional (normas de policía del derecho internacional privado relativas a los datos informatizados).

[5] BO del 2/11/2000.

[6] Sobre la "constitucionalidad" de la intimidad y el *habeas data*, ver Bidart Campos, Germán J., *Manual...*, cit., t. I, ps. 523-27 y t. II, ps. 387-93.

[7] Cf. Bidart Campos, *Manual...*, t. II, cit., ps. 386 y 393.

Mantengo el criterio tradicional de distinguir entre bancos de datos públicos y bancos de datos privados, distinción que no queda superada, a mi juicio, por el hecho de que el Estado frecuentemente "compra" bases de datos privados o, lo que es lo mismo, la autorización para acceder a tales ficheros[8]. Lo esencial es que la responsabilidad en que pueda incurrir el Estado al gestionar datos personales derivada de la violación de la intimidad se rige exclusivamente por el ordenamiento del foro (la coincidencia *forum-jus* es total); en tanto que a la vulneración de la intimidad realizada por particulares resultan aplicables las normas de conflicto del juez interviniente, que pueden remitir a un derecho extranjero[9]. Completo el estudio con la incorporación de capítulos que ya han devenido tradicionales en mis investigaciones: el rol de la autonomía de la voluntad allende la problemática de los contratos; la solución de los conflictos internos de leyes interjurisdiccionales; y el estado de la cuestión en el Mercosur.

III. Funcionamiento de los bancos de datos públicos y control administrativo de los bancos de datos privados

1. Funcionamiento de los bancos de datos públicos

La protección de los datos personales, asentados en registros gestionados por organismos públicos argentinos, como el Registro Nacional de las Personas o la Policía Federal, se rige por el derecho administrativo argentino[10]. No interesa que la base de datos se encuentre físicamente en territorio extranjero. El tratamiento de los datos personales asentados en la llamada "matrícula consular", y cualesquiera otros registros de las embajadas y consulados argentinos en el exterior, está sometido exclusivamente al derecho argentino y exento de la jurisdicción local. Toda acción de protección de los datos personales almacenados en bancos de datos públicos argentinos debe interponerse ante los jueces nacionales, sin que quepa re-

[8] Sosteniendo que la distinción entre bases de datos públicos y privados pierde, en tales hipótesis, lo esencial de su pertinencia, ver Rigaux, "Le Régime...", cit., ps. 313-14 y la bibliografía citada en nota 6.

[9] Ver, en general, Macherey, Augustin, "Réglementation des flux transfrontières de données de caractère personnel", en *Informatique et protection de la personnalité*, Université de Fribourg, 1981, ps. 220 y 245-46; Simitis, Spiros, "Grenzüberschreitender Datenaustauch. Notwendige Vorbemerkungen zu einer dringend erforderlichen Regelund", *Festschrift für Murad Ferid*, Beck, München, 1978, ps. 373-74.

[10] Otras entidades públicas que almacenan y tratan datos personales incluyen la Dirección Nacional de Migraciones, la Secretaría de Inteligencia del Estado (SIDE) y los establecimientos sanitarios del Estado nacional, además de los gobiernos —y entidades que dependen de los gobiernos— provinciales y de la Ciudad Autónoma de Buenos Aires.

conocer ninguna sentencia extranjera que invada la jurisdicción argentina exclusiva. La coincidencia entre jurisdicción y derecho aplicable es total. Las doctrinas de la inmunidad del Estado por actos *iure imperii* y de la inmunidad diplomática y consular justifican sobradamente esta solución [11].

Por las mismas razones, las autoridades argentinas deben abstenerse de intervenir en casos que involucren bancos de datos personales gestionados por órganos estatales extranjeros o por organismos internacionales en los términos del respectivo acuerdo de sede. Ello, sin perjuicio de la reclamación diplomática a que la utilización indebida de los datos personales de residentes argentinos pueda dar lugar. Pensemos en el caso de una embajada extranjera que cede los datos personales, suministrados por residentes argentinos en oportunidad de tramitar una visa, a operadores turísticos locales u otras empresas de la nacionalidad del Estado al que la misión diplomática representa, sin el consentimiento del titular de los datos. El gobierno argentino puede exigir al Estado extranjero que repare el daño causado (es decir, que cese inmediatamente de ejecutar el acto y restablezca la situación que con toda probabilidad habría existido si no se hubiera cometido el acto [12]) invocando el principio de supremacía territorial y el deber de los agentes diplomáticos y consulares de respetar las leyes y reglamentos del Estado receptor (art. 41, Convención de Viena sobre relaciones diplomáticas; y art. 55, Convención de Viena sobre relaciones consulares). La excepción es quizás el caso de los datos pertenecientes a residentes argentinos que son nacionales del Estado acreditante. Adicionalmente, el titular de los datos podrá demandar al cesionario privado de los datos para exigir su supresión y confidencialidad, así como los daños y perjuicios a que hubiera lugar. El Estado argentino también tiene derecho a ejercer la protección diplomática a favor de sus nacionales radicados en el extranjero, si considera que sus derechos fundamentales garantizados por el derecho internacional han sido lesionados por las autoridades de otro Estado.

2. Control administrativo de los bancos de datos privados

Las normas de derecho administrativo por las que el Estado procura controlar los bancos de datos privados son también territoriales, en un doble sentido, formal y material. Las obligaciones legales de los respon-

[11] Cf. Rigaux, "La loi applicable... ", cit., ps. 467-68.

[12] C.P.J.I., serie A, nro. 17, p. 47.

sables privados de bancos de datos frente al órgano público de control [13] son las previstas en la *lex fori* argentina (territorialidad en sentido formal). Asimismo, para que el control sea eficaz, es preciso que se le sometan solamente aquellas fases del tratamiento de datos —recolección, modificación, destrucción, cesión, transferencia, etc.— que se producen en territorio argentino (territorialidad en sentido material). Todo intento de extender el control administrativo a actos realizados en el extranjero que generen obligaciones legales según la ley argentina, aunque sea deseable, es ilusorio [14] sin permiso del Estado extranjero [15].

Los bancos de datos sometidos al control de la autoridad argentina son los formados por personas físicas o jurídicas con domicilio legal, delegación o sucursal en el país. A ellos se dirige el deber de inscripción en el Registro Nacional de Bancos de Datos [16] (arts. 3, 21 y 24) y las normas sobre integridad y seguridad de los datos de la ley 25.326, incluida la prohibición de transferir datos con países que no ofrecen una protección adecuada del art. 12 de la ley. Físicamente la base de datos puede estar alojada dentro o fuera de la Argentina, pero el titular debe declarar su ubicación precisa al momento de inscribir, renovar, modificar o dar de baja al fichero en el Registro. No es necesaria la inscripción cuando todos los datos pertenezcan a personas domiciliadas fuera de la Argentina, ya que, como veremos más abajo, ellos no gozan de protección legal en nuestro país. Pero la incorporación de datos correspondientes a un solo domiciliario argentino somete al responsable del fichero al control de la ley 25.326. Como el fichero puede estar ubicado en el extranjero, la Ley de Protección de los Datos Personales se basa en la jurisdicción argentina sobre la persona del responsable del banco de datos y el recurso a mecanismos de cooperación internacional para garantizar el control del tratamiento de los datos realizados fuera del país.

[13] El órgano de control de la ley 25.326 es la Dirección Nacional de Protección de Datos Personales (DNPDP), creada en el ámbito de la Secretaría de Justicia y Asuntos Legislativos del Ministerio de Justicia y Derechos Humanos de la Nación (dec. 1558/2001; BO del 3/12/2001).

[14] Ver, en general, Rigaux, "La loi applicable...", cit., ps. 449 y 469-70; Carrascosa González, Javier, "Protección de la intimidad y tratamiento automatizado de datos de carácter personal en DIPr.", *REDI*, vol. XLIV, 1992, ps. 419-20.

[15] Sobre la eficacia extraterritorial del acto administrativo, en la literatura argentina, ver Boggiano, Antonio, *Derecho internacional privado*, t. I, Depalma, Buenos Aires, 1991, ps. 535-38.

[16] Habilitado por disposición DNPDP 2/2003 e implementado por disposición DNPDP 2/2005. La normativa y formularios de inscripción en el Registro se encuentran disponibles en el sitio de Internet de la Dirección, en *http://www2.jus.gov.ar/dnpdp/index.html*.

