Ius et Praxis
ISSN: 0717-2877
revista-praxis@utalca.cl
Universidad de Talca
Chile

Suárez Crothers, Christian
Transferencia de datos personales a países terceros y el caso de internet
Ius et Praxis, vol. 7, núm. 2, julio-agosto, 2001, pp. 317-326
Universidad de Talca
Talca, Chile

Ius et Praxis Año 7 No 2: 317 - 326, 2001

ARTÍCULOS DE DOCTRINA

Transferencia de Datos Personales a Países Terceros y el Caso de Internet (**)

Christian Suárez Crothers (*)

(*) Profesor de Derecho Constitucional, Facultad de Ciencias Jurídicas y Sociales de la Universidad de Talca.

Cada vez resulta más indiscutible que la eficacia en el sistema de protección de datos va requiriendo grandes acuerdos de carácter internacional que avancen hacia la regulación de niveles equivalentes o adecuados de protección de los datos entre los Estados. Sin duda se echa de menos la existencia de un convenio internacional, más allá de las fronteras de la Unión Europea, que sirva para articular una mejor armonización entre las legislaciones.

Sin embargo, no debe creerse que la actividad de los organismos internacionales y, especialmente de las Naciones Unidas y de la OCDE haya estado ajena a estas preocupaciones. Desde la Conferencia Internacional de Derechos Humanos de Teherán (1968), la discusión sobre la incidencia de la electrónica en los derechos fundamentales comenzó a hacerse presente. Es así como la Resolución de la Asamblea General de Naciones Unidas N° 2450, de 19 de diciembre de 1968, exige al Secretario General de la ONU que encargue a sus organismos especializados un estudio sobre la materia.

En 1971, la Comisión de Derechos Humanos de las Naciones Unidas, emitió el informe solicitado, aunque sin que en los años posteriores se pudiera avanzar demasiado1, dada la disparidad de intereses existente entre los Estados miembros. Al decir de ESTADELLA YUSTE, el problema se situaba, más o menos del modo siguiente:

"Para los países en desarrollo las tecnologías informáticas no eran un arma peligrosa, sino al contrario: la consideraban como la solución que los podía ayudar a salir del atraso en que se encontraban. Los regímenes totalitarios que existían en los años setenta no compartían la preocupación de las naciones occidentales sobre el peligro que suponían las nuevas tecnologías para tener controlados a los individuos. El bloque socialista consideraba que el argumento sostenido por los países democráticos sobre el tema era una cuestión derivada de la filosofía capitalista de libertades individuales y, por tanto, era un problema que no tenía un alcance universal."

En los años 80, es la Subcomisión para la Prevención de Discriminación y Protección de Minorías, la que siguiendo las orientaciones de la OCDE2, fija unas nuevas directrices para el tratamiento automatizado de datos personales, las que fueron aprobadas por la

Asamblea General mediante resolución adoptada sin votación en su 45. Sesión (Resolución 45/95). Sin embargo estas disposiciones, no vinculantes para los Estados, sólo habían de producir efectos jurídicos en cuanto simples aspiraciones de la comunidad internacional.

A fuer de lo anterior, ESTADELLA YUSTE cree que "las bases del soft law sobre la protección de datos o autodeterminación informativa ya están asentadas"3, pese a que habría que esperar la orientación que la práctica estatal e internacional vaya adoptando, para determinar el grado de obligatoriedad de estas normas.

Es innegable, entonces, que la regulación europea ha resultado ser la más avanzada en este aspecto y, particularmente la que emana del Convenio 108 de 1981 y de la Directiva de 1995.

Pese a que VELÁSQUEZ BAUTISTA4 afirma que "la expresión transferencia de datos debe considerarse aplicable a todos los flujos de datos a través de las fronteras, independientemente de cuál sea el soporte mediante el que se envían los datos o la forma de tratamiento, pues si no se concibiera de esta forma la antedicha expresión, quedarían sin sentido muchas leyes de protección de datos", lo cierto es que sólo con la Directiva 95/45, puede considerarse que dicho supuesto se cumple, desde el momento en que el artículo 25 de esta última "incluye la recogida de datos en la noción legal de tratamiento, ya que el tratamiento comprende asismismo el tratamiento no automatizado"5.

