El Mercosur y la Decisión de la Comisión Europea sobre la adecuación de la legislación argentina en materia de protección de datos personales. ¿Se debe pensar en una solución a nivel regional ?

Pérez Asinari, María Veroníca

Published in:
Revista de Derecho Internacional y del Mercosur

Publication date:
2003

Document Version
le PDF de l'éditeur

Artículo a publicarse en *Revista de Derecho Internacional y del Mercosur*, Editorial La Ley, Buenos Aires, julio 2003.

El Mercosur y la Decisión de la Comisión Europea sobre la adecuación de la legislación argentina en materia de protección de datos personales ¿Se debe pensar en una solución a nivel regional?

María Verónica Pérez Asinari
Investigadora en el *Centre de Recherches Informatique et Droit (CRID)*,
Facultés Universitaires Notre-Dame de la Paix,
Namur, Bélgica.
veronica.perez@fundp.ac.be
http://www.droit.fundp.ac.be/crid/

1) Introducción

La Unión Europea (UE) estableció, a partir de la Directiva 95/46/CE,[1] y en lo que hace a la transferencia internacional de datos personales, un espacio liberalizado *ad intra* y con fuertes obstáculos *ad extra*. Para lograr la liberalización interior fue preciso asegurar un nivel de protección similar (considerada "equivalente") en todos los estados miembros. Con ese objeto se recurrió a la coordinación de legislaciones, de modo que una transferencia no se encontrara con el obstáculo de verse impedida de realizar dada la falta de garantías respecto del derecho fundamental a la intimidad y a la protección de los datos personales en el Estado de destino.

Para poder realizar una transferencia de datos personales con destino a un país que no pertenezca a la UE[2] es preciso considerar los Artículos 25 y 26 de la Directiva.

En el Artículo 25.1 de la Directiva encontramos el principio general por el cual se establece la prohibición para la realización de una tranferencia internacional si el país de destino no garantiza un nivel de protección de los datos personales considerado "adecuado"[3] al de la UE.

[1] Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. DOCE L 281/3, 23/11/95. De aquí en mas "la Directiva". Para un estudio general de la Directiva ver: Marie-Hélène BOULANGER, Cécile de TERWANGNE, Thierry LEONARD, Sophie LOUVEAUX, Damien MOREAU, e Yves POULLET "La Protection des données à caractère personnel en Droit Communautaire", *Journal des Tribunaux Droit Européen*, junio 1997, p. 1 y ss.

[2] La Directiva es también de aplicación en el Espacio Económico Europeo (EEE).

[3] Es preciso diferenciar el método "adecuado" del "equivalente". Mientras el primero implica un análisis integral, flexible, caso por caso y funcional del sistema regulatorio ofrecido en el tercer país (es el sistema elegido por la UE respecto de los países no miembros -*ad extra*-), el segundo implica la existencia de la misma

Dicho precepto es la regla general, la cual será flexibilizada por diversas disposiciones de la misma Directiva que veremos mas adelante. Una de ellas es la posibilidad establecida en el Artículo 25.6 de la Directiva, según la cual la Comisión podrá hacer constar en una Decisión que un país tercero garantiza un nivel de protección adecuado a efectos de la protección de los datos personales, a partir de la cual los datos podrán circular libremente entre la UE y el país en cuestión.

Luego de una solicitud para obtener una Decisión de Adecuación respecto del régimen jurídico argentino en la materia, presentada por el Embajador de la República Argentina ante la Unión Europea a finales de 2001, el Grupo de Trabajo sobre Protección de Datos Personales del Artículo 29[4] emitió un Dictamen favorable al respecto.[5] Recientemente la Comisión adoptó una Decisión de Adecuación de la protección de los datos personales en Argentina[6]. Se trata de la primera Decisión de esta naturaleza respecto de un país latinoamericano, y reviste, notoriamente, una importancia trascendente no sólo a nivel jurídico sino también a nivel de política internacional.

Podemos preguntarnos entonces cómo afectará esta Decisión de Adecuación los flujos de datos personales *intra* Mercosur. ¿Tienen, los países del Mercosur, un régimen jurídico en la materia que podría ser considerado "adecuado" al de la UE? ¿Necesita, el Mercosur, armonización legislativa en este tema para facilitar no sólo la transferencia internacional de datos personales *intra* Mercosur, sino también la transferencia hacia o desde la UE? ¿Es conveniente lograr una posición común *intra* Mercosur *vis-à-vis* las negociaciones para el ALCA (Area de Libre Comercio de las Américas) en aquellas materias con implicancias en el tema que desarrollamos como, por ejemplo, el comercio electrónico?

En este artículo vamos a intentar un acercamiento a estas cuestiones desde la situación interna en materia de protección de datos personales de cada país miembro del Mercosur. No obstante, señalamos que nuestra evaluación es no solo sintética, sino que hace única referencia a fuentes legislativas generales, sin llegar a otras fuentes, por ejemplo autorregulatorias, corregulatorias o legislación sectorial (por ejemplo: sector financiero, salud, publicidad, etc.) las cuales deben ser atendidas como *conditio sine qua non* en todo análisis de adecuación. Haremos antes una breve descripción de la regulación europea en materia de transferencia internacional de datos personales de modo que podamos entender cómo funciona este mecanismo y la importancia que reviste una Decisión de Adecuación a nivel nacional, así como también el valor agregado que podría representar una Decisión de este tipo a nivel regional.

---

protección legislativa en ambos países bajo análisis (es el sistema elegido por la Convención del Consejo de Europa n. 108, y por la UE –*ad intra*-).

[4] El Grupo de Trabajo se creó en virtud del artículo 29 de la Directiva 95/46/CE. Se trata del órgano consultivo independiente de la UE sobre protección de los datos y la vida privada. Sus tareas se definen en el artículo 30 de la Directiva 95/46/CE y en el artículo 14 de la Directiva 97/66/CE.

[5] Grupo de Trabajo sobre Protección de Datos del Artículo 29, Dictamen 4/2002 sobre el nivel de protección de datos personales en Argentina, 3 de octubre de 2002, disponible en : http://www.europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp63_es.pdf

[6] Decisión de la Comisión de 30/06/2003 con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo sobre la adecuación de la protección de los datos personales en Argentina, Bruselas, 30/06/2003, C(2003)1731 final.