IV. Otros problemas suscitados por los bancos de datos privados

1. Protección de la intimidad frente a los responsables de bancos de datos privados

La ley 25.326 no contiene normas de conflicto que indiquen el derecho aplicable a las relaciones jurídicas entre el responsable del banco de datos y las personas cuya intimidad es protegida por la ley. El art. 2°, cuando define como "titular de los datos" a "[t]oda persona física o persona de existencia ideal con domicilio legal o delegaciones o sucursales en el país, cuyos datos sean objeto del tratamiento al que se refiere la presente ley", no constituye (y no debe ser confundido con) una norma de conflicto. Esa disposición autolimita el ámbito espacial de aplicación de la Ley de Protección de los Datos Personales [17]; es decir, subordina la puesta en práctica de las normas materiales de la ley 25.326 al cumplimiento de una condición propia de las personas protegidas: la de tener "domicilio legal" en la Argentina [18]. Se deduce que las personas sin domicilio legal en la Argentina, aun cuando posean tal nacionalidad, no pueden invocar las disposiciones de la ley 25.326 para controlar la información contenida en los bancos de datos de la Argentina. Esta solución es justificada, ya que la Argentina no podría pretender proteger la intimidad de sus ciudadanos que se encuentran en cualquier país del planeta. Además, el hecho generador de la protección es el mismo que causa la aplicación del derecho argentino en virtud de la norma de conflicto del art. 6° del Código Civil, con lo que se evita que ciertos atentados a la vida privada que caen dentro de la competencia legislativa argentina queden sin protección.

En pocas palabras, entiendo que el respeto al derecho a la vida privada constituye uno de los derechos subjetivos integrantes del estatuto personal que, en ausencia de norma de conflicto *ad hoc* (en la ley 25.326), se rige por la ley del domicilio en virtud de los arts. 6° y 7° del Código Civil. Ello, independientemente de la sanción que ocasiona la violación por parte del responsable de un banco de datos privado en el plano de la responsabilidad delictual. Mas como la responsabilidad por hechos ilícitos se rige en el derecho internacional privado argentino por el lugar del daño (según una

[17] Sobre el problema específico del ámbito de aplicación en el espacio de las leyes sobre protección de datos personales, ver en general, Rigaux, "La loi aplicable...", cit., ps. 458-60.

[18] Para la determinación del domicilio (argentino, en este caso), con miras al funcionamiento de las normas argentinas de derecho internacional privado, ver Oyarzábal, Mario J. A., "Observaciones generales sobre el estatuto personal en DIPr", *Revista de derecho*, Tribunal Supremo de Justicia de Venezuela, nro. 14, 2004, esp. ps. 172-76, donde se contemplan los casos de domicilio desconocido y de abandono del domicilio extranjero.

interpretación del art. 43 del Tratado de Montevideo de 1940), y el daño lo sufre el individuo generalmente en su domicilio, en la inmensa mayoría de los casos la misma ley que rige la existencia y el contenido del derecho a la vida privada se aplica a las consecuencias de su violación [19].

No hay que subestimar las dificultades de ejecución cuando el responsable del banco de datos tiene su sede en el exterior, sobre todo si el derecho allí vigente le impone obligaciones menos extensas que el derecho aplicable a su responsabilidad. Por esta y otras razones, la aplicación de la ley de la sede del titular del banco de datos, o al menos del establecimiento de la sucursal responsable del tratamiento, podría parecer eficaz [20]. Pero esta solución no tiene sustento en el derecho argentino. Además, la opción por la ley del domicilio del titular de los datos se justifica por razones muy serias: es esa persona a quien las leyes sobre datos personales buscan proteger, y el interés a salvaguardar se localiza en su domicilio; los datos personales son, a menudo, también recogidos allí e incluyen necesariamente el domicilio del interesado, por lo que la aplicación de ese derecho difícilmente pueda tomar por sorpresa al responsable del tratamiento [21].

2. Protección de la intimidad frente a los usuarios de los datos

Es común que en los contratos de apertura de crédito, financiación o préstamo y de otras prestaciones de servicios, el banco o la empresa proveedora utilice datos personales relativos a su co-contratante, puestos a su disposición por terceras personas, generalmente "entidades de información crediticia" cuyo objeto es colectar, operar y proporcionar indicadores sobre la deuda y antecedentes comerciales de la persona consultada [22]. Otras veces, en ausencia de toda relación contractual, una empresa o persona

[19] El art. 43 del Tratado de Montevideo ha sido tradicionalmente interpretado como remitiendo a la *lex loci actus*. No obstante, también es posible, a mi juicio, interpretar que el "hecho lícito o ilícito" se produce donde se sufre el daño; interpretación ésta ya sugerida con anterioridad en otro artículo de mi autoría. Ver Oyarzábal, Mario J. A., "El nombre y la protección de la identidad de las personas. Cuestiones de derecho internacional público y privado", *Prudentia Iuris*, vol. 58, 2004, ps. 90-92.

[20] Ver Rigaux, "La loi applicable...", cit., ps. 470-71 (rechazando este argumento). Otra razón alude a la eficacia de someter a una ley única todas las actividades del responsable del banco de datos.

[21] Cfr. Rigaux, "La loi applicable...", cit., ps. 470-71.

[22] En la Argentina, la principal empresa en información comercial es Veraz, cuyo sitio de Internet es www.veraz.com.ar. Junto con otras empresas del rubro, Veraz integra la Cámara de Empresas de Información Comercial (CEIC) que, a su vez, es miembro del Consejo Consultivo de la Dirección Nacional de Protección de Datos Personales.

puede revelar, adulterar y en general utilizar datos personales de modo que vulnere el derecho al honor y a la intimidad de su titular. En estos casos, como en las relaciones entre los titulares del banco y de los datos, las normas imperativas de la ley del domicilio de la persona protegida deben combinarse con la ley aplicable a la responsabilidad civil del usuario autor de la violación [23].

El carácter ilícito del tratamiento automatizado de datos no afecta necesariamente la validez del contrato para cuya celebración o cumplimiento los datos fueron recabados, que se rige por la *lex contractus* determinada según los arts. 1209, 1210 y concordantes del Código Civil, y que es la misma que rige la responsabilidad *ex delicto* del usuario de los datos en virtud de la segunda parte del art. 43 del Tratado de Montevideo de 1940, que somete sus obligaciones a la "ley que regula las relaciones jurídicas a que responden". Empero, en la jurisdicción argentina sería nulo, por tener objeto prohibido por el orden público, el contrato por el cual una empresa extranjera utiliza datos cuyo tratamiento está vedado por la ley del domicilio del titular de los datos (v. gr., los "datos sensibles" enumerados en el art. 2° de la ley 25.326); o sin haber obtenido el consentimiento del titular de los datos cuando éste es necesario en virtud de una obligación legal; o en una relación de trabajo o de financiación si el tratamiento de datos regulado por las condiciones generales del contrato internacional es alcanzado por una norma de policía protectora del trabajador o del deudor perteneciente al derecho internacional privado argentino o de un país que una norma de conflicto argentina indica como aplicable al caso [24].

3. El rol de la autonomía de la voluntad

Una cuestión poco abordada por la doctrina iusinternacionalprivatista (no ya la argentina, que ha ignorado el tema del tratamiento automatizado de datos completamente, sino también la extranjera), consiste en saber si las partes en un contrato internacional pueden elegir el derecho aplicable al tratamiento (y la protección) de los datos personales, desplazando las normas imperativas del domicilio de la persona cuyos datos se utilizan. Personalmente no veo objeciones, siempre que el derecho elegido —o para el caso, las normas materiales elaboradas por las partes— garanticen una protección adecuada de la privacidad del titular de los datos. Desde este punto de vista, las normas coactivas de la ley 25.326 deben interpretarse

[23] Ver, en general, RIGAUX, "La loi applicable...", cit., ps. 471-74.

[24] Ver, en general, RIGAUX, "La loi applicable...", cit., ps. 473-74; CARRASCOSA GONZÁLEZ, Javier, "Protección de la intimidad...", cit., ps. 422-25.

como "relativamente" imperativas para el caso en que el derecho elegido (o creado) por las partes no ofrezca una protección equivalente a la que garantiza la legislación argentina. Esta autonomía se condice, a mi juicio, con la amplia libertad que el legislador argentino ha dejado a las personas para disponer de sus datos, incluso para consentir su exportación a sabiendas de que el ejercicio de esta libertad puede conducir en los hechos a privar al titular de los datos de toda protección. No obstante, como el titular de los datos es considerado la parte típicamente más débil del contrato, su libertad de contratar se limita por las normas imperativas de su domicilio, que le aseguran un nivel mínimo de protección.

No es desdeñable el potencial que la autonomía de la voluntad acarrea. Cuando el derecho elegido es el de la sede del tratante de los datos, el método de la autonomía permite conciliar la protección de los datos personales garantizados por su ley domiciliaria con la eficacia jurídico-económica de someter todas las actividades del tratante a una misma y única ley[25]. Además, favorece realizar efectivamente una solución uniforme del caso que no siempre se logra por el funcionamiento normal del derecho internacional privado del foro.

Cuando el titular de los datos se domicilia en el extranjero, la facultad de elegir o crear el derecho aplicable se resuelve conforme a su ley personal, incluidas sus normas imperativas, por ejemplo en cuanto prohíben el tratamiento de datos sensibles como los relativos a la salud y a los antecedentes penales. La ley del delito nada tiene que ver aquí. Si no está claro cómo los jueces del domicilio resolverían el caso, habría que investigar la actitud del derecho internacional privado extranjero respecto de la autonomía de la voluntad en materia de estatuto personal, así como el grado de libertad dejado a los particulares en la disposición de sus datos personales dentro del país. Si las dudas persisten, habría que resolver a favor del derecho elegido que garantice una protección de los datos no inferior a la de la ley domiciliaria.

