LATINOAMÉRICA ANTE LA TENDENCIA EUROPEA Y NORTEAMERICANA EN LA REGULACIÓN DEL FLUJO TRANFRONTERIZO DE DATOS PERSONALES

Abstract. La tecnología de la información ha representado un avance innegable para la humanidad, sin embargo, el uso desproporcionado de la misma puede afectar o vulnerar la esfera mínima de privacidad del individuo sobretodo en lo referente al manejo de su información personal. El objetivo del presente será analizar los diferentes modelos normativos que existen para la regulación de la protección de datos personales que a veces resultan opuestas e incluso contradictorias y con qué mecanismos se puede, en determinado momento, superar una ausencia de disposiciones normativas en la materia.

1. INTRODUCCIÓN

Ante el avance en el uso de las tecnologías de la información y las comunicaciones, han constituido una herramienta de incalculable valor, acercando a regiones más remota, posibilitando la comunicación en fracciones de segundo, permitiendo que cada persona, tal solo con el uso de una computadora y una conexión a Internet pueda realizar operaciones que hasta hace algunos años se consideraban imposibles.

Sin embargo, el uso desproporcionado o inadecuado de este tiempo de tecnologías puede tener consecuencias que afecten sobretodo a los derechos fundamentales del ser humano, entre ellos podemos mencionar la garantía de una esfera mínima de privacidad o intimidad del individuo.

A pesar de que la privacidad puede considerarse como un derecho que abarca varias categrorías (como por ejemplo privacidad en las comunicaciones, el el domicilio, en las posesiones, etc.), el tema principal del presente es el desarrollo normativo que ha tenido un ámbito específico de la privacidad en lo que se refiere al tratamiento de la información personal contenida en bases de datos; este derecho ha tenido diferentes denominaciones: “derecho a la intimidad informática”,[i] “derecho a la protección de datos personales”,[ii] “derecho a la autodeterminación informativa,”[iii] “derecho a la libertad informática”[iv].

La protección de datos personales como derecho de reciente configuración, tiene como finalidad “garantizar la facultad de las personas de conocer y acceder a las informaciones que les conciernen archivadas en bancos de datos; controlar su calidad, lo que implica la posibilidad de corregir o cancelar los datos inexactos o indebidamente procesados, y disponer sobre su transmisión”,[v] con este derecho, “el individuo tutela su propia identidad informática, concretándose en las garantías de acceso y control de las informaciones procesadas en bancos de datos por parte de las personas a las que conciernen”.[vi]

2. REGULACIÓN DEL FLUJO TRANSFRONTERIZO DE DATOS PERSONALES EN EUROPA

La protección de datos personales en la Unión Europea forma parte del programa llamado “Sociedad de la Información”, cuyo fin es que las empresas, gobiernos y ciudadanos de la Unión Europea sigan desempeñando un papel destacado en el desarrollo de una economía mundial del conocimiento y la formación, además de que participen activamente en ella. Los lineamientos que impulsan activamente el desarrollo de esta llamada “Sociedad de la Información” en Europa los encontramos en el Tratado Constitutivo de la Comunidad Europea, (en lo sucesivo citado como TCE)[vii] por medio del impulso a una política de telecomunicaciones,[viii] el apoyo al desarrollo en materia de tecnologías de la información y las comunicaciones,[ix] debiendo estimular la creación de condiciones necesarias para favorecer la competitividad de las empresas comunitarias[x] y el fomento de las redes transeuropeas de transporte, energía y telecomunicaciones,[xi] pero sobretodo la protección de los derechos fundamentales, entre los cuales se encuentra el derecho a la protección de datos personales y que va de la mano con el derecho a la intimidad. “La protección de los datos personales juega un papel crucial, para elevar la confianza y seguridad en cuanto a su transmisión, almacenamiento y control dentro de la Unión”.[xii]