2) Síntesis de la regulación de la UE en materia de transferencia internacional de datos personales a países terceros[7]

2.1. Principio general

Tal como adelantamos en la introducción, el principio general se encuentra enunciado en el Artículo 25.1 de la Directiva:[8] *"Los Estados miembros dispondrán que la transferencia a un país tercero de datos personales que sean objeto de tratamiento o destinados a ser objeto de tratamiento con posterioridad a su transferencia, únicamente pueda efectuarse cuando, sin perjuicio del cumplimiento de las disposiciones de Derecho nacional adoptadas con arreglo a las demás disposiciones de la presente Directiva, el país tercero de que se trate garantice un nivel de protección adecuado."*

La Directiva no aporta una definición respecto de qué debe entenderse por "carácter adecuado". El apartado 2 de este Artículo aclara no obstante que "*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 transferencias 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 país tercero de que se trate, así como las normas profesionales y las medidas de seguridad en vigor en dichos países."*

---

[7] Este apartado fue presentado en videoconferencia por la autora en ECOMDER 2002, *Congreso Internacional por Internet sobre Aspectos Jurídicos del Comercio Electrónico*, bajo el título "Transferencia Internacional de Datos Personales, El Acuerdo de Puerto Seguro", disponible en : http://www.ecomder.com/boletin/boletin0102.htm

[8] Un desarrollo mas profundo del tema se puede ver en: Yves POULLET, Bénédicte HAVELANGE, Axel LEFEBVRE, Marie-Hélène BOULANGER, Herbert BURKERT, Cécile De TERWANGNE, "Elaboration d'une méthodologie pour évaluer l'adéquation du niveau de protection des personnes physiques à l'égard du traitement de données à caractère personnel", *Centre de Recherches Informatique et Droit* (CRID). Commission Européenne – DG XV. Contrat ETD/95/B5-3000/165, Diciembre 1996, este estudio se encuentra disponible en el sitio Web del CRID: http://www.droit.fundp.ac.be/crid/privacy/default.htm . Yves POULLET, Sophie LOUVEAUX y María Verónica PEREZ ASINARI "Data Protection and Privacy in Global Networks: A European Approach…", escrito en el marco del proyecto ECLIP (Electronic Commerce Legal Issues Platform), *The EDI Law Review* 8, Kluwer Law International, Países Bajos, 2001, p. 147-196. Yves POULLET "Pour une justification des articles 4, 25 et 26 de la directive européenne 95/46/CE en matière de flux transfrontières et de protection des données", escrito en ocación de la Conferencia sobre Datos personales organizada por la Comisión Europea, 30 de septiembre, 1 de octubre, 2002, Bruselas, disponible en http://www.europa.eu.int/comm/internal_market/en/dataprot/lawreport/speeches/poullet_fr.pdf. Jan DHONT y María Verónica PEREZ ASINARI "New Physics and the Law. A Comparative Approach to the EU and US Privacy and Data Protection Regulation. Looking for Adequate Protection", a publicarse en *L'utilisation de la métode comparative en droit Européen – Usage of Comparative methodology in European law*, Presse Universitaire de Namur, 2003.

Esta enunciación no es taxativa sino meramente ejemplificativa. La noción de "circunstancias" debe interpretarse en sentido amplio, proveyendo una gama de parámetros que deberán ser incluídos en el análisis. Otros ejemplos pueden mencionarse: códigos de ética internos, métodos de certificación o sellado (labelling), nivel de educación en la materia de protección de datos personales de los empleados que procesan información, nivel de claridad de una política de protección de datos (por ejemplo en un sitio Web), métodos de cumplimiento y ejecución, independencia de los órganos de ejecución, diseño de la arquitectura de programas o software (por ejemplo PETs)[9], métodos de anonimización, etc.

El Grupo de Trabajo del Artículo 29 elaboró diversos documentos relativos a las transferencias internacionales. Quizás, el que revista mayor importancia sea el nº 12: *"Transferencias de datos personales a terceros países: aplicación de los artículos 25 y 26 de la Directiva sobre protección de datos de la UE"*.[10] Entre otras cuestiones, aborda el tema relativo a qué es lo que debe entenderse por "protección adecuada".

Así describe cuáles son los "principios de contenido" y los "requisitos de procedimiento" cuyo cumplimiento puede considerarse un standard mínimo para juzgar adecuada la protección:[11]

"*i) Principios de contenido*

Se sugiere la inclusión de los siguientes principios básicos:

1) Principio de limitación de objetivos - los datos deben tratarse con un objetivo específico y posteriormente utilizarse o transferirse únicamente en cuanto ello no sea incompatible con el objetivo de la transferencia. Las únicas excepciones a esta norma serían las necesarias en una sociedad democrática por una de las razones expuestas en el artículo 13 de la Directiva.

2) Principio de proporcionalidad y de calidad de los datos - los datos deben ser exactos y, cuando sea necesario, estar actualizados. Los datos deben ser adecuados, pertinentes y no excesivos con relación al objetivo para el que se transfieren o para el que se tratan posteriormente.

3) Principio de transparencia - debe informarse a los interesados acerca del objetivo del tratamiento y de la identidad del responsable del tratamiento en el tercer país, y de cualquier otro elemento necesario para garantizar un trato leal. Las únicas excepciones permitidas deben corresponder a los artículos 11.2 y 13 de la Directiva.

---

[9] Privacy Enhancing Technologies. Ver : John BORKING y Charles RAAB "Laws, PETs and Other Technologies for Privacy Protection", *Journal of Information, Law and Technology*, 2001, disponible en http://elj.warwick.ac.uk/jilt/01-1/borking.html

[10] Grupo de Trabajo sobre Protección de Datos del Artículo 29, Documento de Trabajo "Transferencias de datos personales a terceros países: aplicación de los artículos 25 y 26 de la Directiva sobre protección de datos de la UE", 24 de julio de 1998, disponible en : http://www.europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp12_es.pdf

[11] Transcribimos esta consideración dado que reviste importancia para entender qué es lo que se evaluó respecto de la legislación argentina por parte del Grupo del Artículo 29.

4) Principio de seguridad - el responsable del tratamiento debe adoptar medidas técnicas y organizativas adecuadas a los riesgos que presenta el tratamiento. Toda persona que actúe bajo la autoridad del responsable del tratamiento, incluido el encargado del tratamiento, no debe tratar los datos salvo por instrucción del responsable del tratamiento.