Ocurrido el daño, el titular de los datos podría también convenir el derecho aplicable a la indemnización, ya que, como bien argumenta Boggiano, si la pretensión indemnizatoria se establece en interés del damnificado y éste puede renunciar a la indemnización del daño sufrido, también puede acordar la elección del derecho aplicable a ella[26].

[25] Ver *supra* nota 20 y texto acompañante.

[26] Sobre la eficacia extraterritorial del acto administrativo, en la literatura argentina, ver Boggiano, *Derecho internacional...*, cit., t. II, ps. 872-73.

4. Validez espacial de las previsiones penales argentinas de protección de los datos personales

El principio de la unidad, equivalencia o ubicuidad adoptado en el art. 1°, inc. 1, del Código Penal conduce a la aplicación del derecho argentino, tanto si la acción típica se consuma en la Argentina, como si sus efectos deben producirse en el territorio argentino. Los delitos tipificados consisten en insertar o hacer insertar datos falsos en un archivo de datos personales (art. 117 bis, inc 1°, CPen., incorporado por ley 25.326), revelar información falsa contenida en un archivo de datos personales (art. 117 bis, inc. 2°), acceder ilegítimamente a un banco de datos personales (art. 157, inc. 1°, CPen., incorporado por ley 25.326) y revelar información registrada en un banco de datos cuyo secreto estuviere legalmente obligado a preservar (art. 157, inc. 2°)[27]. El objeto del delito es un banco de datos personales o la información contenida en un banco de datos personales de la República Argentina, que son a los que se refiere la ley 25.326. Las mismas conductas, cuando se perpetran contra bancos de datos o información contenida en bancos de datos extranjeros, no justifican en derecho la aplicación de la ley penal argentina. El sujeto pasivo es el titular del banco de datos o el titular de los datos revelados o falsos con domicilio en el país, ya que sólo las personas domiciliadas en la Argentina pueden registrar un banco de datos personales y reclamar la protección de sus datos personales que prevé la ley.

V. Transferencia internacional de datos personales

Con acierto se ha dicho que el flujo transnacional de datos personales es un fenómeno complejo: "dicho flujo puede afectar a las condiciones de la competencia en el mercado; puede constituir en sí mismo una violación de la intimidad de las personas; puede ser necesario a los fines de un adecuado auxilio judicial o de cumplimiento de normas convencionales; puede afectar a la investigación en sectores específicos, como el sector médico respecto de los datos de los pacientes [; y] puede, finalmente, posibilitar en buen número de ocasiones, el nacimiento de supuestos de responsabilidad *ex delicto* en [derecho internacional privado], ya que los resultados lesivos

[27] Ver, en general, Fontan Balestra, Carlos, *Derecho Penal. Parte especial*, actualizado por Guillermo A. C. Ledesma, 16ª ed. actualizada, Buenos Aires, 2002, ps. 191-95 y 383-85.

pueden producirse en el territorio de un Estado distinto a aquel en el que se encontraban originariamente almacenados los datos" [28].

La ley 25.326 regula la transferencia internacional de datos personales en el art. 12, que dispone:

"1. Es prohibida la transferencia de datos personales de cualquier tipo con países u organismos internacionales o supranacionales, que no proporcionen niveles de protección adecuados.

"2. La prohibición no regirá en los siguientes supuestos:

"a)Colaboración judicial internacional;

"b) Intercambio de datos de carácter médico, cuando así lo exija el tratamiento del afectado, o una investigación epidemiológica, en tanto se realice en los términos del inc. e) del artículo anterior;

"c)Transferencias bancarias o bursátiles, en lo relativo a las transacciones respectivas y conforme la legislación que les resulte aplicable;

"d) Cuando la transferencia se hubiera acordado en el marco de tratados internacionales en los cuales la República Argentina sea parte;

"e)Cuando la transferencia tenga por objeto la cooperación internacional entre organismos de inteligencia para la lucha contra el crimen organizado, el terrorismo y el narcotráfico".

El plexo normativo se completa con el decreto reglamentario 1558/2001, que reza así:

"La prohibición de transferir datos personales hacia países u organismos internacionales o supranacionales que no proporcionen niveles de protección adecuados, no rige cuando el titular de los datos hubiera consentido expresamente la cesión.

"No es necesario el consentimiento en caso de transferencia de datos desde un registro público que esté legalmente constituido para facilitar información al público y que esté abierto a la consulta por el público en general o por cualquier persona que pueda demostrar un interés legítimo, siempre que se cumplan, en cada caso particular, las condiciones legales y reglamentarias para la consulta.

"Facúltase a la Dirección Nacional de Protección de Datos Personales a evaluar, de oficio o a petición de parte interesada, el nivel de protección proporcionado por las normas de un Estado u organismo internacional. Si llegara a la conclusión de que un Estado u organismo no protege adecuadamente a los datos personales, elevará al Poder Ejecutivo Nacional un proyecto de decreto para emitir tal declaración.

[28] Carrascosa González, Javier, "Protección de la intimidad...", cit., ps. 425-26. Cursiva en original. Se ha suprimido la nota al pie.

"El proyecto deberá ser refrendado por los Ministros de Justicia y Derechos Humanos y de Relaciones Exteriores, Comercio Internacional y Culto.

"El carácter adecuado del nivel de protección que ofrece un país u organismo internacional se evaluará atendiendo a todas las circunstancias que concurran en una transferencia o en una categoría de transferencia de datos; en particular se tomará en consideración la naturaleza de los datos, la finalidad y la duración de tratamiento o de los tratamientos previstos, el lugar de destino final, las normas de derecho, generales o sectoriales, vigentes en el país de que se trate, así como las normas profesionales, códigos de conducta y las medidas de seguridad en vigor en dichos lugares, o que resulten aplicables a los organismos internacionales o supranacionales.

"Se entiende que un Estado u organismo internacional proporciona un nivel adecuado de protección cuando dicha tutela se deriva directamente del ordenamiento jurídico vigente, o de sistemas de autorregulación, o del amparo que establezcan las cláusulas contractuales que prevean la protección de datos personales".

El legislador argentino siguió en general las pautas de la Directiva Europea 95/46/CE de 1995 (arts. 25 y 26)[29], que refleja la rica experiencia europea de los años 1980-90 en lo que respecta a la protección y a la libre circulación de los datos. La adopción de normas materiales (y el rechazo de la técnica conflictualista) para regir la transferencia al extranjero de datos personales se justifica plenamente por la importancia de los intereses involucrados, en particular el derecho a la intimidad de las personas, que se vería frecuentemente menoscabado sin un control estatal que impida que los datos recogidos o procesados en el Estado del foro salgan hacia un país con un nivel de protección menor del derecho a la intimidad[30].

El objetivo del art. 12 de la ley 25.326 y su reglamentación es conciliar el libre flujo internacional de datos personales con la protección adecuada del derecho a la intimidad. El principio general es que sólo pueden transferirse datos personales con destino a países que ofrezcan un nivel de protección equiparable (es decir, no inferior) al que presta la legislación argentina (inc. 1). Es responsabilidad del transmisor argentino verificar las condiciones del país receptor. La ausencia de una regulación legal o sectorial protectiva en el país receptor puede suplirse obteniendo el transmisor el consentimiento del titular de los datos para la cesión, o mediante cláusulas contractuales (o de otro tipo) entre el transmisor-cedente argentino y el cesionario extranjero de los datos que acuerden una protección

[29] Ver *infra*, IX.

[30] Ver, en general, CARRASCOSA GONZÁLEZ, Javier, "Protección de la intimidad...", cit., ps. 425-26.

semejante a la de la ley 25.326[31]. No se requiere la autorización previa de la Dirección Nacional de Protección de Datos Personales para la transferencia, ni su aprobación de los contratos o cláusulas contractuales que se utilicen. Es que una subordinación a la obtención de autorizaciones administrativas podría ocasionar la parálisis de muchas actividades modernas. Pero la omisión de adoptar esos recaudos compromete la responsabilidad administrativa, civil y aun penal del transmisor que establece la legislación argentina (art. 31, ley 25.326; art. 1071 bis, CCiv.; y art. 157 bis, inc. 2°, CPen.; respectivamente)[32].