La regulación del tráfico transfronterizo, inserta dentro del esquema de la Unión Europea, ha estado muy matizada por el logro de los intereses económicos de la Unión. Esta tendencia ha quedado patente en la actividad del Parlamento Europeo, de la Comisión y del Consejo de Europa. Al decir de ESTADELLA, "la Comisión y el Consejo se han centrado esencialmente en la promoción de la industria europea de procesamiento de datos a fin de hacerla más competitiva frente a otros países como los Estados Unidos y Japón"6. Ello ha derivado en un conflicto entre el interés por proteger los derechos de las personas frente al tratamiento automatizado o no de sus datos personales y las opciones económicas de la política comunitaria. De ahí que se expliquen, según algunos, las vaguedades del Convenio 108 en relación a los flujos de datos transfrontera7.
El Convenio 108, que regula esta materia en su artículo 12, necesariamente debe ser puesto al trasluz de la Directiva 95/46 de 1995, por cuanto, pese a ser esta última un instrumento de precisión de la primera, tienen una diferente manera de enfocarla.

Como ha señalado Marie-Claire PONTHOREAU, "sans qu'il soit question d'un véritable combat entre <deux Europe>, d'un côté, l'Europe des marchands et, de l'autre, l'Europe des droits de l'homme, la directive 95/46 CE es, sin embargo, el resultado de un difícil compromiso entre exigencias contradictorias"8.

El Convenio, a diferencia de lo que pudiera creerse, no fija como principio el de la interdicción de la transferencia de datos a terceros Estados, sino que da por sentado, en el n 2 de su artículo 12, el principio de la libre circulación de los datos. Por ello, dice:

"2. Una parte no podrá, con el único fin de proteger la vida privada, prohibir o someter a una autorización especial los flujos transfronterizos de datos de carácter personal con destino al territorio de otra parte."

De manera que la prohibición de transferir sólo podía proceder en dos casos:

a) Cuando el Estado remitente tiene una reglamentación específica para ciertas categorías de datos, o bien,

b) Cuando los datos transmitidos al país receptor, parte del Convenio, lo sean para ser enviados a un Estado no contratante, burlándose así la legislación del Estado emisor.
La primera de las excepciones, contemplada en la letra a) del numeral 3, es la que, aceptando una contraexcepción, vuelve al principio general de la libre circulación, cuando el Estado receptor tiene una "protección equivalente" en lo que respecta a esas categorías de datos. Ciertamente, acreditada tal situación, no es procedente prohibir la transferencia de los datos, ni someterla tampoco a un régimen de autorización previa. El problema, sin embargo, se radica en resolver qué es lo que deba entenderse por "protección equivalente".

La Directiva comunitaria, en cambio, no se basa en el concepto de protección equivalente, sino en el de "nivel de protección adecuado". Un concepto, a juicio de HEREDERO HIGUERAS, más débil que el del Convenio, pero que indudablemente se relaciona con el interés de facilitar las relaciones de intercambio. Se ha estimado que este criterio de la protección adecuada es un criterio realista y flexible, toda vez que exigir a terceros Estados no miembros del Convenio 108, un nivel de protección equivalente, aparte de resultar un problema difícil de superar, conllevaba en el hecho a que las necesidades del intercambio económico indujera a los propios países suscriptores a violar las obligaciones internacionales que libremente habían contraído.

Se ha sostenido también que la Directiva es expresiva de un segundo compromiso, además del que mencionáramos más arriba entre los intereses de la política económica comunitaria y los derechos y libertades individuales. Este segundo compromiso es el que se verificaría entre dos sistemas antagónicos de protección de datos; a saber, el británico o anglosajón, que privilegia el control a posteriori y el continental, particularmente el francés, alemán y español, que opta por la técnica del control a priori, más adecuado a la protección de las libertades. La consecuencia más directa, probablemente se manifestará en que las obligaciones impuestas a los responsables serán más feblemente controladas9.

