6.
Derecho informativo

Revista de Derecho
de la Pontificia Universidad Católica de Valparaíso
XXXVI (Valparaíso, Chile, 2011, 1er Semestre)
[pp. 327 - 356]

El "nivel adecuado de protección" para las transferencias internacionales de datos personales desde la Unión Europea*

["The "Adequate Level of Protection" for International Personal Data Transfer from the European Union"]

Alberto Cerda Silva**
Universidad de Chile, Chile

Resumen

En 1995, la Unión Europea adoptó una directiva comunitaria para requerir "un nivel adecuado de protección" por terceros países, a efectos de autorizar la transferencia de datos personales hacia ellos. Este artículo analiza qué significa exactamente el criterio de adecuación y cómo ha sido aplicado en el "Acuerdo de Puerto Seguro" entre los Estados Unidos y la Unión Europea y la declaración por ésta de que Argentina constituía un "país seguro". Enseguida, el artículo explora las metas de la política de la Unión Europea y su cumplimiento con el Acuerdo General sobre el Comercio de Servicios.

Abstract

In 1995, the European Unión adopted a communitarian directive requiring "an adequate level of protection" by third countries, in order to authorize the transference of personal data to them. This article analyzes the meaning of the criterion of adequacy and how it has been applied in the "Safe Harbor Agreement" between the United States and the European Union, and in the declaration by the latter that Argentina was a "safe country". Immediately, this article explores the goals of the policy of the European Union and its compliance with the General Agreement on Trade in Servi-

* Este artículo fue preparado para el Seminario "Data Privacy in the United States and European Union", ofrecido por los profesores Reijo Aarnio, Mercedes Ortuño, Elena Gasol Ramos, y Hugh Stevenson, en Georgetown University Law Center, en 2009. El autor desea agradecer las amables recomendaciones recibidas del último de ellos, así como el respaldo brindado por la Fulbright Commission y Georgetown University para proseguir estudios de postgrado en dicha universidad.

** Profesor asistente de Derecho informático de la Facultad de Derecho de la Universidad de Chile. Correo postal: Facultad de Derecho, Universidad de Chile, Pío Nono con Bellavista, Providencia, Santiago, Chile. Correo electrónico: acerda@uchile.cl

La hipótesis subyacente es que, en orden a cumplir con la obligación establecida en ese Acuerdo, que impide la discriminación arbitraria o injustificable entre países, la Unión Europea ha socavado su propósito de obtener un "nivel adecuado de protección" cualquiera sea el lugar a que ésta exporte datos personales.

Palabras clave

Privacidad – Protección de datos – Datos personales – Nivel adecuado de protección – Transferencia internacional de datos.

ces. The underlying hypothesis is that, in order to comply with the obligation set forth by this Agreement, which prevents arbitrary or unjustifiable discrimination between countries, the European Union has eroded its purpose of achieving an "adequate level of protection" anywhere that it exports personal data.

Keywords

Privacy – Data protection – Personal data – Adequate level of protection – International transference of data.

[Recibido el 27 de octubre de 2010 y aprobado el 28 de marzo de 2011].

I. Antecedentes

Temerosos de los riesgos que el creciente uso de la tecnología podría implicar para los derechos fundamentales[1], desde comienzos de los años setenta, varios países adoptaron leyes sobre protección de los datos personales para reglamentar el tratamiento automatizado de la información personal[2]. A pesar de los esfuerzos de la autoridades nacionales en materia de protección de datos para obtener un satisfactorio nivel de protección, la ausencia de leyes en otros países y la precaria armonización legal entre otros impedían la obtención de tal logro. A comienzos de los ochenta, resultaba evidente que dichos países necesitaban una aproximación internacional para lograr cierta concordancia entre sus legislaciones locales y, muy en especial, regular las transferencias de información personal de un país a otro. A través de acuerdos

[1] De hecho, el debate internacional en torno a los límites que una sociedad democrática debe imponer para proteger los derechos humanos frente al creciente uso de las tecnologías comenzó en 1968, con la Conferencia Internacional sobre Derechos Humanos, organizada por las Naciones Unidas. Véase: *Proclamation of Teheran, Final Act of the International Conference on Human Rights*, Teheran, 22 April to 13 May 1968, U.N. Doc. A/CONF. 32/41 at 3 (1968).

[2] Hacia finales de los años setenta, entre los países que habían adoptado leyes en materia de protección de datos se contaban: Suecia, *Data Lag*, 1973; los Estados Unidos, la *Privacy Act*, 1974; la entonces República Federal de Alemania, *Bundesdatenschutzgesetz*, 1977; y Francia, France, Loi 78-17 du janvier, *Relative à l'informatique, aux fichiers et aux libertés*, 1978. Existían también leyes sobre la materia en Austria, Dinamarca, Luxemburgo, y Noruega. Sin embargo, la primera experiencia de adopción de una ley de protección de datos personales corresponde al land alemán de Hesse, en 1970.

internacionales los países podrían proteger el derecho a la privacidad de las personales y, a la vez, evitar innecesarias barreras para la libre circulación de información entre los países[3].

La Organización para la Cooperación y el Desarrollo Económicos (OCDE) aprobó el primer instrumento internacional que intentó reglamentar el procesamiento de datos personales y el flujo internacional de dichos datos, mediante la adopción, en 1980, de unas directrices relativas a la protección de la intimidad y de la circulación transfronteriza de datos personales[4], las cuales promueven la democracia, el respecto por los derechos humanos, y la economía de libre mercado. Las directrices establecen un estándar mínimo a efectos de promover la armonización internacional de las normas relativas al tratamiento manual y automatizado de información personal por los sectores públicos y privado. Respecto del flujo transfronterizo de datos personales, a efectos de proteger los derechos humanos, las directrices evitan la adopción de medidas que establezcan obstáculos innecesarios al libre flujo de información, pero, sin embargo, autoriza la restricción del flujo cuando un país no provee un nivel de protección "equivalente".

Subsecuentemente, la OCDE ha adoptado varias directrices en asuntos relacionados son la protección de los datos personales, tales como transparencia pública y acceso a la información[5], privacidad en redes globales[6],

---

[3] En los siguientes párrafos, para efectos de nuestro análisis, los instrumentos internacionales relevantes son las distintas recomendaciones adoptadas por la Organización para la Cooperación y el Desarrollo Económicos, el "Convenio de Estrasburgo" y las directivas de la Unión Europea. Sin embargo, un panorama completo de los instrumentos internacionales relativos a la transferencia transfronteriza de datos personales también requeriría incluir: los *Principios rectores para la reglamentación de los ficheros computarizados de datos personales*, adoptados por la Asamblea General de la Naciones Unidas en su resolución 45/95, de 14 de diciembre de 1990; el *Asia-Pacific Economic Cooperation Privacy Framework,* adoptado en la 16a Reunión Ministerial de APEC, celebrada en Santiago de Chile entre el 17 y 18 de noviembre de 2004; y el *Anteproyecto de Convención Americana sobre Autodeterminación Informativa*, de la Organización de Estados Americanos.

[4] Organization for Economic Co-operation and Development (OECD), *Recommendation of the Council concerning guidelines governing the protection of privacy and transborder flows of personal data*, adopted by the Council on 23 September 1980 - C(80)58/Final.

[5] Organization for Economic Co-operation and Development, *Declaration on Transborder Data Flows*, adopted by the Governments of OECD Member countries on 11 April 1985 - C(85)139.

[6] Organization for Economic Co-operation and Development, *Declaration on the Protection of Privacy on Global Networks,* adopted by the Governments of OECD Member countries on 8 October 1998 - C(98)177.

y comunicaciones electrónicas no solicitadas ("spam")[7]. Sin embargo, la eficacia de las directrices de la OCDE es limitada por su propia naturaleza: toda recomendación es un documento jurídicamente no vinculante y, por consiguiente, sin posibilidad de su cumplimiento forzado. Como resultado de ello, las directrices de la OCDE han sido incapaces de crear un entorno que garantice el libre flujo de información personal, incluso entre los propios países miembros de la organización[8].

En 1981, el Consejo de Europa adoptó el *Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal*, también conocido como "Convenio de Estrasburgo" o "Convenio 108"[9]. El convenio contiene disposiciones aplicables al tratamiento automatizado de datos personales relativos a personas físicas tanto por el sector público como por el privado[10]; sin embargo, un país parte podría también aplicar sus disposiciones a los datos concernientes a personas jurídicas y al tratamiento manual de los datos[11]. Respecto del flujo transfronterizo de datos personales, para evitar la elusión de las leyes nacionales sobre protección de datos, el convenio requiere una *"protección equivalente"* entre los países partes[12], y provee mecanismos de asistencia recíproca y cooperación internacional a través de las autoridades locales de cada país[13].

Sin embargo, la eficacia del "Convenio 108" decayó y fue también incapaz de resolver los problemas relativos al flujo transfronterizo de datos personales. Durante la primera mitad de los años 90, hubo un reducido

---

[7] Organization for Economic Co-operation and Development, *Recommendation of the Council on Cross-Border Co-operation in the Enforcement of Laws against Spam*, adopted by the Council on 13 April 2006 - C(2006)57.

[8] Entre los países miembros de la OCDE, hay unos con leyes de protección de la privacidad bastante fuertes (e.g., Canadá, Finlandia, Francia, Alemania, y España), otros menos fuertes (e.g., Corea y los Estados Unidos), y algunos bastante débiles (e.g., México). Véanse: *Outsourcing Privacy: Countries Processing U.S. Social Security Numbers, Health Information, Tax Records Lack Fundamental Privacy Safeguards*. Staff Report prepared at the request of Edward J. Markey (U.S. House of Representatives. September 20, 2005), pp. 6-7. La posición de México en el mencionado "ranking" ha debido cambiar, particularmente tras la reciente adopción de la *Ley federal de protección de datos personales en posesión de los particulares*, publicada en el *Diario Oficial de la Federación* el 5 de julio de 2010.

[9] Convenio Nº 108 del Consejo, de 28 de enero de 1981, de Europa, *para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal* (= "Convenio de Estrasburgo").

[10] Artículos 1, 2 a) y c), y 3 del "Convenio de Estrasburgo".

[11] Artículos 3.2 del "Convenio de Estrasburgo".

[12] Artículos 12 del "Convenio de Estrasburgo".

[13] Artículos 13 a 17 del "Convenio de Estrasburgo".

número de nuevos países signatarios del convenio[14]. Adicionalmente, los países partes no siempre implementaron el Convenio en su Derecho interno[15]. Por tales razones[16], la Unión Europea decidió tomar la iniciativa de adoptar una directiva, esto es, una regulación comunitaria vinculante para los países miembros. Dicho proceso cristalizó en la Dir. 95 N° 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (= Dir. 95)[17].