Otros países fuera del continente europeo están adoptando un conjunto de legislación relativo a la privacidad, de acuerdo con David Banisar y Simon Davis, por una o varias de las siguientes razones: para remediar las injusticias del pasado, para promover el comercio electrónico y para asegurar que estas leyes sean coincidentes con la legislación europea, para pertenecer en un futuro a esta Unión o para asegurarse de que su intercambio comercial no se verá afectado por los requerimientos de las Directivas comunitarias, como es el caso de Canadá.[xiii]

En Europa, el derecho a la intimidad se concibe desde el rol tradicional que ha desempeñado el Consejo de Europa, que en su Convención Europea en 1950 estableció firmemente el derecho a la intimidad como un derecho humano reclamado por la Europa de la posguerra. El artículo 8 del Convenio Europeo para la Protección de los Derechos Humanos y las Libertades Fundamentales (CEDH), celebrado en Roma el 4 de noviembre de 1950,[xiv] estableció textualmente que “1. Toda persona tiene el derecho al respeto a su vida privada y familiar, de su domicilio y de su correspondencia. 2. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho, sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y libertades de los demás”.

Es conveniente puntualizar la importancia de las medidas supranacionales que ha tomado la Unión Europea (en adelante UE)[xv] con el fin de armonizar los derechos fundamentales (antes por supuesto, de la propuesta de esta nueva Constitución Europea). Para cumplir este objetivo, la UE se vale de Reglamentos y Directivas, que son actos jurídicos de carácter obligatorio para sus Estados Miembros. El Reglamento puede describirse como la Ley comunitaria, pues su alcance es general y obligatorio en todos sus elementos y

directamente aplicable en cada Estado miembro.[xvi] La Directiva, por su parte, obliga al Estado miembro en cuanto al resultado que deba conseguirse, otorgando sin embargo a las autoridades nacionales la elección sobre la forma y los medios por los cuales se incorpore ésta a su sistema jurídico.[xvii]

El principal ordenamiento relativo a la protección de datos personales es las Directiva 95/46/CE, de 24 de octubre, 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, diseñada para armonizar las políticas públicas de dicha comunidad, mediante la expresión de un conjunto de acuerdos de metas,[xviii] además de que ha tenido un profundo efecto en le desarrollo del derecho a la privacidad, no solo en Europa, sino en todo el mundo.[xix]

Como el flujo transfronterizo o movimiento internacional de datos personales se trata de un problema global, es decir, no se produce exclusivamente en un cierto sector o país, este ordenamiento comunitario ha establecido que la transferencia de datos personales a países ajenos a su marco regulatorio (es decir, fuera de los integrantes de la Unión) únicamente se puede efectuar únicamente si el país destinatario garantiza un nivel de protección "adecuado"[xx]. Pero ¿qué debemos de entender por "nivel adecuado de protección?, ¿quién lo califica?, ¿cómo saber si un país cumple con ciertos requisitos para poder realizar transferencias internacionales de datos?.

Para dar respuesta a las interrogantes planteadas el mismo artículo 25 de la citada directiva nos proporciona algunos parámetros para evaluar la situación de un determinado país. Se debe de realizar un análisis atendiendo a todas las circunstancias que rodean una transmisión de datos, considerando especialmente la naturaleza de los datos, la finalidad y duración del tratamiento, las leyes generales y sectoriales, y por supuesto, las medidas de seguridad que disponga un país de destino.

Por medio de la citada directiva se crea también el "Grupo de Protección de Datos" [xxi] el cual tiene un carácter consultivo e interdependiente, compuesto por un representante de la autoridad de control de cada Estado miembro, un representante de la autoridad comunitaria, y por un representante de la Comisión, la relevancia de este grupo radica en la emisión de un dictamen del nivel de protección existente dentro de la comunidad y los países terceros. La Directiva crea también un Comité[xxii] compuesto por un representante de los Estados miembros, presidido por un representante de la Comisión, este organismo emite un dictamen sobre las medidas que se hayan de adoptar en las transmisiones de datos internacionales.