Veamos ahora de qué manera esta regulación afecta al sistema Internet.

Pero, ¿Qué es Internet?

Desde luego no constituye Internet una sola red digital de intercambio, ni tampoco la única10, aunque, ¿Qué duda cabe?, su sola existencia ha trastocado el mundo de las comunicaciones. Se trata de un sistema que funciona a través "de un conjunto de vinculaciones (fuente telefónica, redes y vinculaciones especializadas, fibra óptica o satélite), de nudos y de redes que constituyen una malla mundial por la cual transitan las comunicaciones entre puntos terminales"11, sobre la base de un lenguaje de

comunicación numérico (TCP/IP: Transmission Control Protocol over Internet Protocol).

No se trata, por tanto, de una red física real, sino de "una comunidad de ordenadores que se comunican entre ellos a través de las redes existentes, gracias a un lenguaje común".

Desde el punto de vista de su estructura física, funciona a partir de dos fuentes continentales (Ebone y Europanet, para Europa y MCInet, SPRINTlink, Ausnet-AOL y CERFnet para los EE.UU). La interconexión entre las diferentes redes internacionales se efectúa de dos maneras: a) A través de organismos encargados de implementar el intercambio entre grandes redes (GIX-Global Internet Exchange) o, b) Por acuerdos de intercambio directo entre operadores12.

Se trata, por tanto, de una estructura descentralizada de redes, respecto de la cual no es posible cuantificar exactamente el número actual de sus usuarios, no obstante que se estima que durante el año 2000 ha alcanzado un universo de usuarios superior a los doscientos millones de personas.

No es una exageración cuando la Misión francesa encargada de estudiar la red Internet en Francia, dirigida por Isabelle FALQUE-PIERROTIN, manifiesta que con Internet se está en presencia, más que de una nueva tecnología, de la construcción de un nuevo espacio social, de una nouvelle civilité. O, en palabras de ARIÑO, AGUILERA y CUÉTARA, en presencia "de algo totalmente nuevo con un desarrollo casi biológico." ¿El mundo de la libertad?13.

Lo impactante del sistema es que comienza a producir cambios en los comportamientos públicos y privados, además de plantear nuevos problemas a las estructuras de poder y especialmente a la democracia.
Desde el punto de vista del derecho a la comunicación, Internet rompe con la clásica distinción entre correspondencia privada y comunicación audiovisual14, dado que no se inserta ni en el mundo de la difusión ni en el de la telemática y se constituye más bien como un mundo de utilizadores, la mayor parte de ellos perfectamente identificados, "que pasan por diferentes redes interconectadas, gracias a un protocolo de comunicación no propietario, para ir en la búsqueda de la información"15.

Quizá por esta razón el jurista alemán Ivo GEIS, que ha considerado a Internet como sinónimo de "internacionalidad del intercambio de información digital", estima que ni las leyes de protección de datos, en referencia a la alemana, ni las normas comunitarias son suficientes para dar cuenta con este verdadero "fenómeno" del siglo XX16. La solución sería, por tanto, aplicar a Internet, conceptos de Derecho internacional17.

Hasta la masificación de esta red, que se produce especialmente a partir del año 1993 cuando NETSCAPE adquirió el software conocido como Word Wide Wed (www.), que fuera inventado en 1989 en Suiza y luego integrado al software mosaico en una Universidad norteamericana, la información digital era patrimonio de una capa privilegiada (principalmente empresas con una red propia) situación que Internet modifica sustancialmente, exigiendo, por tanto, nuevas orientaciones jurídicas, vale decir, un nuevo trazado de los límites de la libertad individual.

¿Es suficiente la legislación nacional o la regulación europea para hacer efectivo el derecho a la autodeterminación informativa frente a Internet.?