La Dir. 95 establece un régimen normativo exhaustivo que reglamenta el tratamiento de los datos personales concernientes a personas naturales que se verifique manual o automatizadamente tanto en el sector público como en el privado[18]. Adicionalmente, la Dir. 95 establece los principios que reglamentan el tratamiento de datos[19], los derechos del titular de datos[20], y

---

[14] Estos fueron: Finlandia, Hungría y Eslovenia. Vid, *Estado del Convenio*, disponible en <http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=108&CL=ENG> (última visita: 27 de enero de 2010).

[15] Este fue, por ejemplo, el caso de España, país que ratificó el Convenio en 1984, pero que sólo la implementó en 1992, a través de la Ley Orgánica N° 5/1992, de 29 de octubre, de *Regulación del tratamiento automatizado de los datos de carácter personal* (LORTAD).

[16] Heredero explica que la propuesta de Directiva inicialmente mostraba una mayor preocupación en la obtención de un "nivel de protección equivalente", a efectos de garantizar el libre flujo de información entre los miembros de la Unión Europea, lo cual era necesario para el adecuado funcionamiento del mercado interno, antes que a efectos de proteger la privacidad de las personas en relación con el tratamiento de sus datos. Heredero, Manuel, *La Directiva comunitaria de protección de datos de carácter personal* (Pamplona, Aranzadi, 1997), pp. 23 – 30. Por ejemplo, de acuerdo a Diana Alonso, la ausencia de equivalencia entre los países europeos en relación a sus leyes sobre protección de datos creaba problemas para la implementación de iniciativas que suponían la transferencia de datos de un país a otro, tal como el Social Security Network Programme (SOSENET) que intentaba coordinar los servicios de seguridad social de Europa. Véase: Alonso, Diana, *El futuro de la protección de datos a nivel europeo, en Encuentros sobre Informática y Derecho* (Madrid, Instituto de Informática Jurídica, Universidad Pontificia Comillas, 1995-1996), pp. 163 – 176.

[17] Directiva N° 95/46/CE del Parlamento Europeo y el 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* ("Directiva de protección de datos"). Para una revisión del proceso de armonización normativa llevado adelante por la Directiva entre los países miembros de la Unión Europea y los distintos mecanismo para asegurar su eficacia, véase: Cerda Silva, Alberto, *Mecanismos de control en la protección de datos en Europa,* en *Ius et Praxis,* 12 (Talca, Chile, 2006), pp. 221-251.

[18] Artículos 1.1, 2 y 3.1 de la "Directiva de protección de datos".

[19] Artículos 6 a 11 de la "Directiva de protección de datos".

[20] Artículos 12 a 15 de la "Directiva de protección de datos".

la responsabilidad de las entidades que procesan datos[21]. La Dir. 95 requiere la existencia de un recurso judicial[22] y de una autoridad publica independiente a cargo de supervigilar el cumplimiento de la ley de protección de datos personales[23]. Los países miembros de la Unión Europea dispusieron de un término de tres años para implementar la Dir. 95 en su respectivo Derecho interno[24]. A pesar de las flexibilidades previstas por la propia Dir. 95, gracias a su progresiva implementación en el Derecho interno, ella ha contribuido notablemente a la armonización entre los países miembros de la Unión Europea[25].

Respecto del flujo transfronterizo de datos personales, la Dir. 95 se refiere a dos distintos niveles: un "nivel de protección equivalente"[26], en el caso de transferencias entre los países miembros de la Unión Europea; y un "nivel adecuado de protección"[27], en el caso de flujos de datos hacia terceros países, esto es, aquellos que no son miembros de la Unión Europea.

¿Qué significa "nivel adecuado de protección"? ¿Hay alguna diferencia entre tal nivel y otro equivalente? En caso de existir tal criterio de adecuación, ¿cómo ha sido este aplicado? A efectos de responder a estas interrogantes en las siguientes páginas revisaremos el criterio adoptado por la Unión Europea para calificar a un país como uno que provee un "nivel adecuado de protección", su diferencia con la protección equivalente, y la aplicación de tal criterio de adecuación, particularmente en relación con dos casos: el "Acuerdo de Puerto Seguro" suscrito entre los Estados Unidos y la Unión

---

[21] Artículo 23 de la "Directiva de protección de datos".

[22] Artículo 22 de la "Directiva de protección de datos".

[23] Artículo 28 de la "Directiva de protección de datos".

[24] Artículo 32 de la "Directiva de protección de datos". A pesar de los requisitos de implementación previstos en el texto de la "Directiva de protección de datos", la Corte Europea de Justicia resolvió que a lo menos ciertas disposiciones de ella son auto-ejecutables ("self-executing") y, por consiguiente, una persona puede esgrimirlas a efectos de evitar la aplicación de una norma de Derecho interno inconsistente. Corte Europea de Justicia, Casos C-465/00, C-138/01, y C-139/01 "Rechnungshof v. Österreichischer Rundfunk y otros", y "Christa Neukomm y Joseph Lauermann v. Österreichischer Rundfunk", 30 de mayo de 2003.

[25] Sólo cuatro países implementaron la Directiva a tiempo. Véase: Commission of the European Communities, *First report on the implementation of the Data Protection Directive* (*95/46/EC*) (Brussels, 15.5.2003 COM, 2003), p. 265 final. De hecho, Francia fue el último que implementó la Directiva modificando su legislación interna mediante ley del 6 de agosto de 2004, relativa a la protección de las personas con respecto al procesamiento de datos personales.

[26] Considerandos 8 y 9 de la "Directiva de protección de datos".

[27] Considerandos 56, 57, 59 y 60; y, artículo 25 de la "Directiva de protección de datos".

Europea, y la decisión de esta última de calificar a Argentina como un "país seguro."

II. Alcance de la exigencia de un "nivel adecuado de protección"

Desde la preparación de los borradores que precedieron a la adopción de la Dir. 95, ha existido cierto desconcierto entre los expertos respecto del uso de la frase "nivel adecuado de protección". Sin embargo, las preocupaciones eran distintas de un lado y otro del Atlántico. En los Estados Unidos, los autores alegaban en contra de la importación europea de su regulación a otros países, sus efectos nocivos para el funcionamiento del libre mercado, y la imposibilidad del sistema estadounidense de satisfacer dicho nivel de protección. En la Unión Europea, los autores estaban preocupados del sentido de la expresión "adecuado", particularmente teniendo en consideración que el "Convenio 108" ya establecía un estándar –"nivel de protección equivalente"– a efectos de permitir el flujo transfronterizo de datos personales[28].

La Dir. 95 eliminó los obstáculos para el flujo de datos desde un país a otro en el mercado interno, asumiendo que el nivel de protección entre los miembros de la Unión Europea es equivalente[29]. A pesar de las diferencias ocasionadas por el "margen de maniobra" que la Dir. 95 autoriza a los países, éstos no pueden bloquear el libre flujo de información, porque se presume un "nivel de protección equivalente" dentro de las fronteras de la Unión Europea. Bajo tal circunstancia, la Dir. 95 está en armonía y es consistente con el "Convenio 108", el cual prohíbe a una parte bloquear la transferencia de datos personales hacia una parte receptora, si ésta provee un "nivel de protección equivalente"[30].

Sin embargo, la Dir. 95 no ha podido exigir un equivalente (i. e., exactamente el mismo) nivel de protección de terceros países, que no son miembros de la Unión Europea. En cambio, ésta les exige un nivel de protección menos

---

[28] Estadella-Yuste, Olga, *La protección de la intimidad frente a la transmisión internacional de datos personales* (Madrid, Tecnos, 1995), pp. 117 ss.

[29] De acuerdo con Heredero, la Directiva asume que una vez que la implementación es efectuada, la disparidad solamente puede tener lugar con terceros países. De hecho, las disposiciones de la Directiva no incluyen ningún mecanismo para establecer dicha equivalencia, porque ello no es un problema o ello será resuelto a través de la aplicación del artículo 30 de la "Directiva de protección de datos". Heredero, Manuel, cit. (n. 16), p. 186.

[30] Artículo 12,3 b del "Convenio de Estrasburgo", y considerando 11 de la "Directiva de protección de datos". Véase el *Explanatory Report of Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, párrafo 69.

fuerte: un nivel "adecuado"[31]. Esto parece más realista como exigencia a terceros países, especialmente considerando que, de otro modo, la Dir. 95 demandaría la adopción global del estándar de la Unión Europea[32]. La Dir. 95 ha prohibido la transferencias de datos personales a terceros países, es decir, países no miembros de la Unión Europea, que no garantizan un "nivel adecuado de protección"[33]; naturalmente, tal regla general cuenta con algunas excepciones, el análisis de las cuales excede los propósitos de este artículo[34].

En síntesis, la Dir. 95 presume un "nivel de protección equivalente" entre los países miembros de la Unión Europea, los cuales no pueden obstaculizar el flujo de datos personales dentro del mercado interno. En cambio, la Dir. 95 requiere un "nivel adecuado de protección" a terceros países; en caso de que un país carezca de tal nivel, las transferencias están prohibidas. Esto ha creado un problema en el caso de aquellos terceros países que sin ser partes de la Unión Europea son partes del "Convenio 108", el cual admite su adhesión por países que no son miembros del Consejo de Europa[35], y prevé un "nivel de protección equivalente"[36]. ¿Deben estos países satisfacer ambos estándares a efectos de obtener transferencias de datos personales desde la Unión Europea? ¿Constituye la exigencia de adecuación de la Dir. 95 una exigencia adicional que infringe las disposiciones del Convenio?

Para responder las interrogantes precedentes, la Dir. 95 provee una cláusula de homologación con compromisos internacionales[37]. Adicionalmente, el Grupo del artículo 29 sobre Protección de Datos, instancia que reúne a las autoridades sobre protección de datos de todos los países miembros de la Unión Europea, ha provisto una interpretación que armoniza las disposiciones de ambos instrumentos, el "Convenio 108" y la Dir. 95[38], y ha

---

[31] Heredero, Manuel, cit. (n. 16), p. 186.

[32] Ibíd., p. 188. Para una usual perspetiva estadounidense al respecto, véase: Goldsmith, Jack - Wu, Tim *Who Controls the Internet: Illusions of a Borderless World* (Nueva York, Oxford University Press, 2008), pp. 173-177.

[33] Artículo 25,1 de la "Directiva de protección de datos".

[34] Artículo 26 de la "Directiva de protección de datos".

[35] Artículo 23 del "Convenio de Estrasburgo".

[36] Este asunto también puede ser suscitado con respecto a las recomendaciones de la OCDE, las cuales adoptan un "nivel de protección equivalente" como estándar. Sin embargo, dichas recomendaciones no son jurídicamente vinculantes, salvo si ellas llegasen a constituir costumbre internacional, lo cual parece bastante improbable dada la ausencia del requisito de *opinio juris* en las mismas.

[37] Artículo 25,6 de la "Directiva de protección de datos". Véase Heredero, Manuel, cit. (n. 16), p. 188.