Solamente la transferencia "activa" de datos personales —desde la Argentina (o desde el país donde se encuentra alojada la base de datos[33]) hacia un Estado extranjero o un organismo internacional— está regulada. La "importación" —que tiene por destino la Argentina— es, en principio, libre, en ausencia de una regulación positiva. Si los datos tienen por destino final un tercer país, también este último debe proporcionar un nivel de protección adecuado (art. 12, párr. 5°, dec. 1558/2001). Las condiciones para la transferencia al extranjero de datos personales contenidas en las legislaciones del país de destino inmediato y de destino final (y no solamente el nivel de protección garantizado frente a violaciones ocurridas en o incurridas por personas de esos países) son, a mi juicio, determinantes para evitar que un país sea utilizado como estación de tránsito y los datos acaben en otro país con un insuficiente nivel de protección de la intimidad.

Un problema se plantea cuando el importador extranjero no cumple voluntariamente con las condiciones de la cesión, ocasionando un perjuicio al titular argentino de los datos. Para Pablo Palazzi, cuyo libro sobre las transferencias internacionales de datos personales sugiero consultar para un análisis detallado del tema[34], el art. 11, inc. 4, de la ley 25.326 "aplica la ley argentina de datos personales a aquellos que reciban datos (incluso aunque estén en el exterior) para asegurarse que la información personal seguirá amparada por la ley"[35]. Esa disposición sujeta al cesionario a las

[31] Ver, en general, Palazzi, Pablo A., "Breve comentario al decreto reglamentario de la ley 25.326", *Derecho y nuevas tecnologías*, 2003-4/5, p. 346.

[32] Ver Gils Carbó, Alejandra M., "La prohibición de transferencia internacional de datos personales (contra los paraísos informáticos)", *Derecho y nuevas tecnologías*, 2000-3-30.

[33] Ver *supra*, § III, 2.

[34] Palazzi, Pablo A., *La transmisión internacional de datos personales y la protección de la privacidad*, Ad-Hoc, Buenos Aires, 2002.

[35] Chacón de Albuquerque, Roberto - Palazzi, Pablo A., "Necesidad de armonizar el derecho a la protección de datos personales en el MERCOSUR", *Derecho y nuevas tecnologías*, 2003-4/5, p. 553.

mismas obligaciones legales y reglamentarias del cedente, a quien, a su turno, responsabiliza solidariamente por la violación de la ley que realice el cesionario. Traducido a términos de mi especialidad, esta norma sería de orden público, no sólo interno, sino también internacional (art. 14, inc. 2, CCiv.), pudiendo calificársela como *norma de policía del derecho internacional privado argentino*. Es una interpretación razonable, que se justifica por el objetivo de la ley 25.326 de proteger a las personas domiciliadas en la Argentina cuyos datos fueron exportados hacia un país con un inadecuado nivel de protección de la privacidad. Empero, si el país de destino protege adecuadamente los datos personales, entonces el art. 11, inc. 4, se aplica solamente cuando el derecho argentino resulta aplicable en virtud de la norma de conflicto del art. 43 del Tratado de Montevideo de 1940. Esta diferenciación se impone, a mi juicio, por el principio por el cual las normas de policía deben interpretarse restrictivamente, en la medida en que resulta indispensable para satisfacer el fin del legislador, que tiende aquí a proteger la privacidad de los residentes argentinos. Cuando el país extranjero proporciona un nivel de protección adecuado, la remisión *a priori* e inflexiblemente al derecho argentino es injustificada, incluso contraria al otro objetivo del legislador, consistente en facilitar la circulación de los datos personales. Según lo veo, también sería abusivo someter apriorísticamente al derecho argentino la responsabilidad del cesionario extranjero de datos pertenecientes a no-residentes de la República Argentina procedentes de un banco de datos de nuestro país, cuando el derecho argentino no les brinda protección legal alguna.

Finalmente, la ley 25.326 reconoce que algunos flujos internacionales de datos personales (datos médicos; de transferencias bancarias o bursátiles; cooperación de inteligencia para la lucha contra el crimen organizado, el terrorismo y el narcotráfico; y auxilio judicial internacional) deben quedar sustraídos del régimen jurídico general para integrarse en los regímenes jurídicos particulares propios del contexto en que tales flujos se desarrollan, a fin de evitar cercenar la unidad de regulación de cada una de estas actividades (art. 12, inc. 2)[36].

[36] Cf. Carrascosa González, Javier, "Protección de la intimidad...", cit., p. 429 (comentando el art. 33 de la Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de Datos de Carácter Personal de España (conocida como LORTAD, y actualmente reemplazada por la Ley Orgánica 19/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal), en que el art. 12, inc. 2, de la ley argentina 25.326 se basó). Por ejemplo, los establecimientos financieros están actualmente afiliados a un sistema informático universal: SWIFT (Society for Worldwide Interbank Financial Telecommunications). Para una síntesis de la política de SWIFT sobre privacidad de los

VI. Jurisdicción internacional argentina

El art. 36 de la ley 25.326 establece que será competente para entender en las acciones de protección de los datos personales el juez del domicilio del actor, el del domicilio del demandado, el del lugar en que el hecho o el acto se exteriorice o pudiera tener efecto, a elección del actor (primer párrafo). Procede la competencia federal cuando la acción se interponga en contra de archivos de datos públicos de organismos nacionales (inc. a) y cuando los archivos de datos se encuentren interconectados en redes interjurisdiccionales, nacionales o internacionales (inc. 2). Naturalmente que en esta última hipótesis, la jurisdicción internacional argentina es un presupuesto de la competencia federal.

Ahora bien, el primer párrafo del art. 36 constituye una norma de competencia territorial (interna), no de jurisdicción internacional. Y aunque se podría aplicar por analogía, ante la ausencia de normas de jurisdicción internacional específicas en la ley 25.326[37], existe un riesgo grave: la posibilidad de que los tribunales argentinos se consideren dotados de jurisdicción para entender en casos sin contactos siquiera mínimos con el foro. Sería suficiente determinar cualquier acto o efecto en la Argentina (por ejemplo, que el tratamiento automatizado de los datos personales se realice en la Argentina o que los datos sean accesibles a través de Internet desde una computadora en la Argentina) para que nuestros tribunales pudieran asumir jurisdicción internacional. La internacionalización del art. 36 conduce a una multiplicación de jurisdicciones argentinas exorbitantes, cuya consecuencia es el muy probable desconocimiento de sentencias nacionales dictadas en casos donde las personas o el banco de datos no se encuentran en territorio argentino.

En estas circunstancias, se me ocurre una única alternativa: aplicar, también por analogía, el art. 56 del Tratado de Derecho Civil Internacional de Montevideo de 1940, que permite a los jueces argentinos asumir jurisdicción cuando el derecho aplicable a la protección de los datos o a la responsabilidad delictual es el argentino, o el demandado está domiciliado en nuestro país. Como la protección de los datos personales se rige por el derecho del domicilio de su titular, y el titular-demandante debe estar domiciliado en Argentina para que el derecho argentino resulte aplicable, el *forum causae* conduce en la práctica al habilitamiento de un *forum actoris*

---

datos personales identificados, recolectados y compartidos con motivo del uso del Sistema, ver http://www.swift.com/index.cfm?item_id=1037.

[37] Ver, en general, Boggiano, Antonio, "Jurisdicción internacional y competencia interna" (nota a la sentencia de la C. Nac. Com., sala A, 20/10/1970), JA 1971-XI-195 y ss.

argentino. La jurisdicción así determinada no es prorrogable a favor de jueces o árbitros extranjeros. Cuando las partes hayan elegido la aplicación de un derecho extranjero, habría que admitir igualmente la jurisdicción argentina conducente a evitar la denegación de justicia (doctrina "Vlasof")[38].

VII. Casos ajenos a la ley 25.326. Derecho aplicable y jurisdicción internacional argentina

Las relaciones jurídicas entre el responsable de un banco de datos y los usuarios de dichos datos (v. gr., por suministrar información falsa o incorrecta), y entre el cedente local de datos personales y el cesionario extranjero (v. gr., por incumplimiento de las condiciones de la cesión) son supuestos típicamente ajenos a un régimen de protección de los datos personales. La excepción viene dada cuando una norma de policía del derecho internacional privado responsabiliza al cedente por las obligaciones del cesionario extranjero, como medio de reforzar la protección de los datos personales, como es el caso del art. 11, inc. 4, de la ley 25.326. Es lógico que el derecho del cedente de repetir del cesionario lo que pagó por indemnización de daños al titular de los datos o en concepto de multa al órgano público de control, quede también sometido al derecho argentino. Allende este supuesto, los derechos y obligaciones entre los responsables de bancos de datos y sus usuarios, y entre cedentes y cesionarios de datos, se rigen por el derecho aplicable al contrato o a la responsabilidad delictual a que responden (arts. 1209 y 1210, CCiv.; y art. 43, Tratado de Montevideo de 1940; respectivamente). Como siempre, la jurisdicción depende del derecho aplicable y del domicilio del demandado (arts. 1215 y 1216, CCiv.; art. 56, Tratado de Montevideo de 1940; respectivamente).