Países como Alemania, que en sus leyes de protección de datos no cuentan con una norma precisa que regule el tráfico transfronterizo de los datos, debieron -según nos indica GEIS- utilizar distintas vías para someter al Derecho las comunicaciones por redes digitales como Internet.

Las normas comunitarias (Convenio y Directiva) no dan una solución clara al problema, dado que no es fácil determinar en el plano intereuropeo qué constituye un nivel de protección equivalente, ni tampoco acreditar respecto a terceros países la existencia de un nivel adecuado de protección, cuando ésta puede simplemente dirigirse a la protección de ámbitos específicos, como sucede, por ejemplo, en Chile.

Una primera vía de solución a este problema ha sido, en estos casos, la solución contractual, socializada a través de la llamada cláusula SCHUFA en Alemania o por la llamada doctrina italiana, que fuera establecida por la CNIL francesa. La cláusula SCHUFA funciona cuando no siendo acreditable que las legislaciones protejan de modo equivalente los datos, se celebra una estipulación en favor del afectado entre el transmisor interno y el receptor extranjero, que se obligan a proteger al afectado según el estándar de la legislación alemana.

En Francia, idéntica doctrina se impuso a partir de la deliberación de 11 de julio de 1989 de la Comisión Nacional de Informática y Libertades, respecto a los datos que la FIAT-France deseaba transmitir a la Casa matriz de la FIAT, en Turín. La deliberación condiciona a la filial a someter la transmisión al régimen de autorización previa, en los términos del Convenio 108, si no se celebraba un contrato, asegurando a los afectados la aplicación de las normas del Convenio y de la Ley francesa. La CNIL ha utilizado idéntico criterio cuando se ha tratado de la transferencia de datos en el sector del empleo y, particularmente, en materias de gestión de personal de sociedades multinacionales, elaborando cláusulas tipos para los flujos transfrontera de los datos. No siempre, sin embargo, se ha exigido un contrato. El ejemplo clásico de ello ha sido en Francia el llamado tratamiento MARINFO, relativo a la gestión de informaciones sobre el tráfico de estupefacientes por la vía marítima a través de intercambio de informaciones entre los Estados europeos, en los que sólo se han exigido simples intercambios de cartas18.

Pero, ciertamente, una estructura de comunicación digital como Internet, sobre la cual la comunicación circula en el instante y que puede ser recolectada desde cualquier país del planeta, parece poco compatible con los mecanismos de autorización previa, de firma del contrato o de un examen del nivel adecuado de la protección ofrecida. Ello parece posible sólo cuando se trata de un contrato de transferencia permanente o duradera de datos, como el que se produce en el ejemplo de la FIAT19.

De ahí que la solución contractual no ofrece ningún reemplazo equivalente a la protección de datos jurídicamente normada. ¿Cuáles son sus principales déficit?: a) Falta la seguridad de la aplicación de un control de protección de datos en el país receptor, b) Los poderes públicos del país receptor pueden acceder a estos datos haciendo tabula rasa de las normas establecidas por Convención y, c) El receptor extranjero no está limitado en la utilización de los datos, sobre los cuales tiene un amplio derecho de disposición.

Algunas vías alternativas de perfeccionamiento se han intentado. Una de ellas, señalada en los comentarios efectuados por la propia CNIL a la deliberación sobre la FIAT-France, es el esfuerzo de los encargados de la protección de datos de la Unión Europea y de la propia Comisión por la adopción de medidas de información y la puesta en práctica de medios técnicos destinados a seleccionar los sitios que se comprometen a ofrecer a los internautas una adecuada protección. Sin embargo, en el hecho ocurre que grandes servidores de Internet ponen a disposición del público datos obtenidos en Europa desde países que no cuentan con niveles de protección adecuados. Estas medidas son, claro está, insuficientes.