5) Derechos de acceso, rectificación y oposición - el interesado debe tener derecho a obtener una copia de todos los datos a él relativos, y derecho a rectificar aquellos datos que resulten ser inexactos. En determinadas situaciones, el interesado también debe poder oponerse al tratamiento de los datos a él relativos. Las únicas excepciones a estos derechos deben estar en línea con el artículo 13 de la Directiva.

6) Restricciones respecto a transferencias sucesivas a otros terceros países - únicamente deben permitirse transferencias sucesivas de datos personales del tercer país de destino a otro tercer país en el caso de que este último país garantice asimismo un nivel de protección adecuado. Las únicas excepciones permitidas deben estar en línea con el artículo 26.1 de la directiva (...)."

A continuación figuran ejemplos de principios adicionales que deben aplicarse a tipos específicos de tratamiento:

"1) Datos sensibles - cuando se trate de categorías de datos 'sensibles' (las incluidas en el artículo 8 de la Directiva), deberán establecerse protecciones adicionales, tales como la exigencia de que el interesado otorgue su consentimiento explícito para el tratamiento.

2) Mercadotecnia directa - en el caso de que el objetivo de la transferencia de datos sea la mercadotecnia directa, el interesado deberá tener en cualquier momento la posibilidad de negarse a que sus datos sean utilizados con dicho propósito.

3) Decisión individual automatizada - cuando el objetivo de la transferencia sea la adopción de una decisión automatizada en el sentido del artículo 15 de la Directiva, el interesado deberá tener derecho a conocer la lógica aplicada a dicha decisión, y deberán adoptarse otras medidas para proteger el interés legítimo de la persona.

ii) Mecanismos del procedimiento/de aplicación

En Europa existe un amplio consenso sobre la necesidad de plasmar los principios de la protección de datos en la legislación. También es amplio el consenso en que un sistema de 'supervisión externa' en forma de una autoridad independiente es una característica necesaria de un sistema de cumplimiento de la protección de datos. Sin embargo, en otras partes del mundo no siempre se encuentran estas características.

Con el fin de sentar las bases para evaluar el carácter adecuado de la protección ofrecida, es necesario distinguir los objetivos de un sistema normativo de protección de datos, y sobre esta base juzgar la variedad de diferentes mecanismos de procedimiento judiciales y no judiciales utilizados en terceros países.

Los objetivos de un sistema de protección de datos son básicamente tres:

1) Ofrecer un nivel satisfactorio de cumplimiento de las normas. (Ningún sistema puede garantizar el 100 % de cumplimiento, pero algunos son mejores que otros). Un buen sistema

se caracteriza, en general, por el hecho de que los responsables del tratamiento conocen muy bien sus obligaciones y los interesados conocen muy bien sus derechos y medios para ejercerlos. La existencia de sanciones efectivas y disuasorias es importante a la hora de garantizar la observancia de las normas, al igual que lo son, como es natural, los sistemas de verificación directa por las autoridades, los auditores o los servicios de la Administración encargados específicamente de la protección de datos.

2) Ofrecer apoyo y asistencia a los interesados en el ejercicio de sus derechos. El interesado debe tener la posibilidad de hacer valer sus derechos con rapidez y eficacia, y sin costes excesivos. Para ello es necesario que haya algún tipo de mecanismo institucional que permita investigar las denuncias de forma independiente.

3) Ofrecer vías adecuadas de recurso a quienes resulten perjudicados en el caso de que no se observen las normas. Éste es un elemento clave que debe incluir un sistema que ofrezca la posibilidad de obtener una resolución judicial o arbitral y, en su caso, indemnizaciones y sanciones."

Con lo cual, la adecuación vendrá dada por la presencia de estos principios en el país de destino, cuando se trate de una Decisión de Adecuación emitida por la Comisión Europea, o de la garantía de los mismos en situaciones específicas cuando se trate de transferencias a países que no cuenten con tal resolución, y la legitimación[12] para la transferencia se busque por otras vías, como podría ser la contractual (ver *infra*).

2.2. Derogaciones especiales

No obstante el principio general de prohibición, y atendiendo a la relevancia económica del mercado de la información y también a los compromisos internacionales por los cuales se impide la creación de barreras injustificadas al comercio[13], el Artículo 26.1 de la Directiva presenta una lista de derogaciones al Artículo 25.1, de modo que los estados miembros dispondrán que pueda efectuarse la transferencia, siempre y cuando:

(a)el interesado haya dado su consentimiento inequívocamente a la transferencia prevista; o
(b)la transferencia sea necesaria para la ejecución de un contrato entre el interesado y el responsable del tratamiento o para la ejecución de medidas precontractuales tomadas a petición del interesado, o

[12] En el caso de España, la notificación es exigida previamente a cada transferencia internacional, y en el caso de transferirse datos sensibles se requiere una autorización por parte de la Agencia de Protección de Datos. Ver : Instrucción 1/2000 de 1 de diciembre, de la Agencia de Protección de Datos, relativa a las normas por las que se rigen los movimientos internacionales de datos., disponible en : https://www.agenciaprotecciondatos.org/datd10.htm

[13] Ver : María Verónica PEREZ ASINARI "Is there any Room for Privacy and Data Protection within the WTO Rules?", artículo a publicarse en *The Electronic Communications Law Review*, Kluwer, Países Bajos, 2003. María Verónica PEREZ ASINARI "The WTO and the Protection of Personal Data. Do EU Measures Fall within GATS Exception? Which Future for Data Protection within the WTO e-Commerce Context?", BILETA Conference, *Controlling Information in the Online Environment*, Institute of Computer & Communications law, Queen Mary, University of London, Londres, 14 y 15 de abril 2003, a publicarse en http://www.bileta.ac.uk

(c)la transferencia sea necesaria para la ejecución de un contrato celebrado o por celebrar en interés del interesado, entre el responsable del tratamiento y un tercero.
d) La transferencia sea necesaria o legalmente exigida para la salvaguardia de un interés público importante, o para el reconocimiento, ejercicio o defensa de un derecho en un procedimiento judicial, o
e) la transferencia sea necesaria para la salvaguardia del interés vital del interesado, o
f) la transferencia tenga lugar desde un registro público que, en virtud de disposiciones legales o reglamentarias, esté concebido para facilitar información al público y esté abierto a la consulta por el público en general o por cualquier persona que pueda demostrar un interés legítimo, siempre que se cumplan, en cada caso particular, las condiciones que establece la ley para la consulta.