VIII. El conflicto de leyes interjurisdiccional interno

En adición al régimen federal, varias provincias han garantizado la protección de los datos de carácter personal en sus constituciones (v. gr., art. 16, Constitución de la Ciudad Autónoma de Buenos Aires; art. 20, inc. 3, Constitución de la Provincia de Buenos Aires; art. 50, Constitución de la Provincia de Córdoba; art. 19, Constitución de la Provincia del Chaco; art. 56, Constitución de la Provincia del Chubut; art. 23, incs. 6 a 8, Constitución de la Provincia de Jujuy; art. 20, Constitución de la Provincia de Río Negro;

[38] Corte Sup., 21/3/1960, Fallos 246:87; JA 1960-III-216; con comentario de Werner Goldschmidt, LL 98-287.

art. 89, Constitución de la Provincia de Salta; art. 26, Constitución de la Provincia de San Juan; art. 21, Constitución de la Provincia de San Luis; y art. 45, Constitución de la Provincia de Tierra del Fuego, Antártida e Islas del Atlántico Sur) y legislación procesal (v. gr., ley 4244 de la Provincia del Chubut[39]; ley 3794 de la Provincia de Misiones[40]; ley 2307 de la Provincia del Neuquén[41]; ley 3246 de la Provincia de Río Negro[42]; ley 6296 de la Provincia de Santiago del Estero[43]; y Código Procesal Constitucional de la Provincia de Tucumán, art. 67[44]). Esas normas reglamentan la *acción* de protección de los datos personales o de *habeas data* o de amparo especial en jurisdicción provincial. Los principios sustantivos de la protección de datos, incluidos los derechos de sus titulares y las obligaciones de usuarios y responsables de bancos de datos, se rigen por la ley nacional 25.326, cuyos capítulos I a IV son de aplicación en todo el territorio nacional (art. 44).

Nada obsta, empero, a que una provincia regule el tratamiento de datos personales en el ámbito de su competencia. Por ejemplo, la Ciudad Autónoma de Buenos Aires, en su función de autoridad sanitaria, prohíbe a los profesionales de la salud hacer pública la información genética de las personas; prohibición que se extiende a las compañías de seguro, obras sociales, empresas de medicina prepaga o aseguradoras de riesgos del trabajo que actúan, se supone, en territorio porteño (ley 712 de Garantías al Patrimonio Genético Humano[45]). Por su parte, la Provincia de Mendoza ha regulado las actividades de las empresas privadas que suministran información sobre antecedentes comerciales, financieros y/o bancarios en territorio mendocino (ley 7251 de Creación del Registro de Empresas Privadas de Información de Deudores[46]); y en una norma de autolimitación del tenor del art. 2° de la ley 25.326, protege la "información sensible" de las personas físicas o jurídicas que tengan domicilio o sucursal en la provincia de Mendoza exclusivamente (art. 2°, inc. c).

Como ocurre con los bancos de datos del gobierno federal, la protección de la privacidad frente a los órganos de los Estados provinciales y sus entes descentralizados se rige por el derecho administrativo propio. Una provincia no podría, empero, restringir la protección de los datos que

[39] BO (Chubut) del 31/12/1996.

[40] BO (Misiones) del 19/11/2001.

[41] BO (Neuquén) del 4/2/2000.

[42] BO (Río Negro) del 7/12/1998.

[43] BO (Sgo. del Estero) del 12/7/1996.

[44] Aprobado por ley 6944; BO (Tucumán) del 8/3/1999.

[45] BO (CABA) del 17/1/2002.

[46] BO (Mendoza) del 15/10/2004.

garantiza a todos los habitantes de Argentina la ley 25.326, que es de orden público nacional (art. 44), por el principio de supremacía del derecho federal (art. 31, CN). Únicamente la Capital ha optado por legislar integralmente el tratamiento de datos personales asentados en archivos del sector público local. La ley 1845 de Protección de Datos Personales de la Ciudad Autónoma de Buenos Aires[47] contempla incluso la transferencia interprovincial e internacional de los datos. Se prohíbe la transferencia a cualquier provincia o municipio cuya administración pública no proporcione niveles de protección adecuados a los establecidos por la ley nacional 25.326 o la propia ley (art. 11, inc. 1). La prohibición no rige en los supuestos de cooperación judicial interjurisdiccional y de intercambio de información entre los respectivos organismos provinciales o nacionales dentro del marco de sus competencias, a requerimiento de la autoridad judicial y en el marco de una causa, así como en las hipótesis de los incs. 2 b), c) y e) del art. 12 de la ley 25.326 (art. 11, inc. 2, ley 1845). El art. 12, que regula la transferencia de datos públicos provinciales al exterior, es idéntico a su homónimo de la ley nacional. Me hago dos preguntas. La primera es si una provincia puede establecer requisitos más laxos para la transferencia internacional de datos que los establecidos en el art. 12 de la ley 25.326. La respuesta es negativa, porque se introduciría una fuga en el sistema nacional de protección de la privacidad. El art. 12, en cuanto prohíbe la transferencia de datos con países que no proporcionen un nivel de protección adecuado, es de orden público y vincula tanto a los responsables de bancos privados como al gobierno federal y los gobiernos provinciales por igual. Teóricamente, las provincias sí podrían establecer condiciones más restrictivas para la transferencia al extranjero que la ley nacional, por ejemplo, requiriendo el consentimiento del titular de los datos en todos los casos, siempre, claro está, que no exista una norma de derecho internacional que obligue a la transferencia. La segunda pregunta es si una provincia puede prohibir la transferencia de datos, no sólo de los bancos públicos sino también de los privados localmente regulados, a otra provincia argentina o al gobierno federal. Creo que sí, con dos limitaciones: si lo ordena una norma federal o lo exige el interés nacional, por ejemplo, para controlar una epidemia.

Volviendo a la acción de *habeas data*, están legitimados para interponerla, en jurisdicción provincial, los habitantes de las provincias respectivas (a quienes las constituciones y leyes provinciales primariamente se dirigen), así como los de las otras provincias argentinas en virtud del art. 8° de la Constitución Nacional, que establece que los ciudadanos de cada

[47] Vetada parcialmente por dec. 1914/2006: BO (CABA) del 29/12/2005.

provincia gozan de todos los derechos de los ciudadanos de las demás[48]. Los sujetos pasivos son típicamente el Estado provincial y los municipios que son titulares de un banco de datos público y los responsables de bancos de datos privados con asiento en el territorio de la provincia. En ocasiones, también los usuarios del banco de datos (ley de Chubut, art. 4°; ley de Misiones, art. 4°; ley de Río Negro, art. 6°), asimismo, se supone, domiciliados o con sucursal en la jurisdicción. La ley de *habeas data* de Misiones también comprende en su ámbito de aplicación a los responsables de bancos de datos privados con asiento fuera de la provincia (¿incluso en otro país?), pero "que generen hechos o actos que se exterioricen o pudieren tener efectos en ella" (art. 1°), por ejemplo, cuando alguna de las fases del tratamiento se realiza en territorio misionero o el titular de los datos está domiciliado allá (?). Empero, como en estos casos lo más seguro es que estén involucrados bancos de datos interconectados en redes interjurisdiccionales, nacionales o internacionales, será procedente la competencia federal en virtud del art. 36, inc. b), de la ley 25.326. Allende este supuesto, la competencia federal también procede por aplicación del art. 116 de la Constitución Nacional, a elección del actor, en las causas en que sean parte un vecino de la provincia en que se suscite el pleito y un vecino de otra, o una provincia y un vecino de otra[49]. En este último caso, hay que distinguir según que se trate de bancos de datos gestionados por los poderes ejecutivo, legislativo o judicial provincial, en cuyo caso tiene competencia originaria la Corte Suprema de Justicia de la Nación; y de los gestionados por sus reparticiones autárquicas, en que intervienen los tribunales federales inferiores. La vecindad se configura por la residencia continua de dos años en la provincia o por tener en ella propiedades raíces, o un establecimiento de industria o de comercio, o por hallarse establecido de modo que aparezca el ánimo de permanecer (art. 11, ley 48). En el caso de sociedades anónimas, se las considera vecinas de la provincia en que se encuentran establecidas y haciendo sus negocios (art. 9°, ley 48). Deberá atenderse tanto a la sede central como a la sucursal que posean en la provincia para los actos allí realizados[50]. Para las otras formas societarias, la vecindad de sus socios es relevante (aplicación analógica del art. 10 de la ley 48)[51].

[48] Ver, en general, Bidart Campos, Germán J., *Tratado elemental de derecho constitucional argentino*, t. I-A, Ediar, Buenos Aires, 1999-2000, ps. 663-64.

[49] Existe un estudio no superado sobre la jurisdicción y la competencia de los tribunales federales, al que remitimos *in totum*, Haro, Ricardo, *La competencia federal - Doctrina. Legislación. Jurisprudencia*, Depalma, Buenos Aires, 1989, con prólogo de Germán J. Bidart Campos.

[50] Cfr. Haro, Ricardo, *La competencia...*, cit., ps. 193-94.

[51] Haro, Ricardo, *La competencia...*, cit., p. 194.