[38] Working Party on the Protection of Individuals with regard to the Processing of Personal Data, *Working Document: Transfers of Personal Data to Third Countries: Applying*, Articles 25 and 26 of the EU data protection directive, 24 July 1998. DG XV D/5025/98 WP 12, pp. 8 – 9.

empleado el hecho de ser un país parte del Convenio como un elemento en su hallazgo de adecuación en el nivel de protección provisto por un tercer país[39]. Finalmente, a efectos de obtener una completa consistencia entre ambos instrumentos internacionales, en 2001, un Protocolo Adicional al Convenio fue adoptado[40], el cual ha introducido modificaciones a las disposiciones que reglamentan el flujo transfronterizo de datos personales[41], y ha incrementado los requisitos de protección entre las partes del Convenio, al requerir la existencia de una autoridad de supervisión, la que debe ejercer sus funciones en completa independencia, como un elemento de la protección efectiva[42].

Volviendo a nuestro análisis del "nivel adecuado de protección", él ha sido criticado por su ambigüedad. Él no contribuye a superar la incertidumbre en torno a similares criterios, tales como "protección equivalente" en el "Convenio 108", y las "garantías comparables" de los Principios formulados por las Naciones Unidas[43]. Olga Estadella-Yuste, profesora de Derecho en la Universidad Autónoma de Barcelona, expresa su desazón con la inexactitud de los documentos internacionales, los que en vez de determinar un nivel de protección han creado vaguedad, socavando los propósitos mismos de su adopción[44].

Efectivamente, la Dir. 95 no provee una definición de adecuación, sin embargo, ello no erosiona el propósito mismo de su adopción. De hecho, la frase "nivel adecuado de protección"brinda suficiente flexibilidad a efectos de su aplicación a las diferentes realidades en que dicho estándar es aplicado. La Dir. 95 provee un concepto jurídico indeterminado, una norma en blanco, pero susceptible de adquirir un colorido contenido a través del uso de aquellos criterios previstos por la propia Dir. 95[45]. Pero, ¿cuáles son dichos criterios y cómo han sido aplicados por las autoridades de la Unión Europea?

De acuerdo a lo mencionado, a efectos de autorizar la transferencia de datos personales hacia terceros países, la Unión Europea no aplica el estándar de equivalencia que presume entre sus miembros. Como ya se ha dicho, dicha equivalencia no existe, ella es con propiedad una ficción jurídica más que una

---

[39] Estos fueron los casos de Hungría, Suiza, Guernsey y la Isla de Man.

[40] *Protocolo Adicional al Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, a las autoridades de control y a los flujos transfronterizos de datos*, hecho en Estrasburgo el 8 de noviembre de 2001.

[41] Artículo 1 del *Protocolo Adicional*.

[42] Artículo 2 del *Protocolo Adicional*.

[43] Párrafo 9 de los *Principios rectores para la reglamentación de los ficheros computarizados de datos personales*, adoptados por la Asamblea General de la Naciones Unidas en su resolución 45/95, de 14 de diciembre de 1990.

[44] Estadella-Yuste, Olga, cit. (n. 28), p. 110.

[45] Heredero, Manuel, cit. (n. 16), p. 188.

presunción[46]. La Unión Europea emplea el estándar de "nivel adecuado de protección" en relación con terceros países. Sin embargo, a efectos de calificar a éstos, la Unión Europea tampoco usa el estándar de equivalencia como punto de referencia, en vez de ello la Dir. 95 provee otros criterios que permiten determinar si un país ofrece un nivel de protección adecuado o no.

En efecto, la Dir. 95 dice que la adecuación *"se evaluará atendiendo a todas las circunstancias que concurran en una transferencia o en una categoría de transferencias de datos"*, e indica algunos de los varios criterios eventualmente aplicables[47]. Al adoptar tan amplio criterio, la Dir. 95 requiere un análisis caso a caso para efectos de determinar si un país provee el nivel de protección requerido. Sin embargo, la multiplicidad y frecuencia de las transferencias de datos han forzado al Grupo del artículo 29 sobre Protección de Datos a racionalizar el proceso, mediante la adopción de una interpretación de autoridad acerca de qué constituye un "nivel adecuado de protección"[48].

De acuerdo al Grupo del artículo 29 sobre Protección de Datos, hay dos elementos esenciales en cualquier análisis relativo al "nivel adecuado de

---

[46] La propia Directiva reconoce que la mencionada equivalencia no existe; por ejemplo, al determinar la adecuación de un tercer país, el artículo 25,2 de la Directiva considera "el país de origen", esto es, la Unión Europea, asume que hay diferencias entre sus propios miembros y que dichas diferencias pueden ser relevantes a efectos de calificar a un tercer país como uno que provee un "nivel adecuado de protección". En parte, dichas diferencias provienen del margen de maniobra que la propia Directiva otorga a los miembros para su implementación; de hecho, cada disposición de la Directiva tiene un reflejo en el Derecho interno de cada país miembro de la Unión Europea. Adicionalmente, la Unión Europea ha adoptado otras Directivas que incluyen disposiciones relativas al tratamiento de datos personales, las cuales, de acuerdo a Ahti Saarenpää, profesor de Derecho y decano de la Escuela de Derecho de la Universidad de Laponia, puede conducir a una fragmentación normativa [véase: Saarenpää, Ahti, *Europa y la protección de los datos personales,* en *Revista Chilena de Derecho Informático*, 3 (2003), pp. 15-29]. En nuestro concepto, tal proliferación hace totalmente ilusorio la idea misma de "un" "nivel de protección equivalente": hay tantos niveles equivalentes de protección dentro de la Unión Europea como países miembros y áreas de aplicación. Como resultado de ello, la Directiva apropiadamente elude establecer un "nivel adecuado de protección" mediante su comparación con esa ficción legal llamada "nivel de protección equivalente".

[47] Artículo 25.2 de la "Directiva de protección de datos".

[48] Los documentos más relevantes para estos efectos son: Working Party on the Protection of Individuals with regard to the Processing of Personal Data, *First Orientations on Transfers of Personal Data to Third Countries - Possible Ways Forward in Assessing Adequacy*. *Discussion Document adopted by the Working Party on 26 June 1997*. XV D/5020/97-EN final WP4; y Working Party on the Protection of Individuals with regard to the Processing of Personal Data, *Working Document: Transfers of Personal Data to Third Countries: Applying Articles 25 and 26 of the EU Data Protection Directive*, 24 July 1998. DG XV D/5025/98 WP 12.

protección": el contenido de las reglas aplicables y los medios para asegurar su efectiva aplicación. En otros términos, la evaluación requiere constatar la apropiada adopción y cumplimiento de las disposiciones sobre protección de datos personales.

En relación al contenido, el Grupo del artículo 29 sobre Protección de Datos entiende que el "nivel adecuado de protección" requiere la existencia de disposiciones que garanticen los derechos de los titulares de datos personales, imponen obligaciones a los responsables de tratamiento, establecen principios aplicables al procesamiento de datos, y responsabilidad, en caso de infracción. Dichos requisitos están presentes en la mayor parte de los instrumentos internacionales relativos a la protección de los datos personales, lo que evidencia un significativo nivel de consenso en torno a ellos. Además, al evaluar, el Grupo del artículo 29 sobre Protección de Datos ha adoptado una aproximación flexible que mira al sistema legal en su conjunto y no sólo a la ley de protección de datos vigente.

Respecto a asegurar una efectiva aplicación de las normas, el Grupo del artículo 29 sobre Protección de Datos intenta identificar el nivel de cumplimiento y la disponibilidad de mecanismos para tal efecto, tales como recursos judiciales y sistema de sanciones. El elemento distintivo de la Dir. 95 en este punto es la existencia de una autoridad independiente que supervisa el cumplimento de la ley; de hecho, este elemento ha sido consagrado como una parte esencial del derecho a la protección de los datos personales previsto en la Carta de los Derechos Fundamentales de la Unión Europea[49]. Sin embargo, el Grupo del artículo 29 sobre Protección de Datos no se concentra en un determinado mecanismo sino que mira hacia los propósitos subyacentes del sistema: la obtención de un buen nivel de cumplimiento de las normas, el apoyo y ayuda hacia los titulares de datos personales para el ejercicio de sus derechos, y la provisión de apropiadas compensaciones para las partes afectadas con la infracción de las reglas[50].

En suma, como es posible apreciar, el Grupo del artículo 29 sobre Protección de Datos ha adoptado criterios flexibles a efectos de establecer si un determinado país provee un "nivel adecuado de protección" y, consecuentemente, puede disfrutar de transferencias de datos personales desde los países miembros de la Unión Europea. Sobre la base de un análisis caso a caso, estos criterios intentan identificar si un país garantiza adecuada protección, a través

---

[49] El artículo 8.3 de la Carta expresa que *"El respeto de estas normas* (sobre protección de datos de carácter personal) *quedará sujeto al control de una autoridad independiente"*. Carta de los Derechos Fundamentales de la Unión Europea, firmada y proclamada por los Presidentes del Parlamento Europeo, el Consejo, y la Comisión en la reunión del Consejo de Europa en Niza, el 7 de diciembre de 2000.

[50] Supra (n. 48).

de la adopción y el cumplimiento de las normas relativas a la protección de los datos personales.

III. Aplicación del "nivel adecuado de protección"

Desde su adopción, en 1995, la Unión Europea ha promovido la implementación de la Dir. 95 y la progresiva armonización de la normativa de Derechos interno de los países que integran el mercado interior. Además, la Unión Europea exige la adopción de la Dir. 95 por los países candidatos, e insta por su adopción entre los países asociados y terceros países. Como resultado de dichos esfuerzos, en varios países se han adoptado legislación interna o redactado propuestas de ley que reflejan los requerimientos de la Unión Europea, a efectos de permitir el libre flujo transfronterizo de datos personales. Sin embargo, en aproximadamente quince años en vigor la Comisión ha reconocido que sólo un extremadamente reducido número de países aseguran un "nivel adecuado de protección"[51].

De aquel puñado de países que proveen un "nivel adecuado de protección", la mayor parte están insertos geográficamente en el entorno europeo y han adaptado sus marcos normativos de modo de garantizar su reconocimiento por las autoridades de la Unión Europea. En cambio, solamente un par de casos corresponden a países fueras de dicho entorno. De entre estos últimos, los casos más interesantes son el "Acuerdo de Puerto Seguro", que permite las transferencias de datos desde la Unión Europea a los Estados Unidos, y la calificación de Argentina como un país que provee un "nivel adecuado de protección". Ambos constituyen excelentes casos de estudio, no sólo por sus significativas diferencias con la Unión Europea, sino también por las inherentes complejidades de sus sistemas políticos y legales federales. En las páginas siguientes revisaremos ambos casos brevemente, a efectos de comprender la aplicación que la Unión Europea ha hecho del criterio de "nivel adecuado de protección".