2.3. Decisiones de adecuación

En el Artículo 25.6 de la Directiva se dispone que la Comisión podrá hacer constar que un país tercero garantiza un nivel de protección adecuado a efectos de la protección de los datos personales.

Hasta el momento la Comisión Europea ha dictado cuatro Decisiones de adecuación basadas en este artículo (además de la relativa a Argentina), respecto de Hungría, Suiza, Canada, y EEUU.[14]

Las dos primeras soluciones revisten un carácter específico y diferenciado de la solución respecto de EEUU (a la cual nos vamos a referir mas adelante). Sin embargo, aclaramos desde ya que mientras las decisiones respecto de Suiza y Hungría fueron adoptadas respecto de todo el régimen normativo de estos países,[15] es decir, sin excluir sector alguno, la Decisión respecto de EEUU no presenta esta característica, y puede ser este un punto crucial que puede generar confusiones.

Actualmente se están llevando a cabo discusiones sobre el uso del Registro de nombres de pasajeros (PNR-Passenger Name Record), habiéndose firmado recientemente una declaración conjunta entre la UE y EEUU sobre el uso del mismo. Esto es consecuencia de lo dispuesto por la *Aviation and Transportation Security Act* del 19 de noviembre de 2001, la cual introduce el imperativo para las empresas que transportan pasajeros de, hacia o dentro de EEUU de proveer, bajo requerimiento, a la Oficina de Protección de Frontera (CBP-*Border Protection Bureau*) acceso electrónico a los datos del PNR contenidos en sus sistemas de reserva y control de embarque.[16]

---

[14] Las Decisiones emitidas por la Comisión , las Opiniones previas del Grupo del Artículo 29 y los comunicados de prensa se encuentran disponibles en :
http://www.europa.eu.int/comm/internal_market/en/dataprot/adequacy/index.htm

[15] La Decisión respecto de Canadá también presenta un régimen especial, dado que solo cubre al sector privado en el curso de operaciones comerciales, según se desprende del ámbito de aplicación de la Canadian Personal Information Protection and Electronic Documents Act (PIPED Act).

[16] Ver : Joint EU-US statement on the transmission of APIS/PNR data from airlines to the United States (6 March 2003), disponible en:
http://www.europa.eu.int/comm/internal_market/privacy/docs/adequacy/declaration_en.pdf

2.3.1. Referencia al *Safe Harbour*

Dada la difusión en la prensa y doctrina internacional que acaeció luego de que se adoptara el acuerdo conocido como *Safe Harbour*[17], y también porque Argentina, dada la regulación que emana del artículo 12 de la ley 25.326, deberá evaluar eneludiblemente cuál es su posición frente a otros países, nos referiremos a sus características generales. ¿En qué consiste el *Safe Harbour*? Como ya mencionamos, no se trata de una Decisión de adecuación respecto de todo el sistema regulatorio y auto-regulatorio de Estados Unidos en general.

La UE presenta un régimen regulatorio general en cuanto a la protección de datos personales mientras que en EEUU el planteamiento es sectorial[18] y tiene como fundamento una mezcla de legislación, reglamentación y autoregulación.[19]

Todo ese sistema complejo, federal y estatal, con leyes para diversos sectores, presentaba lagunas en cuanto a los principios que deben considerarse para declarar que todo el sistema de un país presenta un nivel adecuado. Es por eso, que la UE y EEUU negociaron durante mas de dos años el contenido del acuerdo.

Por lo tanto, lo que se declara en la Decisión que comentamos es que el nivel adecuado de protección en una transferencia desde la UE a EEUU se alcanza si las entidades cumplen con

---

-Grupo de Trabajo sobre Protección de Datos del Artículo 29, Opinion 4/2003 on the Level of Protection ensured in the US for the Transfer of Passengers' Data, Adopted on 13 June 2003, 11070/03/EN, WP 78, disponible en: http://www.europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2003/wp78_en.pdf
- Annex: Undertakings of the United States Bureau of Customs and Border Protection and the United States Transportation Security Administration, disponible en: http://www.europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2003/wp78-pnrf-annex_en.pdf

[17] Decisión 2000/520/CE de la Comisión, de 26 de julio de 2000, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección conferida por los principios de Puerto Seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de Estados Unidos de América.

[18] Algunos ejemplos de leyes sectoriales a nivel Federal: Fair Credit Reporting Act (1970), Fair Credit Billing Act (1974), Equal Credit Opportunity Act (1974), Right to Finantial Privacy Act (1978), Video Privacy Act (1988), Electronic Communications Privacy Act (1986), Cable Communications Policy Act (1984), Telephone Consumer Protection Act(1991), Gramm-Leach-Bliley Act (1998), Children's Online Privacy Protection Act (1998). Ver: Paul M. SCHWARTZ y Joel R. REIDENBERG, "Data Privacy Law. A Study of United States Data Protection", *Michie Law Publishers*, Virginia, 1996.

[19] Joel REIDENBERG y Paul SCWARTZ, "Study of American Personal Data Protection Law" bajo la dirección del Prof. Dr. Spiros SIMITIS, Research Centre for Data Protection, Johann Wolfgang Goethe-Universität, Frankfurt am Main, Alemania, 1994. Lawrence F. STREET, Mark P. GRANT "Law of the Internet", *Lexis Law Publishing*, 1999, p. 109-267. Andrew CHARLESWORTH, "Data Privacy in Cyberspace: Not National v. International but Commercial v. Individual", *Law and the Internet: A Framework for Electronic Commerce* (2nd ed.), eds. Edwards L. and Waelde, Hart Publishing, 2000, pp. 79-122. Daniel J. SOLOVE "Conceptualizing Privacy", *California L. Rev.*, Vol. 90:1087, 2002. Paul M. SCHWARTZ "Internet Privacy and the State", *Connecticut L. Rev.*, Vol 32:815, 2000. Jan DHONT y María Verónica PEREZ ASINARI "New Physics and the Law…", *op. cit.*

los principios de Puerto Seguro (*Safe Harbour*) para la protección de la vida privada y las preguntas más frecuentes (FAQs) en las que se proporciona orientación para aplicar los principios. Además, las entidades deben dar a conocer públicamente sus políticas de protección de datos personales y someterse a la jurisdicción de la *Federal Trade Commission*. Esta adhesión es voluntaria, no obsante, una vez que la entidad ha notificado al Departamento de Comercio su adhesión, el cumplimiento es obligatorio. A su vez, el Departamento de Comercio de EEUU deberá hacer pública una lista de las entidades o empresas que le hayan notificado su adhesión al *Safe Harbour*, para que puedan ser reconocidas por los interesados. Esta lista se encuentra disponible en el sitio Web del Departamento de Comercio de EEUU.[20]

Entonces, quien desee realizar una transferencia de datos personales desde la UE a EEUU, que no se encuentre amparada por las excepciones antes mencionadas, deberá analizar si la entidad receptora figura en la lista de adherentes al *Safe Harbour*.