IX. La cooperación internacional en materia de protección de la privacidad. El tema en el derecho de la integración

Existe conciencia de que un fenómeno tan complejo e intrínsecamente internacional como es el tratamiento de los datos personales no puede ser controlado únicamente mediante legislaciones nacionales[52]. Varias organizaciones internacionales se han interesado en el problema. En 1980, la Organización para la Cooperación y el Desarrollo Económico (OCDE) adoptó las *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*[53] (Directrices sobre Protección de la Privacidad y Flujos Transfronterizos de Datos Personales), que continúan representando el consenso internacional sobre los principios que deben guiar a los gobiernos, a las empresas y a la sociedad civil en la protección de la privacidad y los datos personales sin introducir restricciones innecesarias al flujo de datos. Las Naciones Unidas han adoptado los *Principios Rectores para la Reglamentación de los Ficheros Computadorizados de Datos Personales*[54], aprobados por la Asamblea General por resolución 45/95 de 14 de diciembre de 1990, que establecen las garantías mínimas que deben proporcionase en toda legislación nacional en relación con la recolección, almacenamiento, uso y transmisión de archivos de datos personales informatizados. Los principios incluyen: exactitud, especificación y contenido, no discriminación, seguridad y libre transmisión de datos a través de fronteras en presencia de salvaguardias comparables. En la Organización Mundial del Comercio (OMC), el art. XIV.c.ii del *Acuerdo General sobre el Comercio de Servicios (GATS)*[55], negociado en la Ronda Uruguay en 1995, reconoce el derecho de los países miembros a tomar las medidas necesarias para proteger la privacidad de las personas en relación con el procesamiento y la divulgación de datos personales, así como respecto al carácter confidencial de los registros y cuentas individuales. La OMC estableció en 1998 un programa de trabajo sobre el comercio electrónico, en el cual se abordan cuestiones vinculadas con la privacidad en

[52] Para un raconto de las principales iniciativas internacionales sobre este problema en las décadas de 1980 y 1990, ver Saravalle, Alberto, "Brevi osservazioni...", cit., p. 46, nota 10.

[53] Disponibles en el sitio de Internet de la OCDE en *http://www.oecd.org/document/53/0,2340,en_2649_34255_15589524_1_1_1_1,00.html* (en inglés y en francés, con un resumen en español).

[54] Disponible en Internet en *http://193.194.138.190/spanish/html/menu3/b/71_sp.htm*.

[55] Disponible en el sitio de Internet de la OMC en *http://www.wto.org/spanish/docs_s/legal_s/26-gats.pdf*.

Internet[56]. También en 1998, la Cámara de Comercio Internacional (CCI) adoptó *Cláusulas Modelo para la Utilización en Contratos que Involucran la Transferencia de Datos Personales*[57], las cuales aseguran al titular de los datos un recurso contra el exportador de los datos si el importador de los mismos, en un país que no tiene protección adecuada según la jurisdicción del exportador, viola una regla de privacidad de acuerdo con las leyes del país exportador. Otras iniciativas destinadas a proteger la privacidad en el comercio electrónico han sido tomadas por la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI), la Organización Internacional para la Estandarización (ISO), la Unión Internacional de Telecomunicaciones (UIT), la Organización Mundial de la Propiedad Intelectual (OMPI) y la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO). Incluso la Conferencia de La Haya de Derecho Internacional Privado se ocupó del tema en su sesión de 1988[58], que sin embargo no ha tenido seguimiento. Finalmente, en el ámbito interamericano, el Comité Jurídico Interamericano de la OEA ha elaborado un *Anteproyecto de Convención Americana sobre Autodeterminación Informativa*[59], que se basa en el Convenio del Consejo de Europa de 1981[60], cuyo objeto consiste en garantizar, en el territorio de cada Estado Parte, a cualquier persona física o jurídica, sean cuales fueren su nacionalidad, residencia o domicilio, el respeto de sus derechos fundamentales, concretamente, su derecho a la autodeterminación informativa con relación a su vida privada y demás derechos de la personalidad, así como la defensa de su libertad e igualdad con respecto al tratamiento automatizado o manual de los datos correspondientes a su persona o bienes (art. 1°)[61].

[56] Ver *http://www.wto.org/spanish/tratop_s/ecom_s/ecom_s.htm*.

[57] Disponibles en el sitio de Internet de la CCI en *http://www.iccwbo.org/id911/index.html* (en inglés).

[58] Ver Pelichet, Michel, "Note on Conflict of Laws Occassioned by Transfrontier Data Flows", en *Conférence de La Haye de droit international privé. Actes et documents de la Seizième session (3 au 20 octobre 1988)*, t. I, *Matières diverses*, La Haya, 1991, ps. 113 y ss.

[59] Ver Organización de los Estados Americanos (OEA), *Informe anual del Comité Jurídico Interamericano a la Asamblea General*, OEA/Ser.G, CP/doc.3272/00, 25/8/2000. El Anteproyecto está disponible en Internet en *http://www.ulpiano.com/convencion.htm* (última visita: 18/6/2006).

[60] A diferencia del modelo europeo, el Anteproyecto de Convención Americana contempla los datos de las personas tanto físicas como jurídicas o a sus bienes que figuren en registros, ficheros o bancos de datos de los sectores público y privado, sean éstos automatizados o manuales.

[61] Ver comentario de Palazzi, Pablo A., *La transmisión...*, cit., ps. 49-52.

En las últimas décadas, la mayoría de los países con régimen democrático liberal ha adoptado legislación protectora de la privacidad que en mayor o menor medida sigue los parámetros internacionales, lo que ha provocado un interesante —si no óptimo— nivel de armonización del derecho de los datos informatizados.

El mayor grado de armonización legislativa alcanzado hasta el presente sobre el tratamiento de los datos personales es entre los países europeos[62]. El primer instrumento vinculante (incluso en el mundo) es el *Convenio 108 del Consejo de Europa de 28 de enero de 1981 para la Protección de las Personas con Respecto al Tratamiento Automatizado de Datos de Carácter Personal*[63], que enuncia los principios básicos de la protección de datos que actualmente rigen en los países europeos. Empero, la coordinación legislativa vendría de la mano de la *Directiva 95/46 del Parlamento Europeo y del Consejo de 24 de octubre de 1995 relativa a la protección de las Personas Físicas en lo que Respecta al Tratamiento de Datos Personales y a la Libre Circulación de estos Datos*[64], que retoma y amplía el régimen del Convenio y crea un marco regulador destinado a establecer un equilibrio entre un nivel elevado de protección de la vida privada de las personas y la libre circulación de datos personales dentro de la Unión Europea y, con ese objeto, fija límites estrictos para la recogida y utilización de los datos personales y solicita la creación, en cada Estado miembro, de un organismo nacional independiente encargado de la protección de los mencionados datos. El régimen se completa con la *Directiva 2002/58/CE del Parlamento Europeo y del Consejo de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la pro-*

[62] Ver, en general, Rigaux, François, "Libre circulación de datos y protección de la vida privada en el espacio europeo", JA, 5/1/2005. Para una excelente síntesis del sistema europeo, ver De Frutos Gómez, José M., "El régimen de la Unión Europea sobre la protección de datos personales", ponencia presentada en el IV Encuentro Iberoamericano de Protección de Datos Personales, realizado en la Ciudad de México del 1 al 4 de noviembre de 2005; disponible en Internet en http://www.ifai.org.mx/eventos/2005/ene_Ibero/ponencias/jfrutos.pdf. (El Sr. Gómez Frutos es Administrador Principal de la Unidad de Protección de Datos Personales de la Dirección General de Justicia, Libertad y Seguridad de la Comisión Europea).

[63] Una traducción al español del Convenio está disponible en *https://212.170.242.148/upload/Canal_Documentacion/legislacion/Consejo%20de%20Europa/Convenios/B.28)%20CONVENIO%20N%BA%20108%20DEL%20CONSEJO%20DE%20EUROPA.pdf*. El texto auténtico, en inglés y francés, del Convenio está disponible en el sitio de Internet del CE en *http://conventions.coe.int/Treaty/Common/QueVoulezVous.asp?NT=108&CM=8&DF=6/21/2006&CL=ENG*.