1. El "Acuerdo de Puerto Seguro".

Para comprender los desafíos del flujo de datos personales desde la Unión Europea a los Estados Unidos es previamente necesario identificar las peculiaridades del sistema jurídico estadounidense que hacen una completa diferencia entre ambos bloques. A riesgo de simplificar en exceso, es posible aseverar que existen tres distinciones esenciales entre ambos sistemas: el ám-

[51] Estos países son: los Estados Unidos, en relación al denominado "Acuerdo de Puerto Seguro" y al tratamiento y la transferencia de datos del registro de nombres de los pasajeros; Hungría y Suiza (1999); Argentina, Guernsey, y la Isla de Man (2003); Jersey (2008); y, más recientemente, el Principado de Andorra e Israel (2009).

bito del derecho a la privacidad, la opción entre un sistema de protección de los datos personales exhaustivo y general o uno fragmentario, y la importancia de los mecanismos de autorregulación y autocontrol.

A pesar de la ausencia de un expreso reconocimiento constitucional, el derecho a la privacidad ha sido reconocido como un derecho humano en los Estados Unidos[52]. Sin embargo, a diferencia de la Unión Europea, este Derecho tiene dos limitaciones significativas: la primera es la libertad de expresión, ya que en prácticamente todos los casos en que los intereses en competencia son el derecho a la privacidad y la libertad de expresión, el derecho garantizado en la primera enmienda ha prevalecido y, consiguientemente, el derecho a la privacidad ha sido relegado a un segundo lugar; y, el segundo es que el derecho a la privacidad, como todo derecho humano en el contexto del sistema jurídico estadounidense, tiene eficacia y es exigible sólo respecto del sector público, no del privado. Estos dos factores implican que el derecho a la privacidad tiene un ámbito más limitado en los Estados Unidos que en la Unión Europea.

Mientras la Unión Europea ha adoptado y promovido la adopción de una exhaustiva legislación sobre protección de datos personales, los Estados Unidos han adoptado un régimen fragmentario. En otros términos, cada país miembro de la Unión Europea tiene una ley general de protección de datos que reglamenta el tratamiento de la información personal por el sector público y privado; en cambio, en los Estados Unidos existe una multitud de leyes especiales, tanto a nivel federal como estatal, que regulan el procesamiento de información personal en circunstancias específicas por determinadas entidades responsables de dicho tratamiento[53]. Como resultado de ello, la protección de los datos personales tiene un ámbito más reducido en el sistema estadounidense que en el europeo.

Autorregulación y autocontrol tienen un rol más relevante en el sistema legal estadounidense que en la Unión Europea. Como resultado de ello, en los Estados Unidos existe escaso margen para el establecimiento de una autoridad federal que regule, promueva y supervise el cumplimiento de la normativa so-

---

[52] En los Estados Unidos, el derecho a la vida privada carece de un expreso reconocimiento constitucional, sin embargo, su protección se ha derivado de la primera, la cuarta y la decimocuarta enmiendas a la Constitución, las que proveen protección frente a la intrusión gubernamental en la vida privada, pero no así respecto de privados.

[53] Entre el farragoso número de leyes federales y estatales, a modo de ejemplo, pueden ser mencionadas: *Fair Credit Reporting* (1970), *Privacy Act* (1974), *Electronic Funds Transfer Act* (1978), *Right to Financial Privacy Act* (1978), *Cable Communications Policy Act* (1984), *Electronic Communications Privacy Act* (1986), *Video Privacy Protection Act* (1988), *Telephone Consumer Protection Act* (1991), *Driver's Privacy Protection Act* (1994), *Telecommunications Act* (1996), *Consumer Credit Reporting Reform Act* (1996), *Aviation and Transportation Security Act* (2001), y *Can Spam Act* (2003).

bre protección de datos personales, a diferencia de la Unión Europea, donde la existencia de una autoridad tal es considerada un elemento esencial para la protección de los datos personales. Incluso en aquellos casos en que existe alguna autoridad pública competente en los Estados Unidos, ésta usualmente tiene menos mecanismos para supervisar el efectivo cumplimiento de la ley en relación a aquéllos de que disponen las autoridades europeas.

Las diferencias antes mencionadas hacen un tanto complicado para las autoridades de la Unión Europea autorizar la transferencia de datos personales hacia los Estados Unidos, un país que no satisface el estándar de adecuación en el nivel de protección que provee a los datos personales. A efectos de evitar el bloqueo a la transferencia de datos, la Unión Europea y los Estados Unidos trabajaron intensamente durante la segunda mitad de los años noventa en negociaciones que, finalmente, concluyeron con la adopción del "Acuerdo de Puerto Seguro", el cual intenta reconciliar ambos sistemas a través de la provisión de un "nivel adecuado de protección" los datos personales transferidos desde la Unión Europea a los Estados Unidos[54].

A través de su adhesión al "Acuerdo de Puerto Seguro", los organismos asumen la obligación de cumplir con varios principios relativos al tratamiento de datos personales, los cuales básicamente reconocen los derechos de los titulares de datos personales, imponen obligaciones en los responsables de tratamiento, establecen principios aplicables al procesamiento de la información, y responsabilidad para el caso de infracción. Además, dichas entidades deben adoptar mecanismos para garantizar la efectiva aplicación de los mencionados principios, tales como recursos independientes, procedimientos de monitoreo, medidas de reparación, y sanción de infracciones. En otros términos, las entidades partícipes de la iniciativa adoptan mediante autorregulación, en vez de que por ley, las reglas aplicables al tratamiento de datos y los medios para asegurar su efectiva aplicación.

El "Acuerdo de Puerto Seguro" no es legalmente obligatorio o exigible *per se,* sino que las organizaciones estadounidenses que desean ser receptoras de datos personales provenientes de la Unión Europea deben aceptar voluntariamente la aplicación del Acuerdo, certificar su compromiso, y notificar este al Departamento de Comercio de los Estados Unidos. Dicha notificación debe ser renovada anualmente, incluyendo información básica sobre la organización, el procesamiento de los datos que provienen de la

[54] El "Acuerdo de Puerto Seguro" y sus anexos están disponibles en el sitio web del Departamento de Comercio de los Estados Unidos, en <http://www.export.gov/safeharbor/> (última visita: 29 de enero de 2010), mientras que los reportes, opinión y decisión de las autoridades de la Unión Europea están disponibles en <http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_en.htm> (última visita: 29 de enero de 2010).

Unión Europea, y las políticas de la organización a su respecto. La misma organización o terceras partes verifican el cumplimiento de las obligaciones asumidas. Huelga decir que las organizaciones adheridas no deben proveer un "nivel adecuado de protección" a toda la información, si no que a lo menos a aquélla proveniente de la Unión Europea desde el momento de su adhesión al Acuerdo[55].

A efectos de supervisar el cumplimiento del Acuerdo, a pesar de los mecanismos previstos por las mismas instituciones que adhieren, el Departamento de Comercio de los Estados Unidos ha designado a la Federal Trade Commission (FTC) como autoridad supervisora. La FTC tiene competencia para enfrentar actos y prácticas injustas y defraudatorias que afectan el comercio. Sin embargo, en principio, la FTC carece de competencia cuando la información tiene otros propósitos, tal como en telecomunicaciones y transporte; en estos casos la FTC tiene, en el mejor de los casos, una competencia residual o concurrente con otras autoridades, tales como el Federal Reserve Board, la Office of Thrift Supervision, el National Credit Union Administration Board, el Departamento de Transporte, y el Departamento de Agricultura.

Inicialmente, el "Acuerdo de Puerto Seguro" creó optimistas reacciones, ya que anticipaba la posibilidad de armonizar los marcos normativos de los Estados Unidos y de la Unión Europea[56]. Sin embargo, el tiempo ha permitido apreciar los reales efectos del Acuerdo: la multiplicidad de las disposiciones legales aplicables, el mosaico de autoridades de supervisión, el limitadísimo "enforcement", el amplio margen para la autorregulación, el aún reducido número de organizaciones que han adherido[57], y la credibilidad del mecanismo de auto-certificación[58], son factores que generan cierta decepción

---

[55] El "Acuerdo de Puerto Seguro" establece algunos casos en los cuales el procesamiento de datos personales no es reglamentado por sus principios, tales como las actividades periodísticas; otros en los cuales sus principios son aplicables sólo parcialmente, tales como el procesamiento de datos personales en el contexto de una relación laboral; y, también, algunas disposiciones aplicables a circunstancias especiales, como la fusión y la absorción de entidades.

[56] Muñoz, Santiago, *La regulación de la red. Poder y Derecho en internet* (Madrid, Taurus, 2000), pp. 181-189.

[57] De acuerdo a un reciente estudio realizado por Galexia, una empresa consultora especializada en privacidad y comercio electrónico, a diciembre del 2008, de las 1.597 organizaciones registradas en Puerto Seguro, sólo 1.109 eran efectivamente miembros. Véase: Galexia, *The US Safe Harbour-Fact or Fiction?*, 2008, disponible en <http://www.galexia.com/public/about/news/about_news-id143.html> (última visita: 5 de mayo de 2010).

[58] De las 1.597 organizaciones registradas en Puerto Seguro sólo 348 reunían los requisitos básicos previstos en los Acuerdos de Puerto Seguro. Ibíd.

sobre la eficacia del "Acuerdo de Puerto Seguro" y el nivel de protección que este proveería para los datos personales[59].

A pesar de las limitada utilidad del "Acuerdo de Puerto Seguro", la Unión Europea ha reconocido a las entidades adheridas a él como proveedoras de un adecuado nivel de protección y, consiguientemente, ha autorizado la transferencia de datos personales desde la Unión Europea hacia ellas. Así pues, pareciera ser que ni la ausencia de una autoridad de supervisión independiente ni la carencia de un régimen legal comprensivo, inclusivo del tratamiento de datos efectuadas tanto en el sector público como el privado, han constituido barreras para el libre flujo de información desde la Unión Europea a los Estados Unidos, ni, como veremos, deberían constituirlo en lo sucesivo.

2. *La adecuación de Argentina*

El 2000, Argentina adoptó su primera ley de protección de los datos personales[60]. La nueva ley seguía muy de cerca las provisiones de la ley española de 1992[61]; como resultado, la ley argentina tiene un alcance general y aplica al tratamiento automatizado y manual de datos personales efectuados por el

---

[59] El sistema estadounidense ha sido seriamente criticado por la insuficiente protección que brinda al derecho a la privacidad, especialmente en conexión con el procesamiento de información personal, y por su excesiva atención a los requerimientos del mercado. Algunos autores abogan por la adopción de una autoridad de supervisión federal, a similitud de la adoptada en otros países, o a lo menos capaz de armonizar las distintas políticas existentes en la materia. Para una temprana sugerencia en tal sentido, véase: Shapiro, Andrew, *The Control Revolution: How the Internet Is Putting Individuals in Charge and Changing the World We Know* (Nueva York, Public Affairs, 1999). En el mismo sentido: Schwartz, Paul, *Prepared Statement at Senate Commerce Committee Hearing on Internet Privacy*, July 11, 2001; y, Dash, Eric, *Europe Zips Lips; U.S. Sells ZIPs,* en *New York Times*, 7 de agosto de 2005. En referencia a la transferencia de datos personales de pasajeros y abogando por un sistema ecléctico, similar al australiano, véase: Manny, Carter, *EU Privacy and U.S. Security: The Tension Between EU Data Protection Law and U.S. Efforts to Use Airlines Passenger Data to Fight Terrorism and Other Crimes*, Conference Paper, 2004. A favor, pero abogando por la adopción de un tratado sobre la materia, Reidenberg, Joel, *E-Commerce and Trans-Atlantic Privacy,* en *Houston Law Review*, 38 (2001), pp. 717-749. En desacuerdo, argumentando a favor de preservar los estándares estadounidenses: Cate, Fred, *The Changing Face of Privacy Protection in the EU and the U.S.,* en *Indiana Law Review*, 33 (1999), pp. 173-232; y Cate, Fred, *Prepared Statement at Senate Committee Hearing on Internet Privacy*, July 11, 2001.