No obstante, no todos los sectores se encuentran incluidos, ya que para poder adherir al *Safe Harbour* la entidad debe estar sujeta a la jurisdicción de la *Federal Trade Commission* o del Departamento de Transporte de EEUU.

La *Federal Trade Commission*, por ejemplo, carece de jurisdicción en el sector de bancos, cooperativas de ahorro y crédito, compañías de servicio público de telecomunicaciones, etc.

Para estos ámbitos se deberá recurrir a otra solución para poder efectuar una transferencia, como, por ejemplo, la utilización de las claúsulas tipo elaboradas por la Comisión Europea, o redactar clausulas específicas.

La Decisión contiene 7 anexos. Consta de un casuismo notorio, propio del *common law*, y producto, en este caso particular, de unas negociaciones que fueron muy controvertidas, y cuyo resultado sigue siendo cuestionado tanto a nivel político como jurídico.[21]

El anexo 1 está compuesto por los principios de Puerto Seguro relativos a la: notificación, opción, transferencia ulterior, seguridad, integridad de datos, acceso y aplicación.

El anexo 2 son las preguntas mas frecuentes (FAQs), que tienen por objeto aclarar algunos aspectos específicos u oscuros de los principios, como los relativos a los datos sensibles, las excepciones al periodismo, la responsabilidad subsidiaria de los proveedores de servicios de Internet, etc.

Los restantes anexos son aclaratorios o explicativos de determinados aspectos del régimen estadounidense, los cuales presentaban mayores preocupaciones en EEUU o cierta oscuridad, como el sistema de aplicación, la reparacion de daños y perjuicios, etc.

---

[20] Ver: *Safe Harbour List*, disponible en: http://web.ita.doc.gov/safeharbor/SHList.nsf/WebPages/Safe+Harbor+List , última visita 19/03/03

[21] Yves POULLET "The 'Safe Harbour Principles' : An Adequate Protection ?", *International Colloquium organised by IFCLA*, Paris, 15 y 16 de junio, 2000, disponible en el sitio Web del CRID: http://www.droit.fundp.ac.be/crid.htm. Joel REIDENBERG "E-commerce and Trans-Atlantic Privacy", 38 Houston L. Rev. 717, 2001, disponible en: http://reidenberg.home.sprynet.com/Transatlantic_Privacy.pdf.

2.4. Claúsulas contractuales

Hay otro modo alterntivo de hacer una transferencia segura basada en la auto-regulación. Tal es el caso de las clausulas contractuales.[22] El Artículo 26.2 de la Directiva prescribe que los estados miembros podrán autorizar una transferencia de datos personales cuando el responsable del tratamiento ofrezca garantías suficientes respecto de la protección de la vida privada, y que dichas garantías podrán derivarse en particular de clausulas contractuales apropiadas.

Incluso, la Comisión Europea puede elaborar "clausulas contractuales tipo" que deberán ser aceptadas por los estados miembros. La Comisión ha adoptado dos decisiones relativas a este respecto para la transferencia de datos personales a un tercer país, una aplicable a transferencias entre responsables del tratamiento de datos,[23] y la otra entre responsable y encargado.[24]

3) La situación legislativa de los países miembros del Mercosur en materia de protección de datos personales

[22] Podemos considerar, a modo de ejemplo, la experiencia alemana en el caso de las tarjetas de tren. En 1994, la empresa alemana de trenes decidió cooperar con la subsidiaria alemana del Citibank. Las tarjetas de viaje (abonos) comenzaron a emitirse a su vez como tarjetas de crédito Visa, sin costos adicionales para el consumidor. El agregado de la tarjeta de crédito no podía ser rechazado por los consumidores. Se consideró así que la empresa monopolística de trenes había vendido los datos de los abonos de tren al banco con sede principal en EEUU, el cual, muy probablemente, usaría esos datos para marketing directo no solo de su propio negocio. La autoridad de protección de datos alemana criticó numerosos puntos del formulario emitido por la empresa de trenes y el Citibank, especialmente el referido a la colecta de datos sobre capacidad financiera respecto de gente que solo quería viajar en tren. Las fuertes protestas públicas de grupos de defensa del consumidor y de la autoridad de protección de datos personales hicieron que se renegociara el Acuerdo de modo que la tarjeta de crédito fuera una opción y no una obligación para los usuarios del tren. En 1995, habiéndose dictado ya la Directiva 95/46/CE, la autoridad alemana señaló además que la tercerización del procesamiento de los datos personales implicados en esta transacción resultaba en un masivo flujo de datos personales a un país no miembro de la UE, por lo cual, los artículos 25 y 26 de la Directiva resultaban de aplicación. La solución encontrada fue la realización de claúsulas contractuales para lograr el nivel de adecuación en el tratamiento de los datos que se exportaban, en donde se señaló claramente quién era el responsable de tratamiento de los datos, se delimitó la responsabilidad civil al respecto, la ley aplicable (alemana), la finalidad del procesamiento, medidas de seguridad, auditoría, etc. Para una descripción completa del caso ver : "Case Study : North America and the European Directive. The German RailwayCard. A model contractual solution of the 'adequate level of protection' issue?", *Daten Schutz Berlin*, disponible en: http://www.datenschutz-berlin.de/sonstige/konferen/ottawa/ale3.htm , última visita 20/08/01.

[23] Decisión 2001/497/CE de la Comisión de 15 de junio de 2001 relativa a cláusulas contractuales tipo para la transferencia de datos personales a un tercer país previstas en la Directiva 95/46/CE.