[64] Diario Oficial L 281 de 23/11/1995, ps. 31-50; también disponible en el sitio de Internet de la UE en *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:ES:HTML*.

tección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas)[65], la *Directiva 2006/24/CE del Parlamento Europeo y del Consejo de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE*[66] y el *Reglamento CE 45/2001 del Parlamento Europeo y del Consejo de 18 de diciembre de 2000 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos*[67]. Es preciso agregar que la protección de los datos de carácter personal fue expresamente reconocida como un derecho fundamental de la persona humana en la *Carta de los Derechos Fundamentales de la Unión Europea* (art. 8)[68], derecho que también aparece en el proyecto de tratado por el que se establece la *Constitución Europea* (art. I-51)[69]. Finalmente, debe citarse el *Convenio Para la Protección de los Derechos Humanos y de las Libertades Fundamentales del Consejo de Europa de 1950*[70], cuyo art. 8°, que reconoce el derecho de toda persona a su vida privada, ha sido utilizado por la Corte Europea de Derechos Humanos (CEDH) para decidir los temas relativos a la protección de los datos personales. En el ámbito jurisprudencial, merecen destacarse dos sentencias del Tribunal de Justicia de las Comunidades Europeas (TJCE) dictadas en 2003, afirmando la aplicabilidad de la Directiva 95/46 a las actividades de tratamiento de datos que se realizan en territorio comunitario, aun cuando no presenten

[65] Diario Oficial L 201 de 31/7/2002, ps. 37-47; también disponible en el sitio de Internet de la UE en *http://europa.eu.int/eur-lex/pri/es/oj/dat/2002/l_201/l_20120020731es00370047.pdf.*

[66] Diario Oficial L 105 de 13/4/2006, ps. 54-63; también disponible en el sitio de Internet de la UE en *http://eur-lex.europa.eu/LexUriServ/site/es/oj/2006/l_105/l_10520060413es00540063.pdf.*

[67] Diario Oficial L 8 de 12/1/2001, ps. 1-22; también disponible en el sitio de Internet de la UE en *http://europa.eu/eur-lex/pri/es/oj/dat/2001/l_008/l_00820010112es00010022.pdf.*

[68] Diario Oficial C 364 de 18/12/2000, ps. 1-22; también disponible en el sitio de Internet de la UE en *http://www.europarl.europa.eu/charter/pdf/text_es.pdf.*

[69] Disponible en el sitio de Internet de la UE en *http://europa.eu/constitution/es/lstoc1_es.htm.*

[70] Una traducción al español del Convenio está disponible en el sitio de Internet de la CEDH en *http://www.echr.coe.int/NR/rdonlyres/1101E77A-C8E1-493F-809D-800CBD20E595/0/Spanish/Espagnol.pdf.* El texto auténtico, en inglés y francés, del Convenio está disponible en el sitio de Internet del CE en *http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=005&CM=8&DF=6/21/2006&CL=ENG.*

un vínculo directo con la libertad de circulación garantizada por el Tratado Constitutivo de la Comunidad Europea (es decir, aunque se trate de operaciones puramente nacionales). En los casos "Österreichischer Rundfunk y otros"[71], y "Bodil Lindqvist s/cuestión prejudicial"[72], el TJCE fundamentó esta interpretación en el objetivo de la Directiva de establecer un régimen apropiado para la protección del derecho a la intimidad de las personas en lo que respecta al tratamiento de los datos personales y que elimine los obstáculos al funcionamiento del mercado interior que derivan de las disparidades entre las legislaciones nacionales.

La armonización de las legislaciones nacionales en materia de privacidad resulta igualmente necesaria entre los países del Mercosur para concretizar el establecimiento del mercado común que comanda el Tratado de Asunción. El objetivo de armonización se ve dificultado, sin embargo, por el hecho de que no todos los Estados miembros del Mercosur poseen aún una normativa óptima protectora de la intimidad[73]. De hecho, Argentina es el único país del Mercosur —y aun de América Latina— que ha recibido el reconocimiento de país con un nivel adecuado de protección por lo que respecta a los datos personales transferidos desde la Comunidad Europea[74].

En lo que respecta al ámbito supranacional subregional, el tema de la protección de datos personales está siendo tratado por el Subgrupo de Trabajo nro. 13 "Comercio electrónico", que ya ha elaborado un proyecto de norma sobre "Protección de datos personales y libre circulación de datos" del Mercosur. El proyecto ha sido elaborado sobre la base de un estudio comparativo de las legislaciones protectoras de la intimidad de los países miembros del Mercosur y con la normativa europea. En la XIV Reunión Ordinaria del Subgrupo de Trabajo los días 19 y 20 de marzo de 2005 en

[71] Casos acumulados C-465/00, C-138/01 y C-139/01, sent. del 20/5/2003.

[72] Caso C-101/01, sent. del 6/11/2003.

[73] Entre los países miembros y asociados del Mercosur, sólo en Chile y Paraguay se han dado legislaciones protectoras de la privacidad que contienen principios sobre protección de los datos personales (Chile: ley 19.628 sobre Protección de la Vida Privada, Diario Oficial del 28/8/1999; Paraguay: ley 1682 "que reglamenta la información de carácter privado", Diario Oficial del 16/1/2001). Bolivia, Brasil y Uruguay carecen de una ley de protección de datos, si bien es posible encontrar en sus textos constitucionales y/o legales algunos principios parciales. Para un análisis de los regímenes de privacidad en los países del Mercosur, ver Palazzi, Pablo A., *La transmisión...*, cit., ps. 63-65, 70-77, 93 y 171-95.

[74] Comisión de las Comunidades Europeas, Decisión C(2003) 1731, del 30/6/2003: Diario Oficial L 168 del 5/7/2003; también disponible en el sitio de Internet de la Comisión en *http://ec.europa.eu/justice_home/fsj/privacy/docs/adequacy/decision-c2003-1731/decision-argentine_es.pdf*.

Asunción del Paraguay, las delegaciones acordaron remitir las consideraciones sobre el proyecto de norma a la delegación argentina, la que será la encargada de circular la primera versión revisada de la propuesta. El proyecto de norma Mercosur, una vez adoptado, se adaptará al formato de un proyecto de Decisión (del Consejo del Mercado Común)[75].

Allende lo expuesto, la única norma aprobada hasta el presente por un órgano comunitario es la *relativa a los procedimientos y seguridad en el intercambio y consulta de datos obrantes en los sistemas informáticos aduaneros*, adoptada por Decisión del Consejo del Mercado Común 19/2005 de 14/12/2005[76]. La norma tiene por objetivo implementar entre los Estados Parte un enlace informático, a través del cual podrán intercambiar información o efectuar consultas de las bases de datos obrantes en las respectivas administraciones aduaneras, a los fines de prevenir, investigar y combatir los ilícitos aduaneros, agilizar las prácticas comerciales y el intercambio eficaz de información (art. 1°). Con esos fines solamente, se autoriza la transferencia y utilización de datos personales relativos a personas físicas y jurídicas, salvo los relativos al origen racial, opiniones políticas, convicciones religiosas, salud o vida sexual (art. 4°). La administración aduanera de cada Estado Parte es responsable de la fase del tratamiento de los datos que lleva a cabo, conforme a sus leyes internas (arts. 11, 13 y 16), las que deberán garantizar un grado de protección y confidencialidad adecuados (art. 5°, inc. 1). En ausencia de normas internas o de menor nivel de protección, se aplican las normas de la presente normativa (art. 5°, inc. 2).

X. Consideraciones finales

Desde la órbita del derecho internacional, tanto público como privado, la ley argentina de Protección de Datos Personales es bastante satisfactoria. La ley favorece la transferencia internacional de datos personales hasta el límite que permite el respeto al derecho a la intimidad; conciliando adecuadamente dos valores tan fundamentales como antagónicos: el de la preeminencia del respeto a los derechos del hombre, con el de la libertad de información entre los pueblos, necesario para alcanzar el desarrollo económico y social.

Dicho ello, el régimen jurídico establecido en la ley 25.326 suscita algunas críticas. En primer lugar, deja fuera del ámbito de protección legal a la mayoría de los datos personales registrados en los archivos de las

[75] Cf. MERCOSUR/SGT nro. 13/Acta 1/2005, § 2.2.

[76] Disponible en el sitio de Internet del Mercosur en *http://www.mercosur.int*.

embajadas y consulados argentinos en el exterior. Es que, como vimos [77], la ley restringe la protección que organiza a una categoría determinada de destinatarios: las personas con domicilio legal en el país (art. 2°). Como los "libros de matrícula" y otros ficheros que llevan las representaciones se conforman principalmente —si no únicamente— de datos de personas residentes en el exterior (los domiciliados en el territorio que cubre la respectiva misión), esas personas no son "titulares de los datos" en el sentido de la ley 25.326. Situación ésta que es grave y paradójica. Es grave, si se recuerda que los ficheros de las embajadas y consulados están exentos de la jurisdicción del Estado receptor; con lo que la persona cuya privacidad ha sido menoscabada no puede ampararse en ningún sistema nacional de protección. Y es paradójica si se tiene en cuenta que las representaciones argentinas en el extranjero, en tanto que órganos del Estado argentino, sí están sometidas a las obligaciones (y los funcionarios están sujetos a las sanciones) legales y administrativas que establece la ley 25.326 (art. 1°). Frente a este sistema incompleto de protección, creo que a las víctimas de las violaciones sólo les queda prevalerse de una normatividad superior constitucional (art. 43 de la Constitución Nacional que reconoce el *habeas data*) e internacional (art. V, Declaración Americana de los Derechos y Deberes del Hombre; art. 12, Declaración Universal de Derechos Humanos; art. 11, Pacto de San José de Costa Rica; art. 17, Pacto Internacional de Derechos Civiles y Políticos; art. 16, Convención sobre los Derechos del Niño; etc., que garantizan el derecho a la vida privada) para reclamar reparación.