[60] Ley N° 25.326 sobre *Protección de los datos personales*, de 30 de octubre de 2000.

[61] Gils Carbó, Alejandra, *Régimen legal de las bases de datos y habeas data* (Buenos Aires, 2001), p. 47; Carranza, Luis, *Habeas data: la protección jurídica de los datos personales* (Córdoba, Argentina, Alveroni, 2001), p. 46.

sector público y el privado y, a diferencia de la Dir. 95 de la Unión Europea, la ley aplica tanto a los datos concernientes a personas naturales como a personas jurídicas[62]. Adicionalmente, mediante decreto presidencial, se creó un servicio público que supervigilaría el cumplimiento de la ley: la Dirección Nacional de Protección de los Datos Personales (DNPDP)[63].

Tres años más tarde, la Unión Europea declaró que, a pesar de algunos puntos débiles, Argentina garantiza un "nivel adecuado de protección"[64]. En general, la ley de Argentina cumple con todos los requerimientos sustantivos que la Unión Europea suele constatar en su examen. De hecho, al analizar la seguridad del país, el Grupo del artículo 29 sobre Protección de Datos constató un satisfactorio nivel de protección en las disposiciones sustantivas, tales como aquellas relativas al ámbito de aplicación, los principios generales aplicables al tratamiento de datos, los derechos del titular de datos personales, y las obligaciones de las entidades responsables de dicho tratamiento[65].

---

[62] Artículo 1 Ley N° 25.326.

[63] Decreto N° 1558/2001 Reglamentación de la Ley N° 25.326, 29 de noviembre de 2001.

[64] Commission of the European Communities, Commission Decision of 30/06/2003 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data in Argentina. Brussels, C(2003) 1731 of 30 June 2003 - OJ L 168, 5.7.2003. Disponible en <http://ec.europa.eu/justice_home/fsj/privacy/docs/adequacy/decision-c2003-1731/decision-argentine_en.pdf> (última visita: 26 de enero de 2010).

[65] Article 29, *Data Protection Working Party*, Opinion 4/2002 on the Level of Protection of Personal Data in Argentina, adopted on 3 October 2002. 11081/02/EN/Final WP 63, pp. 11-12. Entre las disposiciones sustantivas, la autoridad de la Unión Europea observó que existen ciertas excepciones para la transferencia transfronteriza de datos personales en la legislación de Argentina que no garantizan un "nivel adecuado de protección" al ser más amplias que aquellas previstas en la Directiva; y que la ley no incluye a favor del titular de datos personales el derecho a no ser objeto de decisiones de relevancia jurídica basadas exclusivamente en el tratamiento automatizado de datos (artículo 15 de la "Directiva de protección de datos"). Adicionalmente, puede agregarse que existe una extensa discusión entre expertos argentinos en cuanto a definir el ámbito de aplicación de la ley en relación con las bases de datos privadas. Para algunos autores, la *Constitución* y la ley parecen limitar su ámbito de aplicación a *"registros o bancos de datos* [...] *privados destinados a proveer informes*"; otros, en cambio, entienden que ello incluye los bancos de datos privados que proveen dichos informes, incluso si ellos no fueron destinados a tal propósito inicialmente. Véanse e.g.: Uicich, Rodolfo, *Habeas Data: Ley 25.326 Comentada y Anotada* (Buenos Aires, Ad Hoc, 2001), pp. 27 y 140; Puccinelli, Oscar, *Protección de datos de carácter personal* (Buenos Aires, Astrea, 2004), pp. 151-153; Basterra, Marcela, *Protección de datos personales: Ley 25.326 y Decreto 1558/01 Comentados* (Buenos Aires, UNAM, 2008), pp. 91-92 y 255-256. Carranza, Luis, cit. (n. 61), p. 49, va aún más lejos en su argumento, sugiriendo que la expresión "informes" puede ser entendida como una limitación adicional al ámbito de aplicación de la ley.

Sin embargo, la ley argentina ha suscitado varias cuestiones en torno a su efectivo cumplimiento. En particular, de acuerdo al reporte elaborado por el Grupo del artículo 29 sobre Protección de Datos, hay tres dificultades asociadas con su cumplimiento: la ausencia de una autoridad de protección de datos independiente, la necesidad de crear agencias de control, y la urgencia de implementar la normativa sobre medidas judiciales a nivel de las provincias[66].

La autoridad sobre protección de datos de la Argentina no es independiente[67]. Inicialmente, la propuesta de ley que devino en la ley de protección de datos establecía una autoridad con "autonomía funcional", pero ello fue eliminado a través de veto presidencial[68], por razones presupuestarias[69]. Mas tarde, nuevamente a través de un decreto presidencial, la DNPDP fue creada, como un servicio público dependiente del Ministerio de Justicia y Derechos Humanos[70]. El propósito del decreto era garantizar independencia funcional a la DNPDP, pero no existe consenso entre la literatura argentina de que el estándar adoptado en el país satisfaga una independencia funcional, ni financiera ni administrativa[71].

---

[66] Article 29, *Data Protection Working Party*, Opinion 4/2002, cit. (n. 65), pp. 7 y 14.

[67] Es interesante constatar que la falta de independencia de la autoridad de supervisión no ha sido un obstáculo para la calificación de Israel como un país que ofrece un "nivel adecuado de protección". Véase el article 29, *Data Protection Working Party*, Opinion 6/2009 *on the Level of Protection of Personal Data in Israel*, adoptado el 1 de diciembre de 2009. 02316/09/EN WP 165. De acuerdo a los dichos del profesor Omer Tene, quien brindó asesoría al gobierno de Israel en el proceso, al enfrentar el dilema entre independencia o *enforcement*, la Unión Europea escogió esto último. Entrevista con Omer Tene, por Martin E. Abrams, article 29 Working Party's Recommendation on Israel's Data Protection Law, disponible en <http://www.huntonprivacyblog.com>, 19 de marzo de 2010 (última visita: 29 de enero de 2010).

[68] Decreto N° 995/2000. Veto y Promulgación de la Ley N° 25.326, 30 de octubre de 2000.

[69] Puccinelli, Oscar, cit. (n. 65), pp. 443 – 444.

[70] La DNPDP es una dependencia de la Secretaria de Justicia y Asuntos Legislativos que depende del Ministerio de Justicia y Derechos Humanos. artículo 29,1 del Decreto N° 1.558/2001.

[71] Gozaní, Osvaldo, *Habeas data: protección de los datos personales: ley y reglamentación* (Santa Fe, Argentina, Rubiznal-Culzoni, 2002), pp. 361-363. En el mismo sentido, Basterra, Marcela, cit. (n. 65), pp. 500-503; Carranza, Luis, cit. (n. 61), pp. 130-131; y Puccinelli, Oscar, cit. (n. 65), pp. 252, 443-447 y 629-640. El Director Nacional de la DNPDP es designado por el Ejecutivo (artículo 29,2 del Decreto N° 1558/2001), el cual N° 1./2001). A efectos de garantizar su independencia, el decreto establece que la DNPDP *"ejercerá sus funciones con plena independencia y no estará sujeto a instrucciones";* sin embargo, ésta no es garantía suficiente, porque está apenas establecida por una disposiciones reglamentaria que es, por definición, incapaz de derogar

Argentina todavía necesita crear agencias de control a nivel de las provincias. La normativa de la DNPDP es ley federal pero no provincial[72]; como resultado, la competencia de la DNPDP está limitada a asuntos federales, y los asuntos provinciales quedan fuera de su competencia, lo cual explica porqué la ley se limita a *"invitar a las provincias a adherir"* a las disposiciones federales[73]. Para superar los inconvenientes creados por la ausencia de agencias de control en las provincias, existe la intensión de crear una red territorial con otros servicios públicos, una vez éstos hayan sido creados[74]. Sin embargo, actualmente no existe tal categoría de agencias ni la mencionada red, lo cual pone en riesgo la efectiva existencia de un "nivel adecuado de protección" para los datos personales.

La implementación de leyes disponiendo por recursos judiciales a nivel de provincias es aún un tema sin resolver en Argentina. La Constitución Federal garantiza un recurso judicial para proteger al titular de los datos personales, denominado *habeas data*[75]. La ley de protección de datos personales ha extendido el ámbito de aplicación y adoptado reglas procesales para tal recurso. Sin embargo, estas disposiciones son ley federal, no ley provincial; de hecho, es competencia de cada provincia adoptar leyes sobre la materia[76], lo cual explica la *"invitación a adherir"* que hace la ley federal[77]. Al año 2008, de acuerdo a Marcela Basterra, catedrática argentina en la materia, solamente dos tercios de las constituciones provinciales y menos de un tercio de la legislación provincial habían introducido las modificación requeridas[78]. Como resultado de ello, la eficacia del habeas data ha sido socavada[79].

---

disposiciones legales, particularmente aquéllas que garantizan el debido proceso. Véase: Gozaní, Osvaldo, cit. Ibíd, p. 361. En el mismo sentido, Puccinelli, O., cit. (n. 65), p. 444, asegura que el sistema no garantiza una mínima independencia de criterio ni la necesaria estabilidad de su Director, conspirando decisivamente contra la plena independencia, especialmente en consideración a su trabajo controlando la enorme cantidad de bases de datos de responsabilidad del Ejecutivo.

[72] Basterra, Marcela, cit. (n. 65), p. 570.

[73] Artículo 44 de la Ley N° 25.326.

[74] Basterra, Marcela, cit. (n. 65), p. 505.

[75] Artículo 43,2 de la *Constitución de la Nación Argentina*. Disponible en <http://www.senado.gov.ar/web/interes/constitucion/english.php> (última visita: 27 de enero de 2010).

[76] Basterra, Marcela, cit. (n. 65), pp. 111-194. En el mismo sentido, Carranza, Luis, cit. (n. 61), p. 54; Peyrano, Guillermo, *Régimen legal de los datos personales y habeas data: comentario a la Ley 25.326 y a la reglamentación adoptada por Decreto 1558/01* (Buenos Aires, Depalma - Lexis-Nexis, 2002); Uicich, Rodolfo, cit. (n. 65), pp. 154-155.