[24] Decisión 2002/16/CE de la Comisión de 27 de diciembre de 2001 relativa a cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países, de conformidad con la Directiva 95/46/CE

El Mercosur, como bloque de integración económica internacional, no posee aún regulación específica sobre protección de datos personales. Es por ello que deberemos remitirnos, en esta aproximación, a los ordenamientos internos exclusivamente. Varios países latinoamericanos han regulado en sus Constituciones nacionales y legislación derivada la protección de datos personales a través de un instituto denominado *Habeas Data*. Tal es el caso de Argentina, Brasil y Paraguay, no así de Uruguay.

A su vez, es dable señalar que los cuatro países han firmado y ratificado la Convención Americana de Derechos Humanos, Pacto de San José de Costa Rica, la cual en su artículo 11 regula la protección de la vida privada[25] (no ha habido aun juripudencia de la Corte Americana de Derechos Humanos en la materia). A continuación nos referiremos brevemente al estado legislativo de los países miembros del Mercosur.[26]

3.1. Argentina

Nuestro país regula la protección de datos personales en diversas normas generales, a saber: el artículo 43.3 de la Constitución Nacional, la ley nº 25.326, el decreto nº 1558/2001. El Dictamen 4/2002 del Grupo de Trabajo del Artículo 29 hace un estudio sobre estas normas siguiendo la metodología descripta en el Documento de Trabajo nº 12 (ver *supra*).

El método de Derecho Comparado utilizado hace que se tenga en cuenta, a su vez, la jurisprudencia para clarificar determinados puntos, tal es el caso del ámbito de aplicación. Este punto resultaba dudoso para el Grupo de Trabajo del Artículo 29 en lo que hace al ámbito de aplicación material. El razonamiento seguido ha sido el siguiente:

"En cuanto a los archivos de datos privados, el Grupo de Trabajo observa que tanto el tercer párrafo del artículo 43 de la Constitución como el artículo 1 de la Ley se refieren a 'archivos, registros, bancos de datos u otros medios técnicos privados, destinados a dar informes'. La misma redacción aparece en otras disposiciones de la citada Ley, como los artículos 14 (derecho de acceso), 21 (obligación de inscribirse en el Registro), 29 (atribuciones del órgano de control), 33 y 35 (requisitos del recurso judicial *habeas data*) y 46 (disposiciones transitorias). No obstante, la interpretación amplia [antes indicada][27] se desprende de varios argumentos expuestos por las autoridades argentinas:

---

[25] Ver: Lee BYGRAVE "Data Protection Pursuant to the Right to Privacy in Human Rights Treaties", *International Journal of Law and Information Technology*, vol. 6 no. 3.

[26] Ver: Andres GUADAMUZ, "Habeas Data: The Latin-American Response to Data Protection", *The Journal of Information, Law and Technology*, 2000, disponible en: http://elj.warwick.ac.uk/jilt/00-2/guadamuz.html , última visita 28/04/03. Roberto CHACON de ALBUQUERQUE y Pablo PALAZZI "Habeas Data y protección de datos personales en el Mercosur", *Revista de Derecho Privado y Comunitario*, Rubinzal-Culzoni, Buenos Aires, 2001/2, p. 607-641. Ver a su vez en el sitio Web *Ulpiano* : Pablo PALAZZI "Protección de Datos Personales, Privacidad y Habeas Data en América Latina. Recopilación de Doctrina, Legislación y Jurisprudencia", disponoible en : http://www.ulpiano.com/Recursos_Privacy_LatinAmerica.htm , última visita 28/04/03.

[27] Ver el Dictamen 4/2002 a efectos de observar el contenido de la interpretación amplia dada al ámbito de aplicación material. Nota agregada por nosotros.

- El artículo 1 del Reglamento proporciona una interpretación jurídica de la Ley. En particular, define jurídicamente el concepto de 'archivos, registros, bases o bancos de datos privados destinados a dar informes' como 'aquellos que exceden el uso exclusivamente personal y los que tienen como finalidad la cesión o transferencia de datos personales, independientemente de que la circulación del informe o la información producida sea a título oneroso o gratuito'.

- El artículo 24 de la Ley dispone que 'los particulares que formen archivos, registros o bancos de datos que no sean para un uso exclusivamente personal deberán registrarse conforme lo previsto en el artículo 21'. El artículo 21 de la Ley obliga a inscribir en el Registro las bases de datos privadas *destinadas a proporcionar informes*. El artículo 24 no tendría sentido si la Ley sólo se aplicara a las bases de datos destinadas a proporcionar informes. Estos dos artículos confirman el paralelismo de las expresiones 'bases de datos *destinadas a proporcionar informes*' y 'bases de datos *[...] que no sean para un uso exclusivamente personal*', como establece la definición jurídica del artículo 1 del Reglamento (…).

- Por otra parte, cabe mencionar que tanto la Ley como el Reglamento contienen normas sobre tratamiento de datos relativos a la salud (artículo 8 de la Ley) o publicidad directa (artículos 27 de la Ley y el Reglamento), según las cuales dichas bases de datos, aunque exceden el uso exclusivamente personal, no pueden estar destinadas a proporcionar informes. Una vez más, estas normas serían superfluas si la Ley sólo fuera aplicable a las bases de datos destinadas a proporcionar informes."[28]

Por último, el Dictamen hace referencia a dos casos de jurisprudencia invocados por las autoridades argentinas, en los cuales los tribunales han seguido la interpretación amplia mencionada anteriormente.[29]

La conclusión del Dictamen fue favorable en lo concerniente a la adecuación del régimen jurídico de la República Argentina de protección de datos personales respecto del de la UE. *A posteriori* del Dictamen no vinculante del Grupo de Trabajo del Artículo 29 se debió recabar un Dictamen del Comité del Artículo 31. Luego comenzó a correr un plazo de 30 días para el Parlamento Europeo con el objeto de que pueda chequear si la Comisión había utilizado correctamente sus poderes ejecutivos. El Parlamento puede elaborar una recomendación al respecto[30]. Transcurrido este plazo la Decisión de Adecuación sería adoptada por el Colegio de Comisarios.

Efectivamente, tal ha sido el proceso seguido para la adopción de la Decisión de Adecuación respecto de nuestro país. Resulta relevante hacer énfasis en lo señalado en el Considerando 15 de dicho documento: "El Gobierno argentino ha facilitado información y garantías sobre la manera en que debe interpretarse la legislación argentina, y ha garantizado que las normas

[28] Dictamen 4/2002, ver *supra*.