La segunda reflexión se refiere a la transferencia de datos personales intersocietaria con empresas jurídicamente vinculadas que actúan en el exterior. Como las disposiciones de la ley 25.326 se aplican sólo a los bancos de datos "destinados a dar informes" (art. 1°), parece posible que responsables argentinos de un archivo de datos compartan datos personales con empresas pertenecientes al mismo grupo económico —y aun con empresas no afiliadas— radicadas en países que no proporcionan niveles adecuados de protección, si ello no es considerado "proveer informes", escapando a las reglas de la ley. Aunque existe la tendencia jurisprudencial a considerar que todos los bancos de datos —estén o no destinados a proveer informes— deben cumplir con los recaudos de la ley 25.326 [78], la expansión del accionar de las sociedades multinacionales, del que no

[77] Ver *supra*, IV, 1.

[78] Cf. Palazzi, Pablo A., *La transmisión...*, cit., p. 70.

es ajena la Argentina, quizás habría merecido una atención específica del legislador[79].

La última crítica es la falta también de previsión legislativa de una norma de conflicto que indique el derecho aplicable a la protección de la intimidad frente al tratamiento de datos personales en la ley 25.326. Efectivamente, la ley omite especificar qué derecho rige tanto la existencia y contenido del derecho a la vida privada, en el mejor de los casos cuando el titular de los datos tiene domicilio en el extranjero, como qué derecho gobierna en todos los casos la responsabilidad civil por la violación. Ello deja al jurista —juez o académico— un margen demasiado amplio para la interpretación. Baste recordar que existen argumentos doctrinarios para extraer a los derechos de la personalidad (entre los que se cuenta al derecho a la intimidad) del ámbito del estatuto personal y plantear el problema en el campo de la responsabilidad extracontractual[80], y que aún la cuestión de qué ley rige los actos ilícitos es materia disputada en el derecho internacional privado argentino[81].

XI. Bibliografía

Argentina

Ciuro Caldani, Miguel Ángel, "Los perfiles de la persona en el DIPr. argentino", *Investigación y docencia*, nro. 7, 1988, ps. 49-53.

De Slavin, Diana, *MERCOSUR: la protección de los datos personales*, Depalma, Buenos Aires, 1999.

Gils Carbó, Alejandra M., "La prohibición de transferencia internacional de datos personales (contra los paraísos informáticos)", *Derechos y nuevas tecnologías*, 2000-3-21, reproducido en LL 2000-A-939.

Palazzi, Pablo A., *La transmisión internacional de datos personales y la protección de la privacidad*, Ad-Hoc, Buenos Aires, 2002.

— "Breve comentario al decreto reglamentario de la ley 25.326", *Derecho y nuevas tecnologías*, 2003-4/5-345.

Palazzi, Pablo A. - Chacon de Albuquerque, Roberto, "Necesidad de armonizar el derecho a la protección de datos personales en el MERCOSUR", *Derecho y nuevas tecnologías*, 2003-4/5-545.

[79] Ver Carrascosa González, Javier, "Protección de la intimidad...", cit., ps. 428-29, y la bibliografía citada en la nota 30.

[80] Para una discusión autorizada sobre la calificación de los atentados a la personalidad, ver Audit, Bernard, *Droit international privé*, 2ª edición, Economica, Paris, 1997, ps. 514-17.

[81] Para dos posiciones antagónicas, ver Goldschmidt, Werner, *Derecho internacional privado*, 8ª edición revisada, Depalma, Buenos Aires, 1992, ps. 425-26; y Boggiano, Antonio, *Derecho internacional privado*, cit., t. II, ps. 869-70. Ver también mi interpretación del art. 43 del Tratado de Montevideo de derecho civil internacional que desafía la posición tradicional, *supra*, nota 19.

PERUGGINI, Alicia, "Reseña sobre la protección internacional de los derechos del hombre", Asdrúbal Aguiar, *Signos Actualización Bibliográfica*, año 2, nro. 3, 1991/1, Universidad de El Salvador.

RIGAUX, François, "Libre circulación de datos y protección de la vida privada en el espacio europeo", JA del 5/1/2005.

Extranjera

AUDIT, Bernard, *Droit international privé*, 2ª édition, Economica, ps. 513-18.

BOUREL, Pierre, "Du rattachement de quelques délits spéciaux en droit international privé", *Recueil des cours*, t. 214, 1989-II, ps. 251 y ss.

BÜCHER, Andreas, *Personnes physiques et protection de la personnalité*, Helbing & Lichtenhahn, Bâle, 1985.

CARRASCOSA GONZÁLEZ, Javier, "Protección de la intimidad y tratamiento automatizado de datos de carácter personal en DIPr.", *REDI*, vol. XLIV, 1992, ps. 417-41.

CHENAUX, Jean-Luc, *Les droit de la personnalité face aux médias internationaux*, Droz, Genève, 1990.

CONETTI, Giorgio, "Aspetti internazionali di una progettata normativa italiana sul trattamento automatizzato di dati personali", *Riv. dir. int. pr. proc.*, vol. XIX, 1983, ps. 589-600.

ESLAVA RODRÍGUEZ, Manuela, *La protección civil del derecho a la vida privada en el tráfico privado internacional: derecho aplicable*, SPUEX. Cáceres, 1996.

ESTADELLA YUSTE, Olga, *La protección de la intimidad frente a la transmisión internacional de datos personales*, Tecnos, Madrid, 1995.

FAUGEROLAS, Laurent, *L'accès international à des banques de données*, GLN, Paris, 1989.

FLAHERTY, David H., *Privacy and Government Data Banks: An International Perspective*, Mansell, London, 1979.

FOCSANEANU, Lazar, "La protection des données à caractère personnel contre l'utilisation abusive de l'informatique", *Journ. dr. int. (Clunet)*, t. 109, 1982, ps. 55-98.

GAILLARD, Emmanuel, "Les conflits de lois relatifs au droit patrimonial à l'image aux Etats-Unis", *Rev. crit. dr. int. pr.*, 1984, ps. 1 y ss.

GARZÓN CLARIANA, Gregorio, "La protección de datos personales y la función normativa del Consejo de Europa", *Revista de Instituciones Europeas*, vol. 8, 1981, ps. 9-25.

GELLMAN, Robert M., "Can Privacy Be Regulated Effectively on a National Level? Thoughts on the Possible Need for International Privacy Rules", *Villanova Law Review*, vol. 41, 1996, ps. 129-72.

HANOTIAU, Bernard, "The Transborder Flow of Data: Applicable Law and Settlement of Disputes", en *International Contracts for the Sale of Information Services*, ICC Institute, Paris, 1997, Publication nr. 440/5, ps. 175-197.

MACHERET, A., "Règlement des flux transfrontières de données de caractère personnel", *Informatique et protection de la personnalité*, Freiburg i.Br., 1981, ps. 240 y ss.

MESTRE, Jacques, "Conflits de lois relatifs à la protection de la vie privée", *Etudes offertes à Pierre Kayser*, t. II, PUF d'Aix-Marseille, 1979, ps. 239 y ss.

REIDENBERG, Joel R., "Resolving Conflicting International Data Privacy Rules in Cyberspace", *Stanford Law Review*, vol. 52, 2000, ps. 1315-71.

RIGAUX, François, "La loi applicable à la protection des individus à l'égard du traitement automatisé des données à caractère personnel", *Rev. crit. dr. int. pr.*, 1980, ps. 443-78.

— "L'élaboration d'un *right of privacy* par la jurisprudence americaine", *Revue internationale de droit comparé*, vol. XXXIII, 1980, ps. 701-30.

— "Le Régime des données informatisées en droit international privé", *Clunet*, vol. 113, 1986-2, ps. 311-28.

— *La protection de la vie privé et des autres biens de la personnalité*, LGDJ, Paris, 1990.

— "La liberté de la vie privée", *Rev. int. dr. comp.*, 1991, núm. 3, ps. 539-63.

RITTER, Jeffrey B. - HAYES, Benjamin S. - JUDY, Henry L., "Emerging Trends in International Privacy Law", *Emory International Law Review*, vol. 15, 2001, ps. 87-156.

SALBU, Steven R., "The European Union Data Privacy Directive and International Relations", *Vanderbilt Journal of Transnational Law*, vol. 35, 2002, ps. 655-95.

SHAFFER, Gregory, "Globalization and Social Protection: The Impact of EU and International Rules in the Racketing up of U.S. Privacy Standards", *Yale Journal of International Law*, vol. 25, 2000, ps. 1-88.

SWIRE, Peter P., "Of Elephants, Mice and Privacy: International Choice of Law and the Internet", *International Lawyer*, vol. 32, 1998, ps. 991-1025.