[77] Artículo 44 de la Ley N° 25.326.

[78] Basterra, Marcela, cit. (n. 65), p. 194.

[79] Sin embargo, de acuerdo a Basterra, Marcela, cit. (n. 65), p. 185, al menos las

Es a lo menos impresionante que, a pesar de los problemas antes mencionados, cuando el Grupo del artículo 29 sobre Protección de Datos analizó los mecanismos de cumplimiento y procedimentales previstos en la ley argentina, la autoridad europea concluyera que Argentina garantiza un satisfactorio nivel de cumplimiento con los estándares requeridos por la Unión Europea. Para obtener tal resultado, el Grupo del artículo 29 sobre Protección de Datos apreció: un buen nivel de cumplimiento con las reglas, mediante sanciones administrativas y criminales efectivamente disuasivas; el suministro de soporte y ayuda a los titulares de datos individuales para el ejercicio de sus derechos a través de accesiones judiciales generales; y, la disponibilidad de apropiados mecanismos para compensar a una parte afectada, mediante la aplicación de las reglas generales sobre responsabilidad que son comunes a los países que siguen la tradición del Derecho civil europeo[80].

En verdad, la opinión del Grupo del artículo 29 sobre Protección de Datos acerca del nivel de protección argentino hace suponer que los miembros del grupo no estaban totalmente satisfechos con sus hallazgos; pero esperaban que la real y efectiva aplicación de la ley ratificarían los resultados positivos de su evaluación[81]. Adicionalmente, no podemos prescindir del escenario en el cual la decisión fue fraguada, con la economía argentina padeciendo la peor crisis de su historia, el llamado "corralito", que congeló completamente las cuentas bancarias del país por casi un año. En tal contexto, la decisión de la Unión Europea puede ser vista como una concesión a la debilitada economía del país, a fin de superar un significativo obstáculo para atraer inversión extranjera, particularmente si ésta suponía algún tratamiento de datos personales proveniente de Europa.

La decisión de la Unión Europea sobre el nivel de protección a los datos personales proporcionado en la Argentina y el "Acuerdo de Puerto Seguro" con los Estados Unidos pueden ser analizados como parte de un cuadro mayor. ¿Será posible a partir de ellos pronosticar las decisiones de la Unión Europea en el caso de otros países a futuro? ¿Cómo pueden dichas decisiones ser entendidas y armonizadas en el contexto del GATS? ¿Puede la aplicación del estándar "nivel adecuado de protección" por la Unión Europea ser desafiado ante la Organización Mundial de Comercio? Responder a estas preguntas es especialmente importante para aquellos países que esperan ser reconocidos como seguros, y también para aquéllos que objetan la política de la Unión Europea en materia de privacidad. Responder a dichas preguntas es el propósito de las siguientes páginas.

---

disposiciones federales deberían aplicarse suplementariamente al Derecho provincial.

[80] Article 29, *Data Protection Working Party*, Opinion 4/2002, cit. (n. 65), pp. 13-16.

[81] Ibíd., p. 17.

IV. El "nivel adecuado de protección" En el contexto del Gats

Considerando las causas de la Segunda Guerra Mundial, con el propósito de evitar el proteccionismo y garantizar un régimen de libre comercio, en 1948 fue adoptado el Acuerdo General sobre Aranceles Aduaneros y Comercio (GATT), y posteriormente, en 1995, el Acuerdo General sobre el Comercio de Servicios (GATS), tratados multilaterales que establecen las reglas que gobiernan el comercio internacional, las cuales son hechas cumplir por la Organización Mundial de Comercio (OMC).

A efectos de cumplir con su objetivo, particularmente aquellos concernientes a asegurar un justo y equitativo trato entre todos los partícipes del comercio internacional, el GATS garantiza un tratamiento no discriminatorio entre los miembros de la OMC, a través del cumplimento de varias obligaciones. Para efectos de nuestro análisis, es relevante traer a colación dos de dichas obligaciones: el "principio de trato nacional", que requiere que cada miembro no adoptará medidas discriminatorias entre servicios nacionales y extranjeros[82]; y, el "principio de la nación más favorecida", de acuerdo al cual cada miembro dará inmediata e incondicionalmente a cualquier otro miembro un tratamiento no menos favorable que aquél provisto a cualquier otro miembro[83]. En síntesis, estos principios consagran un tratamiento no discriminatorio entre servicios nacionales y extranjeros, así como entre estos últimos.

Las leyes sobre protección de datos personales podrían infringir ciertas provisiones del GATS, ya que, al requerir un determinado estándar de protección para la información, un país podría adoptar medidas discriminatorias entre los servicios provistos por sus propios nacionales y aquéllos suministrados por extranjeros, o realizar tal tipo de distinción entre los servicios prestados por nacionales de otros países. Como resultado de lo dicho, un país podría verse impedido de adoptar restricciones en el flujo transfronterizo de datos personales, socavando las metas de la política pública implicada en las leyes sobre protección de los datos personales. Para evitar que ello suceda, el GATS ofrece algunas excepciones que permiten adoptar medidas de política pública inconsistentes con las obligaciones del mismo GATS, una de ellas relacionadas con la protección de la privacidad de las personas en relación con el procesamiento y diseminación de sus datos personales[84]. De este modo,

---

[82] Artículo XVII GATS.

[83] Artículo II GATS.

[84] Artículo XIV c) (ii) GATS, que, en lo pertinente, dispone: *"Excepciones generales. A reserva de que las medidas enumeradas a continuación no se apliquen en forma que constituya un medio de discriminación arbitrario o injustificable entre países en que*

el GATS autoriza la adopción y el efectivo cumplimiento de medidas de política pública en principio inconsistentes con el Acuerdo.

Sin embargo, la excepción para protección de datos no es ilimitada[85], ella está sujeta a varios test establecidos en el artículo XIV del GATS a efectos de prevenir un abuso de las excepciones[86]. En nuestro concepto, la apropiada interpretación del artículo XIV requiere que una determinada medida cumpla con un triple test[87]:

i) La medida debe ser alguna de aquellas previstas en el artículo[88]. No existe acuerdo entre los expertos sobre si las excepciones contempladas en el artículo XIV son una lista abierta o cerradas de hipótesis[89]. Sin embargo,

---

prevalezcan condiciones similares, o una restricción encubierta del comercio de servicios, ninguna disposición del presente Acuerdo se interpretará en el sentido de impedir que un Miembro adopte o aplique medidas:/ [...]/ c) *necesarias para lograr la observancia de las leyes y los reglamentos que no sean incompatibles con las disposiciones del presente Acuerdo, con inclusión de los relativos a:*/ [...]/ ii) *la protección de la intimidad de los particulares en relación con el tratamiento y la difusión de datos personales y la protección del carácter confidencial de los registros y cuentas individuales*; [...]".

[85] Swire, Peter - Litan, Robert, *None of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directive* (Washington, D.C., The Brookings Institution, 1998), p. 191. Con sugerencia de una lectura más permisiva, mediante la omisión de cualquier referencia a las limitantes, véase: Papademetriou, Theresa, *EU: Privacy and Personal Data Protection, the "Safe Harbor" Agreement* (Washington, D.C., Law Library of Congress, 2002), p. 6.

[86] Véase: "Work Programme on Electronic Commerce, Progress Report to the General Council", adoptado por el Consejo del Comercio de Servicios el 19 de julio de 1999, WTO document S/L/74, 27 July 1999, párrafo 14.

[87] El artículo XX GATT sirvió de modelo al artículo XIV GATS. Como resultado de ello, los autores suelen estar de acuerdo en que, a pesar de algunas diferencias, es posible usar el primer instrumento para interpretar el segundo de ellos: Krejewski, Markus, *National Regulation and Trade Liberalization in Services: Legal Impact of the General Agreement on Trade and Services (GATS) on National Regulatory Autonomy* (The Netherlands, Kluwer Law International, 2003), p. 157; Trebilcock, Michael - Howse, Robert, *The Regulation of International Trade* (3ª edición, Londres, Routledge, 2005), p. 362; Wounters, Jan - Coppens, Dominic, *Domestic Regulation Within the Framework of GATS*, en Byttebier, Koen - Van Der Borght, Kin (editores), *WTO Obligations and Opportunities: Challenges of Implementation* (Gran Bretaña, The Good New Press, 2007), p. 33; y Swords, Colleen, *At the Department of Foreign Affairs in 2001-2*, en *Canadian Yearbook of International Law*, 40 (2002), pp. 469 ss. De acuerdo con dicha interpretación, pero formulando un test de dos pasos, véase: Footer, Mary - George, Carol, *The General Agreement on Trade and Services*, en Macrory, Patrick F. J. y otros (editores), *The World Trade Organization: Legal, Economic and Political Analysis* (Nueva York, Springer, 2005), I, pp. 799 ss.

[88] Swords, Colleen, cit. (n. 87), p. 486.

[89] Existe desacuerdo entre los expertos en torno a si las excepciones establecidas en el artículo XIV, y la letra c) en particular, constituyen una lista abierta o cerrada.

dicha discusión es irrelevante para los propósitos de analizar las medidas para asegurar el cumplimiento de las leyes o regulaciones sobre protección de la privacidad de las personas en relación con el procesamiento y diseminación de los datos personales, ya que, a diferencia del GATT, ellas están previstas expresamente en el artículo XIV c) (ii) del GATS[90].

ii) La medida debe satisfacer el test de necesidad[91]. De hecho, el GATS establece expresamente que ninguna disposición del Acuerdo se interpretará en el sentido de impedir que un Miembro adopte o aplique medidas "necesarias" para asegurar el cumplimento con la ley. Para satisfacer el test de necesidad, en la mayor parte de los casos, la medida ha balanceado dos factores: la contribución de la medida a la realización de los fines propuestos para ella y la restricción que la medida impone al comercio internacional. Sin embargo, como ha sido recientemente resuelto en el llamado "Gambling case"[92], el test de necesidad no requiere que no exista una medida alternativa consistente con las obligaciones de la OMC "razonablemente disponible"[93].

iii) La medida debe ser consistente en su aplicación. En adición, cualquier medida específica –en nuestro caso, una medida que restringe el flujo transfronterizo de datos personales basada en consideraciones de privacidad– debe

---

Véanse: Krejewski, Markus, cit. (n. 87), pp. 157-161; Wunsch-Vincent, Sacha, *Trade Rules for the Digital Age*, en Panizzon -Pohl - Sauvé (editores), *GATS and the Regulation of International Trade in Services* (Nueva York, Cambridge University Press, 2008), pp. 504-505.

[90] Una parte debe probar un vínculo o conexión entre la medida específica y el interés previsto en el GATS. Véase: "U.S.-Measures Affecting the Cross-Border Supply of Gambling and Betting Services - AB-2005-1 - Report of the Appellate Body", WTO document WT/DS285/AB/R, 7 April 2005, párrafo 292.