[29] Cámara Civil de Apelación, Mantovano c/ Banco Regional de Cuyo, 2000; Becker José c/ Banco de la Provincia de Buenos Aires, 2002

[30] Tal ha sido el caso respecto del Safe Harbour. Ver: *Report on the Draft Commission Decision on the adequacy of the protection provided by the Safe Harbour Privacy Principles* (C5-0280/2000 – 2000/2144(COS)), Committee on Citizens' Freedoms and Rights, Justice and Home Affairs, Rapporteur: Elena Ornella Paciotti. Disponible en:
http://www.europa.eu.int/comm/internal_market/privacy/docs/adequacy/0117-02_en.pdf

argentinas en materia de protección de datos se aplican de conformidad con dicha interpretación. La presente Decisión se basa en las citadas informaciones y garantías y está subordinada a ellas, y, en particular, a las explicaciones y garantías proporcionadas por las autoridades argentinas sobre la manera en que debe interpretarse la legislación argentina en lo que se refiere a qué situaciones se hallan dentro del ámbito de aplicación de la legislación argentina de protección de datos".

Esta referencia subraya la responsabilidad en la aplicación de la legislación que tratamos por la autoridad de aplicación, la Dirección Nacional de Protección de Datos Personales, y los jueces del modo en que ha sido descripta a las autoridades europeas. A su vez, una tarea pedagógica deberá ser diseñada con el objeto de divulgar y dar a conocer a los ciudadanos, empresas y organismos públicos cuáles son los derechos y obligaciones que emanan de la regulación nacional.

En la parte dispositiva de la Decisión, en el Artículo 4, se establece que "1. La presente Decisión podrá adaptarse en cualquier momento de conformidad con la experiencia de su funcionamiento o los cambios de la legislación argentina, su aplicación o su interpretación". Con lo cual, se debe tener presente que la Decisión es susceptible de modificarse, y en caso extremo revocarse, si los derechos garantizados no se respetan.

Como ya hemos señalado anteriormente: "La importancia política de poder participar en el diálogo internacional como un país donde se garantizan los derechos fundamentales trasciende la materia específica que tratamos e implica la voluntad de construir un modelo de desarrollo sustentable para la Sociedad de la Información, siendo la protección de datos personales una expresión de ese concepto"[31].

3.2. Brasil

La Constitución brasileña de1988 regula el *Habeas Data* en el artículo 5, del siguiente modo:

"LXXII. Se concederá 'habeas data': a) para asegurar el conocimiento de informaciones relativas a la persona del impetrante que consten en registros o bancos de datos de entidades gubernamentales o de carácter público;

b) para la rectificación de datos, cuando no se prefiera hacerlo por procedimiento secreto, judicial o administrativo;"[32]

La ley nº 9507/97 de 12 de noviembre regula el derecho de acceso y la rectificación de los datos personales y establece el procedimiento para el ejercicio de la acción de *Habeas Data*. Esta ley no regula ciertos principios como es el caso de restricciones en transferencias ulteriores, limitación de la finalidad, transparencia, etc. No obstante, debemos considerar que

[31] María Verónica PEREZ ASINARI "Notas sobre la Conferencia de protección de datos personales organizada por la Comisión Europea", *La Ley Actualidad*, 18-03-2003, p. 3.

[32] Esta norma se ve complementada por otras contenidas en el mismo artículo 5 de la Constitución brasileña (VIII, X, XII, XXXII, XXXIII, XXXIV, LX, LXIX, LXXIV, LXXVII).

existe legislación sectorial específica que puede complementar la ley de mención. Ese es el caso, por ejemplo, de la ley nº 7232/1984 sobre Tecnología de la Información, cuyo artículo 2, VIII, contempla el principio de seguridad.

3.3. Paraguay

En la Constitución Nacional del Paraguay se reglamenta el *Habeas Data* de la siguiente manera: Artículo 135 *Habeas Data* : "Toda persona puede acceder a la información y a los datos que sobre sí misma o sobre sus bienes obren en registros oficiales o privados de carácter público, así como conocer el uso que se haga de los mismos y de su finalidad. Podrá solicitar ante el magistrado competente la actualización, la rectificación o la destrucción de aquellos si fuesen erróneos o afectaran ilegítimamente sus derechos."[33]

El Congreso paraguayo dictó la ley nº 1682 que reglamenta la información de carácter privado. En esta norma se legisla sobre aspectos tales como la calidad de los datos, derechos de acceso y rectificación, sanciones por violaciones a las reglas establecidas en la misma, prohibición de dar publicidad y divulgar datos sensibles, etc. Dicha ley carece, no obstante, de regulación en lo que hace al principio de limitación de la finalidad, seguridad, restricciones en transferencias ulteriores, etc.

3.4. Uruguay

Tal como señalamos en párrafos anteriores, Uruguay carece de regulación del instituto del *Habeas Data* en su Constitución nacional. No obstante, podrían resultar de aplicación otras normas generales contenidas en ella. Así, el artículo 7 de la Constitución provee: "Los habitantes de la República tienen derecho a ser protegidos en el goce de su vida, honor, libertad, seguridad, trabajo y propiedad. Nadie puede ser privado de estos derechos sino conforme a las leyes que se establecieron por razones de interés general", el cual debe ser interpretado conjuntamente con el artículo 72 : "La enumeración de derechos, deberes y garantías hecha por la Constitución, no excluye los otros que son inherentes a la personalidad humana o se derivan de la forma republicana de gobierno".

4) Valoración

La ley argentina contiene una regulación que estatuye la prohibición de flujos transfronterizos de datos personales desde Argentina hacia países que no otorguen un nivel de protección a los datos personales considerado "adecuado" *vis-à-vis* la legislación argentina (artículo 12, ley 25.326). Esta regla fue uno de los puntos considerados en el Dictamen 4/2002 del Grupo de

[33] Esta norma se ve complementada por otras contenidas en los artículos 28, 33, 34, 35 y 36 de la Constitución paraguaya.

Trabajo del Artículo 29, siguiendo la metodología delineada en el Documento de Trabajo nº 12, para evaluar el nivel de adecuación del régimen argentino de cara al de la Unión Europea.

Entonces, podemos considerar que las transferencias de datos personales dentro del Mercosur, con origen en Argentina, serían, en principio, restringidas por la ley de mención. A su vez, esa regla se vería reforzada por las implicaciones internacionales derivadas de la Decisión de Adecuación, respecto de los datos de origen europeo.