Como podemos observar, los términos de este ordenamiento comunitario resultan bastante ambiguos e imprecisos, pues se tiene que valorar cada situación en lo particular, siguiendo a Heredero Higueras "el concepto de `nivel de protección adecuado´ se configura como una norma en blanco, que deberá de `rellenar´ la Comisión".[xxiii] Los Estados podrán utilizar los lineamientos señalados por esta Directiva, precisando de manera interna las condiciones de licitud en el tratamiento de sus datos a través de disposiciones legales que marquen específicamente las medidas de seguridad, los medios

para asegurar la eficacia de las normas y el establecimiento de principios básico relativos al tratamiento de esta información, como la limitación de objetivos, proporcionalidad, calidad de datos, transparencia y seguridad, además de incluir los derechos de acceso, rectificación y oposición del interesado. El tercer país, al igual que la UE, deberá garantizar que no podrán hacerse transferencias de datos personales a países que no cuenten con un nivel de protección adecuado. Adicionalmente se exige el consentimiento explícito para el tratamiento de datos sensibles, y en el caso de decisiones individuales automatizadas e interesado tendrá derecho a saber la lógica aplicada a dicha decisión.

Por otra parte, las excepciones que marca la Directiva respecto al tratamiento de datos son la seguridad del Estado, la defensa, la seguridad pública, la prevención, investigación, detección y represión de infracciones penales o infracciones de la deontología de las profesiones reglamentadas, el interés económico y financiero importante de un Estado miembro, una función de control, inspección o reglamentaria relacionada, y finalmente, la protección del interesado, o de los derechos y libertades de otras personas[xxiv].

A pesar de que la solución contractual no es la forma más idónea para proteger las trasferencias internacionales de datos, si son una herramienta bastante eficaz para poder regular de alguna manera este tipo de operaciones, a través de los llamados contratos tipo, sobretodo en los países que a juicio de la Comisión no tiene este nivel de protección adecuado de sus datos.

La Comisión de las Comunidades Europeas ha adoptado dos decisiones relativas a las cláusulas contractuales tipo para la transferencia de datos personales a un tercer país[xxv]. La primera es la 2001/497/CE, la cual se refiere a transferencias de datos realizadas entre responsables del tratamiento establecidas entre un Estado miembro de la UE y destinatarios fuera del territorio comunitario que actúen solamente como encargados del tratamiento; por lo tanto, la responsabilidad por incumplimiento y pago de la compensación recaerá de manera solidaria en los dos. El interesado tendrá pues, derecho a emprender acciones y percibir una indemnización del importador de los datos o de ambos en caso de daños y perjuicios resultantes de cualquier acción incompatible con las obligaciones estipuladas en las cláusulas contractuales tipo[xxvi].

El segundo caso la decisión 2002/16/CE, se refiere a las transferencias de datos destinadas a encargados de tratamiento establecidos en un país tercero, el cual actuará conforme a las instrucciones que reciba y las obligaciones impuestas en las cláusulas. En caso de que el particular sufra un daño tendrá derecho a emprender acciones y en su caso, recibir indemnización de parte del exportador de datos que sea responsable del tratamiento, excepto si hubiere desaparecido de facto, cesado de existir o fuere insolvente, en tal caso responderá el importador de datos subsidiariamente.

Ambos documentos contienen cláusulas en común, especialmente mencionaremos la cláusula de tercero beneficiario, por medio de la cual la persona física que ha consentido a que sus datos personales sean tratados,

aun no siendo parte interviniente en la formación del contrato, pueda hacer valer sus derechos en caso de que resultare afectado por el incumplimiento del este contrato. Mediante esta cláusula, en caso de conflicto, el importador de datos aceptará ofrecer al interesado la elección de mediación, arbitraje o procedimiento judicial.