[91] Wounters, Jan - Coppens, Dominic, cit. (n. 87), p. 33; Krejewski, Markus, cit. (n. 87), p. 159; Wunsch-Vincent, Sacha, cit. (n. 89), p. 504. Véase: Working Party on Domestic Regulation, *Necessity Test in WTO*, WTO document S/WPDR/W/27, 2 December 2003.

[92] Para una completa explicación del artículo XIV GATS, en el contexto del conocido "Gambling case", véanse: Dogan, Irem, *Taking a Gamble on Public Morals: Invoking the Article XIV Exception to GATS*, en *Brooklyn Journal of International Law*, 32 (2006-2007), p. 1.131; y Petrova, Albena, *The WTO Internet Gambling Dispute as a Case of First Impression: How to Interpret Exceptions Under GATS Article XIV (a) and How to Set the Trend for Implementation and Compliance in WTO Cases Involving "Public Morals" and "Public Order" Concerns?* en *Richmond Journal of Global Law and Business*, 6 (2006-2007), p. 45.

[93] Véase: "U.S.-Measures Affecting the Cross-Border Supply of Gambling and Betting Services - AB-2005-1 - Report of the Appellate Body". WTO document WT/DS285/AB/R, 7 April 2005, párrafos 306 ss. En desacuerdo con el test de necesidad: Regan, Donald, *The Meaning of 'Necessary' in GATT Article XX and GATS Article XIV: the Myth of Cost-Benefit Balancing,* en *World Trade Review* 6 (2007) 3, pp. 347–369.

ser aplicada en una manera que no infringe el GATS, a través de un abuso de las excepción. De acuerdo al encabezado del artículo XIV, una medida no puede ser aplicada en un modo que podría constituir una "discriminación arbitraria o injustificable" entre países en que prevalezcan condiciones similares, o una "restricción encubierta del comercio de servicios".

De acuerdo a Krejewski Markus, la última hipótesis recién mencionada no constituye un test sobre la medida en sí, sino sobre su aplicación, ya sea su aplicación general o su aplicación práctica. La prohibición de "discriminación arbitraria o injustificable" aplicada generalmente obliga a las autoridades gubernamentales a aceptar los estándares adoptados por otros países miembros de la OMC, si ellos son "de una efectividad comparable"[94]. En nuestro caso, al analizar las recomendaciones provistas por el Grupo del artículo 29 sobre Protección de Datos[95], es posible apreciar que la Unión Europea no exige de terceros países exactamente el mismo nivel de protección que el provisto por sus propios miembros, sino un nivel adecuado[96]; y, para efectos de determinar tal nivel, la Dir. 95 sobre Datos Personales y las autoridades de la Unión Europea han introducido suficientes flexibilidades, las que obstan a calificar dichas recomendaciones como una discriminación arbitraria o injustificable *per se*.

Por su parte, Peter Swire y Robert Litan han identificado cuatro hipótesis en las cuales las medidas adoptadas para asegurar el cumplimiento de las leyes o regulaciones relativas a la protección de la privacidad podrían infringir el GATS mediante su real aplicación práctica. De ellas, y considerando el estándar de adecuación de la Unión Europea, dos parecen relevantes: la determinación por las autoridades europeas de que un tercer país no brinda una protección adecuada pese a disponer una fuerte protección legal y práctica de la privacidad; y la obstaculización a las transferencias de datos hacia un país que provee adecuado nivel de protección a ciertos individuos (o en determinados casos), a pesar de carecer de un régimen general que garantice un "nivel adecuado de protección"[97].

---

[94] Krejewski, Markus, cit. (n. 87), p. 162.

[95] Working Party on the Protection of Individuals with regard to the Processing of Personal Data, Working Document: *Transfers of Personal Data to Third Countries*: *Applying Articles 25 and 26 of the EU data protection directive*, 24 July 1998. DG XV D/5025/98 WP 12.

[96] Aquí hace sentido la distinción entre niveles de protección "adecuado" y "equivalente".

[97] Los mencionados autores agregan otros dos casos: *i*) cuando una específica ley de protección de datos es en los hechos una disfrazada restricción al comercio de servicios, una hipótesis que los autores rechazan para el caso de la Directiva; y *ii*) cuando la ley impone una carga significativamente desproporcionada en un tercer país y no hay una adecuada justificación que no sea meramente proteccionista, algo bastante difícil de

La primera hipótesis de desafío para el estándar de la Unión Europea podría presentarse en el caso de adoptarse una decisión de inadecuación respecto de un tercer país que tiene una protección legal y práctica de la privacidad más fuerte que otro país que ha sido calificado de adecuado previamente. Para ejemplificar esto, supongamos que Uruguay desea ser reconocido como un país que provee un adecuado nivel de protección para los datos personales[98]. El 2008, Uruguay adoptó una ley sobre protección de datos, la cual en general sigue la normativa de la Unión Europea[99]. Como un pequeño estado unitario, Uruguay facilita nuestro análisis y la implementación de su ley; como país depositario de la tradición del Derecho civil, disfruta de varias –si no de todas– las ventajas de Argentina. Al igual que su país vecino, Uruguay no ha establecido una autoridad de protección de datos independiente; solamente ha creado un servicio público bajo la dependencia del Ministerio de Economía[100]. Sin embargo, esta última circunstancia no debería ser un obstáculo para el reconocimiento de Uruguay como un país que ofrece un "nivel adecuado de protección"; en caso contrario, Uruguay podría reclamar en contra de la autoridades de la Unión Europea por una arbitraria e injustificable discriminación, ya que la Unión Europea ya ha aceptado que un país provee un "nivel adecuado de protección", a pesar de carecer de una autoridad independiente que supervise el cumplimiento de la ley.

La segunda hipótesis de desafío para el estándar de la Unión Europea podría presentarse en caso de que ciertos individuos (o transferencias) recibiesen un adecuado nivel de protección en un tercer país, a pesar de que éste no provee adecuación en su régimen de protección de la privacidad en general. Nuevamente a modo de ejemplo, supongamos que Chile decide

---

acreditar en la práctica. Swire, Peter - Litan, Robert, cit. (n. 85), pp. 192-193. En desacuerdo, puntualizando que dichas hipótesis pueden ser encontradas en la política de la Unión Europea: Bergkamp, Lucas, *EU Data Protection Policy: The Privacy Fallacy: Adverse Effects of Europe's Data Protection Policy in an Information-Driven Economy*, en *Computer Law & Security Report* (31 de enero 2002), pp. 31-47.

[98] Recientemente, el Grupo de Trabajo en Protección de Datos ha emitido opinión calificando el nivel de protección brindado por Uruguay como adecuado, lo cual permite vaticinar que próximamente tal país obtendrá dicho reconocimiento por las autoridades de la Unión Europea. Vid., Article 29 – *Data Protection Working Party*, Opinion 6/2010 *on the Level of Protection of Personal Data in the Eastern Republic of Uruguay*, adopted on 12 October 2010. 0475/10/EN WP 177.

[99] Uruguay adoptó la Ley N° 18.331 *Protección de datos personales y acción de habeas data personales*, publicada en el *Diario Oficial* el 18 de agosto de 2008.

[100] La Unidad Reguladora y de Control de Datos Personales depende de la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento (AGESIC), la que, a su vez, depende de la Presidencia de la República. artículo 32 Ley N° 18.331.

que, en vez de modificar su normativa interna para ser un país que ofrece un "nivel adecuado de protección", implementará una suerte de "puerto seguro" similar al adoptado en los Estados Unidos, a efectos de proveer un "nivel adecuado de protección" a los datos personales provenientes de la Unión Europea[101]. Sin mencionar el hecho de que Chile dispone de una ley general sobre protección a la vida privada, que reglamenta el tratamiento de datos personales en el sector público y privado[102], él es un estado unitario y también un receptor de la tradición jurídica del Derecho civil, todos factores que perecen proveer más garantías a las autoridades de la Unión Europea. Parecería que dichas autoridades deberían aprobar la propuesta chilena y que no podrían rehusarla sin adoptar una decisión arbitraria o injustificadamente discriminatoria, pues la Unión Europea ya ha aceptado que las transferencias de datos personales a un país que no provee un "nivel adecuado de protección" en general pueden tener lugar si dicho país provee protección específica para tal transferencia de datos personales.

Naturalmente, como ha sido mencionado previamente, la Unión Europea adopta decisiones caso a caso, como respuesta a un complejo análisis de cada sistema legal, en vez de la simple revisión de la respectiva ley de protección de datos. Adicionalmente, al evaluar un determinado país o un determinado flujo de datos, las autoridades de la Unión Europea usan criterios flexibles. En consecuencia, nuestros recién mencionados casos hipotéticos deben ser leídos como un simple ejercicio especulativo. Sin embargo, en cualquier caso,

---

[101] Este caso hipotético es bastante improbable, porque Chile ha adoptado varias medidas en orden a satisfacer los requerimientos del estándar de protección de la Unión Europea: primero, al incluir el tema en el Acuerdo de Asociación suscrito entre Chile y la Unión Europea en Bruselas, el 18 de noviembre de 2002; segundo, al suscribir un acuerdo de cooperación técnica con la Agencia Española de Protección de Datos, en marzo de 2008; y, tercero, al introducir un proyecto de ley en el Congreso Nacional mediante el cual se modifica la ley de protección de datos en vigor de acuerdo a los estándares de la Unión Europea y de la OCDE, en octubre del 2008, el cual aún se encuentra en tramitación legislativa ante la Cámara de Diputados. Vid. Moción legislativa que *Introduce modificaciones la Ley N° 19.628, sobre protección de la vida privada, y a la Ley N° 20.285, sobre acceso a la información pública* (Boletín: 6120-07).

[102] De hecho, Chile fue el primer país latinoamericano que adoptó una ley general sobre protección de 1999. Sin embargo, por varios años, la legislación chilena careció de una autoridad pública de supervisión en la materia; sólo a partir del 2009, el Consejo para la Transparencia desempeña tal rol, aun cuando exclusivamente respecto de las entidades responsables de tratamiento de datos personales del sector público. Para una sucinta explicación de los principales desafíos para la legislación chilena a efectos de proveer un "nivel adecuado de protección" de acuerdo a los estándares de la Unión Europea, véase: Arrieta, Raúl, *Chile y la protección de datos personales: compromisos internacionales,* en *Chile y la protección de datos personales: ¿Están en crisis nuestros derechos fundamentales?* (Santiago, Ediciones UDP, 2009), pp. 13-22.

teóricamente a lo menos, ni la complejidad ni la flexibilidad autorizan a la adopción de una decisión que aplica criterios basados en una discriminación arbitraria o injustificada, que eventualmente podrían infringir las obligaciones de los países miembros de la OMC.