Otra forma de construir una alternativa a la vía contractual es que al perfeccionamiento del contrato se incorpore una suerte de chek-liste, que implique que los estándares mínimos de protección de las leyes nacionales que no regulan el tema, sean incorporados a los elementos esenciales del contrato. Del mismo modo, se puede acordar en favor del afectado el ejercicio de los derechos de defensa.

Ahora bien, cuando se trata de la transmisión de datos entre países de la Unión europea, al no existir en la realidad un nivel equivalente, la manera de evitar las diferencias en la protección de los datos puede ser solucionada a través de dos vías: 1.- Mediante la aplicación del llamado standortprinzip o principio del domicilio, conforme al cual la transmisión sigue las condiciones del Estado miembro en el que se domicilia el emisor, mientras que la elaboración y utilización de los datos se regla por las normas del domicilio del receptor y, 2.-Mediante la armonización de las legislaciones.

Respecto de los países terceros (no miembros de la Unión), al no existir un estándar mínimo que haga aplicable el standortprinzip, el régimen jurídico habrá de ser inevitablemente diferenciado, según cual sea su nivel de protección de los datos.

Si el tercer país tiene un adecuado nivel de protección, fórmula diplomática, al decir de GEIS20, destinada a evitar que Europa se convierta en una especie de fortaleza de la protección desde el cual ningún dato pudiera ser exportado, la transmisión será posible.

Para determinar si existe o no ese nivel, la Directiva comunitaria del 95, establece en su artículo 31 un procedimiento de comprobación, aunque la misma recurre a vagas expresiones para señalar cómo ha de practicarse la evaluación. En efecto, el artículo 25, apartado 2. de la Directiva, prescribe que: "2. El carácter adecuado del nivel de protección que ofrece un país tercero 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 del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, las normas de Derecho, generales o sectoriales, vigentes en el tercer país de que se trate, así como las normas profesionales y las medidas de seguridad en vigor en dichos países".

Si la Comisión comprueba que el tercer país no tiene un nivel adecuado de protección, debe tomar las medidas para impedir toda transferencia de datos a dicho país, solución que, como hemos dicho, sólo puede ser parcialmente aplicada a Internet.

En el fondo, se está en presencia de un procedimiento de determinación realizado por dos órganos políticos: los Estados miembros y la Comisión, de manera que la consideración de si concurre o no un nivel adecuado, se producirá después de finalizadas las negociaciones de la Comisión con el tercer Estado.

Pese a que la transmisión de datos a un país con protección inadecuada se encuentra prohibida por la Directiva, el artículo 26 permite la transferencia: a) si media el consentimiento inequívoco del interesado; b) si es necesaria para la ejecución de un contrato entre el interesado y el responsable o para la ejecución de medidas precontractuales tomadas a petición del interesado; c) si es necesaria para la celebración o ejecución de un contrato celebrado o por celebrar, en interés del interesado entre el responsable y un tercero; d) si es necesaria para salvaguardar un interés público importante, o para ejercer o defender un derecho en un procedimiento judicial; e) para la salvaguardia de un interés vital del interesado; f) si se trata de transferir desde registros públicos abiertos a consultas.

El problema aquí es la existencia de conceptos jurídicos indeterminados como "interés público importante", que pudo perfectamente catalogarse bajo la forma de específicos contenidos.

Finalmente, la Directiva somete al régimen de autorización previa la transferencia a países que no cuentan con un nivel adecuado de protección, cuando el responsable del tratamiento ofrece garantías suficientes respecto a la protección de los derechos del afectado, así como respecto a su ejercicio, todo lo cual puede derivar en las correspondientes cláusulas contractuales.

Sin embargo, como nos recuerda HEREDERO HIGUERAS, la doctrina ve con recelo estos contratos, toda vez que se celebran entre los responsables de los tratamientos, sin audiencia de los afectados21.

En Chile la Ley sobre Protección a la Vida Privada no ha introducido una norma reguladora del ejercicio de las libertades de información y a la vida privada en el contexto de Internet, no obstante que la importancia, incluso económica de estos temas, debería motivar al legislador a realizar una revisión profunda de nuestra incipiente protección de los datos de carácter personal.