3. REGULACIÓN DEL FLUJO TRANSFRONTERIZO DE DATOS PERSONALES EN ESTADS UNIDOS

No es un secreto que Estados Unidos carece de una ley general que regule específica y omicomprensivamente los datos de carácter personal de sus ciudadanos, más bien posee una serie de disposiciones normativas que regulan ciertas áreas específicas, por lo que se considera que ofrece una protección de carácter sectorial que dista mucho del nivel de protección de la información que requieren la Comisión Europea para considerar a este país con una protección de nivel "adecuado". Pero tampoco es un secreto que en Estados Unidos se priorice el intercambio de información y que el intercambio de bases de datos sea una práctica cotidiana. Pero entonces, ¿cómo solventar esta diferencia de concepciones de protección a la privacidad en la información personal contenida en bases datos?

Con el objeto de no impedir tajantemente los movimientos transfronterizos de datos personales, Europa y Estados Unidos celebraron el acuerdo conocido como *Safe Harbor* o "Acuerdo de Puerto Seguro" para configurar un puente para la búsqueda de soluciones al problema creado en la transmisión internacional de datos personales y la privacidad, puesto que, Estados Unidos a pesar de tener disposiciones sectoriales, no tiene un nivel de protección adecuado, conforme lo establecido en los parámetros señalados en el artículo 25 apartado 2º de la citada Directiva, Además, específicamente en lo que se refiere al sector privado, existe una clara falta de transparencia respecto al uso secundario de datos recabados del público constituyen una práctica común y carente de un eficiente control judicial por parte de los registrados.

La decisión sobre Puerto Seguro tiene varias características particulares: se trata de una decisión sectorial, es decir, declara "adecuado" el nivel de protección a las empresas que aceptan someterse a sus reglas, no a un país entero.[xxvii] Además las empresas que deseen disfrutar de los beneficios que implica la adhesión a los principios de Puerto Seguro deben de cumplir con las siguientes condiciones mínimas: ser una compañía establecida en Estados Unidos, sujeta a la Comisión Federal de Comercio (FTC),o al Departamento de Transportes de los Estados Unidos (únicas entidades reconocidas hasta el momento por la Unión Europea) además de haber manifestado de forma inequívoca y pública su compromiso de cumplir las condiciones establecidas en este *Safe Harbor*.

Los principios de Puerto Seguro son siete: notificación, opción, transferencia ulterior, seguridad, integridad de los datos, acceso y aplicación,[xxviii] mismos que se complementan por las Preguntas más Frecuentes (FACs) que precisan el alcance de éstos y pretenden aclarar algunas dudas respecto a su interpretación[xxix].

Este sistema de Puerto Seguro no está exento de críticas y deficiencias, pero constituye un referente importante en lo que se refiere a las regulación de este tema y al vínculo de cooperación que establece en el movimiento internacional de datos personales entre Europa y Estados Unidos

4. LA TRANSMISIÓN DE DATOS PERSONALES A LATINOAMÉRICA

Los países latinoamericanos han regulado el tema de la protección de datos personales de una manera tardía comparado con los parámetros europeos[xxx]. Aunque por la extensión del presente no es posible detallar las características que cada país latinoamericano emplea en la protección de su información, generalmente se realiza a través de la figura del habeas data, es decir, una garantía que se deriva de los términos: "«*Habeas*» segunda persona del presente subjuntivo de *habeo...habere*, que significa en este supuesto «conserva tu posesión», que es una de las acepciones del verbo, y «*data*» que es el acusativo plural de *datum*, que los más modernos diccionarios brasileños definen como representación convencional de los hechos, conceptos o instrucciones de manera apropiada para la comunicación y procesamiento por medios automáticos, es decir, conservar los registros o los datos[xxxi] .

El *habeas data* es básicamente una herramienta del derecho procesal constitucional que contempla derechos de acceso, rectificación y corrección de datos sobre su persona y sus bienes, incluyéndose en algunos supuestos la posibilidad de supresión de la información. Sin embargo, el *habeas data* no incluye una serie de principios de protección de datos que están presentes en las legislaciones europeas, sino que se limita a reconocer específicamente los derechos arriba mencionados.