De la breve referencia efectuada sobre el marco legal de los restantes países del Mercosur podemos inferir la existencia de disparidades que podrían llevar a considerarlo como no adecuado al régimen argentino o al de la UE. No obstante, debemos puntualizar que sólo hemos hecho referencia a fuentes legislativas, no habiendo considerado otras fuentes que "deben" complementar todo análisis de adecuación (conf. art. 12, 4to y 5to párrafo, Decreto Nº 1558/2001 – Argentina-; y art. 25.2 de la Directiva 95/46/CE).

El Mercosur debe prevenir abusos respecto de los datos personales de sus ciudadanos, tal como el ocurrido en la venta de bases de datos de nacionales latinoamericanos a la empresa estadounidense ChoicePoint, para la posterior venta por parte de esta a las autoridades de EEUU, sin el consentimiento ni conocimiento de los titulares de los datos.[34]

Por otra parte, resulta claro que el hecho de alcanzar el estadio de Mercado Común, tal como es descripto en el artículo 1 del Tratado de Asunción, se vería facilitado, entre otros factores evidentemente, si se lograra una armonización en materia de protección de datos personales, de modo que éstos pudieran circular libremente entre las empresas y organismos públicos de los países socios, dentro del marco legal diseñado.

Esta situación sería a su vez positiva para intercambios de datos personales con la UE; más aún, estaría en línea con lo dispuesto en el Acuerdo de Cooperación Interregional entre las Comunidades Europeas y el Mercosur, firmado en Madrid el 15 de diciembre de 1995.

Finalmente, y como una consecuencia de lo expresado anteriormente, una posición común del Mercosur en esta materia debería ser reforzada con el objeto, entre otros, de favorecer el respeto por la conceptualización dada al *Habeas Data* -y la protección otorgada en los países

---

[34] Ver: ChoicePoint, International Searches, disponible en el sitio Web de EPIC : http://www.epic.org/privacy/publicrecords/inschoicepoint.pdf , última visita 30/04/03. En este documento se describen los datos que procesa y vende ChoicePoint y los países de los cuales provienen esos datos y de cuyos ciudadanos se trata. Por ejemplo : lista completa de ciudadanos mexicanos, colombianos y argentinos ; números de teléfono no registrados en las listas públicas en Mexico, Brasil y Argentina ; datos sobre las licencias de conducir mexicanas ; lista completa de empresas colombianas ; información personal de gente de negocios de Brasil, etc. Ver : Orden de prestación de servicios emitida por el Departamento de Justicia de EEUU en favor de ChoicePoint, Inc., disponible en : http://www.epic.org/privacy/publicrecords/citizenprices.pdf . En este documento constan los precios de los servicios de búsqueda y provisión de bases de datos personales clasificados por países y tipo de dato (los países latinoamericanos de los cuales se ofrecen datos de ciudadanos y empresas son : Argentina, Brasil, Colombia, Costa Rica, Mexico, Honduras, Nicaragua, Guatemala y Venezuela). Ver también la amplia cobertura de la prensa extranjera: The Atlanta Journal-Constitution "Mexico claims ChoicePoint stepped across the line", 27-04-03, disponible en: http://www.ajc.com/business/content/business/0403/27privacy.html , última visita 30/04/03. MNSBC News "US buys data on foreign citizens", 13-04-03, disponible en: http://www.msnbc.com/news/899805.asp?cp1=1 , última visita 30/04/03. O Estado de S. Paulo "Tabela de preços para cidadãos latinos", 30-04-03, disponible en : http://www.estado.estadao.com.br/colunistas/robson.html , última visita 30/04/03. Terra, "Exigen investigar venta de datos", 15-04-03, disponible en: http://www.terra.com.mx/noticias/articulo/113119/ , última visita 30/04/03.

miembros del Mercosur a los datos personales- en la conducción de las negociaciones para el ALCA en temas que presenten implicancias en lo atinente a la protección de datos personales.[35] Se debe tener en cuenta que en la materia existen concepciones claramente diversas entre los futuros miembros, como por ejemplo el caso de EEUU -que en el ámbito del comercio electrónico privilegia la autorregulación sobre la legislación-, respecto de los miembros del Mercosur -quienes privilegian la via legislativa general-. Es preciso conocer en profundidad las diferencias regulatorias y sus consecuencias respecto de las garantías que tratamos, para evitar que la protección otorgada por la legislación de los países miembros se vea debilitada por alguna normativa en el ámbito del ALCA.

5) A modo de colofón

Sin lugar a dudas la Decisión de Adecuación respecto de la República Argentina reviste una significativa importancia. De ahora en más existe libre circulación de datos personales entre la Unión Europea y la República Argentina, lo cual facilita el procesamiento de datos en uno y otro lugar que se deba hacer como consecuencia de transferencias internacionales de datos personales que obedezcan al comercio electrónico, el gerenciamiento de datos de recursos humanos, el procesamiento de datos a fines de investigación científica, etc., garantizando un alto nivel de protección para los titulares de los datos. Ello implicará, claro está, la responsabilidad en el cumplimiento de la legislación nacional *ad intra* y *ad extra*, de modo que las garantías que se otorgaron en las discusiones a nivel diplomático sean ejercitadas en la práctica tanto por la Dirección Nacional de Protección de Datos Personales de la República Argentina, como por los jueces, en salvaguarda de los derechos de los titulares de los datos.

En el caso de proceder a armonizar la legislación en el ámbito del Mercosur, lo cual resultaría un valor agregado clave a nivel regional, se debería apuntar a estándares altos para proteger los derechos de los individuos debidamente y, como consecuencia, poder encaminarse hacia la libre circulación de datos personales de bloque a bloque, es decir, Mercosur-Unión Europea, lo cual facilitaría, por ejemplo, la confianza para el desarrollo de negocios en el sector la Sociedad de la Información de un modo sustentable.

[35] Ver: Comité Conjunto de Expertos del Gobierno y del Sector Privado sobre Comercio Electrónico – ALCA, Nota de la Presidencia, "Temas sobre el Usuario: establecimiento de la confianza del Mercado en la seguridad del comercio electrónico, la codificación, autenticación y las firmas digitales", 25 de mayo de 1999. Comité Conjunto de Expertos del Gobierno y del Sector Privado sobre Comercio Electrónico – ALCA, Nota de la Presidencia, "Protección de la privacidad en el comercio electrónico", 16 de junio de 1999.