En síntesis, al armonizar el estándar de adecuación de la Unión Europea con las obligaciones de la OMC, es posible decir que el GATS ha anticipado los obstáculos que las normas sobre privacidad pueden implicar para el comercio internacional. De hecho, el acuerdo GATS tolera la adopción de medidas en principio inconsistentes con los principios de la OMC, si ellas son necesarias para asegurar el cumplimiento de las leyes sobre protección de la privacidad de las personas en relación con el tratamiento y la diseminación de datos personales. Sin embargo, tales medidas no puede ser aplicadas en un modo que podría constituir un medio de discriminación arbitrario o injustificable entre países en que prevalezcan condiciones similares, o una restricción encubierta del comercio de servicios. En tal contexto, las decisiones previas de la Unión Europea suscitan un cuestionamiento legítimo acerca de si serán sustentadas consistentemente en futuros casos, manteniendo los flexibles criterios mostrados en el "Acuerdo de Puerto Seguro" con los Estados Unidos y la calificación de Argentina como un país que ofrece un "nivel adecuado de protección" a los datos personales, o bien si la Unión Europea reculará respecto de ciertos requerimientos a riesgo de un caso ante la OMC.

V. Conclusiones

El creciente flujo transfronterizo de datos personales muestra la urgente necesidad de adoptar una aproximación internacional a efectos de garantizar un apropiado nivel de protección para las personas concernidas por la información, pero también para evitar la adopción de barreras innecesarias al libre movimiento de tal información, con sus nocivos efectos para una economía global e interconectada.

Al enfrentar los desafíos recién mencionados, la Unión Europea ha adoptado una directiva comunitaria que regula el procesamiento de datos personales, la cual prohíbe el flujo transfronterizo de datos personales hacia terceros países que no garantizan un "nivel adecuado de protección". Para determinar dicha adecuación, las autoridades de la Unión Europea han adoptado un criterio flexible que requiere la adopción y el cumplimiento de normativa sobre protección de los datos personales, lo cual, a su vez, satisface las disposiciones del GATS.

Desafortunadamente, el estándar de "nivel adecuado de protección" ha sido aplicado en un extremadamente reducido número de casos. De ellos, los más relevantes parecen ser el "Acuerdo de Puerto Seguro", que permite

la transferencia de datos personales desde la Unión Europea a los Estados Unidos, y la calificación de Argentina como un tercer país que provee un "nivel adecuado de protección". Sin embargo, ambos casos recién mencionados suscitan cuestionamiento acerca del límite concedido por la Unión Europea en su evaluación de terceros países.

En el caso de los Estados Unidos, como ha quedado dicho, ni la ausencia de una autoridad de supervisión independiente ni la carencia de un régimen legal comprensivo, inclusivo del tratamiento de datos efectuadas tanto en el sector público como el privado, han constituido barreras para el libre flujo de información desde la Unión Europea a los Estados Unidos, en los permisivos términos del Acuerdo de Puerto Seguro.

En el caso de Argentina, si bien el país dispone de una normativa sobre protección de datos comprensiva, cuyas disposiciones sustantivas siguen muy de cerca los estándares de la Unión Europea, no sucede lo mismo con los mecanismos previstos para garantizar su cumplimiento. En este punto, la normativa argentina parece aún insatisfactoria. En primer término, la autoridad nacional carece de independencia, un requisito que la Unión Europea ha calificado de esencial para la protección de los datos personales. En adición a lo mencionado, la ley aún requiere la implementación de sus disposiciones, en lo concerniente a mecanismos de protección, en un significativo número de las provincias, esto es, la protección es aún fragmentaria.

Las decisiones de las autoridades de la Unión Europea en los casos de los Estados Unidos y la Argentina crean razonables dudas acerca de su consistencia con decisiones futuras sobre la adecuación de terceros países en relación con las provisiones de la Dir. 95 de Protección de Datos y el GATS; como resultado de ello, la protección de los datos personales o el libre flujo transfronterizo de la información personal podían verse seriamente amenazados. En efecto, en orden a cumplir con la obligación establecida en el GATS, que impide la discriminación arbitraria o injustificable entre países, la Unión Europea ha socavado su propósito de obtener un nivel de protección adecuado cualquiera sea el lugar a que ésta exporte datos personales, ya que ni la carencia de un régimen comprensivo de protección a los datos personales ni la relativa precariedad de los mecanismos previstos para garantizar el cumplimiento de la ley podrán constituir óbices al reconocimiento de un tercer país como uno que provee un nivel de protección adecuado.

El dilema de la Unión Europea entre obtener un nivel de protección adecuado para los datos personales por terceros países, acorde a los criterios de la Dir. 95 de Protección de Datos, y honrar la obligación establecida en los GATS en orden a no ejercer discriminación arbitraria o injustificable respecto de terceros países, pone en entredicho la capacidad de un país o un conglomerado de ellos para imponer unilateralmente un estándar global de

protección en materia de datos personales. Pese a la poco halagüeña experiencia en la materia, parece necesario insistir en la construcción multilateral de, a lo menos, un mínimo común denominador internacional para lograr simultáneamente una apropiada protección de los datos personales y un satisfactorio nivel de libertad para el flujo de información personal.

Bibliografía

Alonso, Diana, *El futuro de la protección de datos a nivel europeo*, en *Encuentros sobre Informática y Derecho* (Instituto de Informática Jurídica, Universidad Pontificia Comillas, Madrid, 1995 – 1996).

Arrieta, Raúl, *Chile y la Protección de Datos Personales: Compromisos Internacionales,* en *Chile y la Protección de Datos Personales: ¿Están en crisis nuestros derechos fundamentales?* (Santiago, Ediciones UDP, 2009).

Basterra, Marcela, *Protección de datos personales: Ley 25.326 y Decreto 1558/01 Comentados* (Buenos Aires, UNAM, 2008).

Bergkamp, Lucas, *EU Data Protection Policy: The Privacy Fallacy: Adverse Effects of Europe's Data Protection Policy in an Information-Driven Economy*, en *Computer Law & Security Report* (31 de enero de 2002).

Carranza, Luis, *Habeas Data: La protección jurídica de los datos personales* (Córdoba-Argentina, Alveroni Ediciones, 2001).

Cate, Fred, *Prepared Statement at Senate Committee Hearing on Internet Privacy* (11 de julio de 2001).

Cate, Fred, *The Changing Face of Privacy Protection in the EU and the U.S.,* en *Indiana Law Review*, 33 (1999).

Cerda Silva, Alberto, *Mecanismos de control en la protección de datos en Europa,* en *Ius et Praxis,* 12 (Talca, Chile, 2006).

Dash, Eric, *Europe Zips Lips; U.S. Sells ZIPs,* en *New York Times* (7 de Agosto de 2005).

Dogan, Irem, *Taking a Gamble on Public Morals: Invoking the Article XIV Exception to GATS.*, en *Brooklyn Journal of International Law*, 32 (2006-2007).

Estadella-Yuste, Olga, *La protección de la intimidad frente a la transmisión internacional de datos personales* (Madrid, Editorial Tecnos, 1995).

Footer, Mary - George, Carol, *The General Agreement on Trade and Services*, en Macrory, Patrick F. J. y otros (editores), *The World Trade Organization: Legal, Economic and Political Analysis* (Nueva York, Springer, 2005).

Gils Carbó, Alejandra, *Régimen legal de las bases de datos y habeas data* (Buenos Aires, 2001).

Goldsmith, Jack - Wu, Tim *Who Controls the Internet: Illusions of a Borderless World* (Nueva York, Oxford University Press, 2008).

Gozaní, Osvaldo, *Habeas data: protección de los datos personales: ley y reglamentación* (Santa Fe - Argentina, Rubiznal-Culzoni, 2002).

Heredero, Manuel, *La Directiva 95 Comunitaria de Protección de Datos de Carácter Personal* (Pamplona, Aranzadi, 1997).

Krejewski, Markus, *National Regulation and Trade Liberalization in Services: Legal Impact of the General Agreement on Trade and Services (GATS.) on National Regulatory Autonomy* (The Netherlands, Kluwer Law International, 2003).

Manny, Carter, *EU Privacy and U.S. Security: The Tension Between EU Data Protection Law and U.S. Efforts to Use Airlines Passenger Data to Fight Terrorism and Other Crimes* (Conference Paper, 2004).

Muñoz, Santiago, *La regulación de la Red. Poder y Derecho en internet* (Madrid, Taurus, 2000).

Papademetriou, Theresa, *EU: Privacy and Personal Data Protection, the "Safe Harbor" Agreement* (Washington, D.C., Law Library of Congress, 2002).

Petrova, Albena, *The WTO Internet Gambling Dispute as a Case of First Impression: How to Interpret Exceptions Under GATS. Article XIV (a) and How to Set the Trend for Implementation and Compliance in WTO Cases Involving "Public Morals" and "Public Order" Concerns?*, en *Richmond Journal of Global Law and Business*, 6 (2006-2007).

Peyrano, Guillermo, *Régimen legal de los datos personales y habeas data: comentario a la Ley 25.326 y a la reglamentación adoptada por Decreto 1558/01* (Buenos Aires, Depalma - LexisNexis, 2002).

Puccinelli, Oscar, *Protección de datos de carácter personal* (Buenos Aires, Astrea, 2004).

Regan, Donald, *The Meaning of 'Necessary' in GATT. Article XX and GATS. Article XIV: the Myth of Cost-Benefit Balancing,* en *World Trade Review*, 6 (2007) 3.

Reidenberg, Joel, *E-Commerce and Trans-Atlantic Privacy,* en *Houston Law Review*, 38 (2001).

Saarenpää, Ahti, *Europa y la protección de los datos personales,* en *Revista Chilena de Derecho Informático,* 3 (2003).

Schwartz, Paul, *Prepared Statement at Senate Commerce Committee Hearing on Internet Privacy* (11 de julio de 2001).

Shapiro, Andrew, *The Control Revolution: How the Internet Is Putting Individuals in Charge and Changing the World We Know (*Nueva York, Public Affairs, 1999).

Swire, Peter - Litan, Robert, *None of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directive* (Washington, D.C., The Brookings Institution, 1998).

Swords, Colleen, *At the Department of Foreign Affairs in 2001-2*, en *Canadian Yearbook of International Law*, 40. (2002).

Trebilcock, Michael - Howse, Robert, *The Regulation of International Trade* (3ª edición, Londres, Routledge, 2005).

Uicich, Rodolfo, *Habeas Data: Ley 25.326 comentada y anotada* (Buenos Aires, Ad Hoc. 2001).

Wounters, Jan - Coppens, Dominic, *Domestic Regulation Within the Framework of GATS.*, en Byttebier, Koen - Van Der Borght, Kin (editores), *WTO Obligations and Opportunities: Challenges of Implementation* (Gran Bretaña, The Good New Press, 2007).

Wunsch-Vincent, Sacha, *Trade Rules for the Digital Age*, en Panizzon - Pohl - Sauvé (editores), *GATS. and the Regulation of International Trade in Services* (Nueva York, Cambridge University Press, 2008).