(**) Este trabajo es resultado del Proyecto Fondecyt N° 1010453/2001 sobre "El derecho a la libertad de opinión e información frente al derecho del honor y la vida privada en Chile: Estudio jurídico del Derecho positivo chileno e internacional."

1 Estadella Yuste, Olga, La Protección de la Intimidad Frente a la Transmisión Internacional de Datos Personales, Editorial Tecnos, Madrid, 1995, pp. 59 y ss.

2 Recomendación del Consejo de Ministros de la OCDE de 23 de septiembre de 1980.

3 Estadella Yuste, Olga, Op. cit, p. 61.

4 Velásquez Bautista, Rafael, Protección Jurídica de Datos Personales Automatizados, Editorial Colex, Madrid, 1993, p. 171.

5 Heredero Higueras, Manuel, La Directiva Comunitaria de Protección de Datos de carácter personal, Editorial Aranzadi, Pamplona, 1997, p. 186.

6 Estadella Yuste, Olga, La Protección de la Intimidad Frente..., Op. cit., p. 69.

7 Ponthoreau, ha hecho notar en "La directive 95/46 du. 24 octobre 1995 relative à la protection des personnes physiques à l' égard du traitement des donées à caractèr personnel et à la libre circulation de ces données", Revue Francaise de Administration N° 13, Janv-févr., 1997, p. 125, que: "La directive élabore à cette fin un corps de principes communs de nature à concilier l'impératif économique et la protection des droits fondamentaux".

8 Ibidem, p. 125.

9 Ponthoreau, Marie-Claire. "La directive n. 95/46 CE du...", Op. cit., p. 127.

10 Canales distintos de transmisión son, por ejemplo, la propia Red por línea telefónica conmutada por un modem, RDSI (Red Digital de Servicios Integrados), Redes públicas, numérica de Integración de Servicios RNIS profesionales, EDI Multimedia, que permite intercambiar archivos CAD o fotagrafías de alta calidad, OSIT (Oficina de Servicios Integrados de Telecomunicaciones), entre otras. Todas ellas mencionadas en: Barriuso Ruiz, Carlos, Interacción del Derecho y la Informática, Editorial Dykinson, Madrid, 1996, p. 224.

11 MISSION INTERMINISTÉRIELLE SUR L'INTERNET PRÉSIDÉE PAR ISABELLE FALQUE-PIERROTIN. Internet. Enjeux juridiques. La documentation française, Paris, 1996, p. 19.

12 Cfr. Ibidem, p. 17.

13 Ariño, Gaspar; Aguilera, Lucía; De la Cuétara, J.M., Las telecomunicaciones por cable. Su regulación presente y futur, Marcial Pons, Ediciones Jurídicas y Sociales S.A., Madrid, 1996, pp. 50 y 51.

14 Se entiende que hay correspondencia privada cuando el mensaje es exclusivamente destinado a una (o muchas) personas físicas o morales, determinadas. En cambio, existe comunicación audiovisual cuando: a) el mensaje es destinado al público de manera indiferenciada o, b) cuando en su origen el mensaje transmitido se pone a disposición de todos los usuarios del servicio, sea a título gratuito u oneroso.

15 MISSION INTERMINISTÉRIELLE SUR L'INTERNET PRESIDÉE PAR ISABELLE FALQUE-PIERROTIN. Op. cit., p. 8.

16 Cfr. Comentario N° 5 de la deliberación de la CNIL francesa de 11 de julio de 1989.

17 Geis, Ivo, "Internet und Datenschutzrecht". NJW 1997, Heft 5, p. 288.

18 Cfr. COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS. Les libertés et l'informatique. Vingt délibérations commentéees. La documentation française, Paris, 1998, pp. 63 y ss.

19 Cfr. Geis, Ivo. Op. cit., p. 289.

20 Ibidem, p. 290.

21 Heredero Higueras, Manuel, Op. cit., p. 193.