Coincidimos con Palazzi en el sentido de que el *habeas data* representa apenas un intento dirigido a corregir distorsiones extremas del proceso comunicativo informático, ya que de un lado reduce la invisibilidad de los gestores o titulares de los bancos de datos porque los hace sujetos de una responsabilidad clara ante el titular de los mismos, y por el otro lado, permite a las personas en cierta medida adquirir conciencia de la transparencia externa e incluso de la importancia que tiene su propia información personal[xxxii]. Sin embargo, no coincidimos con el autor en que representa un intento "incipiente y tímido" puesto que para accionar el *habeas data* se requiere el funcionamiento del aparato jurisdiccional establecido por los países (en su mayoría latinoamericanos); en todo caso, estaríamos hablando de la mejora de las instituciones judiciales y no de que representara una falla en la estructuración del mismo *habeas data*.

A pesar de que algunos países latinoamericanos regulan esta garantía procesal,[xxxiii] Argentina es el único país latinoamericano que tiene el reconocimiento de poseer un "nivel de protección adecuado" de acuerdo a los parámentros establecidos por la Unión Europea, gracias un conjunto una serie de acciones concretas: reformó su Constitución en 1994 para incorporar la figura del *habeas data* como garantía constitucional, el 14 septiembre de 2000, se aprueba la ley de protección de datos personales y posteriormente su ley reglamentaria a través del decreto 1558/01, se crea también un órgano de

control independiente (al estilo de las agencias de protección de datos europeas), implementación los principios de protección de datos, tanto de personas físicas como jurídicas, y establecimiento de mecanismos de control efectivo de los mismos.

5. CONCLUSIONES

El tratamiento de datos personales contenidos en registros principalmente electrónicos es un derecho que se debe de proteger independientemente de la ubicación de su titular. Europa lleva ya un largo camino en su regulación, estableciendo parámetros bien definidos para su debida protección (a través del cumplimiento de las directivas comunitarias, el establecimiento de principios, órganos encargados del control y vigilancia con la modalidad que desee cada país miembro, entro otros recursos).

Estados Unidos, tiene otras prioridades que atienden a incentivar el intercambio comercial de las bases de datos que a proteger la privacidad de la información personal que contengan las mismas. Sin embargo, el establecimiento de las medidas de Puerto Seguro contribuyen a crear un vínculo que une de alguna manera sistemas jurídicos hasta cierto punto contrapuestos.

El reto principal está en la regulación de este derecho en países latinoamericanos, que como en algunos otros aspectos, se va regulando de manera posterior al surgimiento de los problemas jurídicos, hasta ahora con la figura del habeas data que no deja de representar una protección limitada (hay que observar también el funcionamiento y la eficacia de los tribunales de administración de justicia en estos países y el tiempo que puede llevar el llegar a sentencia), eso en países que regulan este derecho, México por ejemplo, solo tenemos disposiciones relativas al manejo de bases de datos públicas[xxxiv], pero hay una importante carencia de regulación específica en bases de datos privadas.

Mientras no existan leyes específicas en la materia, organismos encargados en asegurar el efectivo cumplimiento de las mismas, mecanismos rápidos y expeditos para facilitar el efectivo cumplimiento de esots derechos por parte de los individuos, estaremos hablando solamente de buenas intenciones y no de protección integral a un derecho que es una realidad y que va cobrando importancia día con día con el avance en el uso masivo de las tecnologías de la información.

---

[i] Ruiz Miguel, Carlos, *La configuración constitucional del derecho a la intimidad*, Madrid, Tecnos, 1995, pp. 94 y ss.

[ii] Herrán Ortiz, Ana Isabel, *Derecho a la protección de datos personales en la Sociedad de la Información,* Bilbao, Universidad de Deusto, 2003, p. 12.

[iii] Término que consagró la Sentencia del Tribunal Constitucional Alemán de 15 de diciembre de 1983 (*Informattionelle Selbstbestimmunsrecht).*
[iv] Frosini, Vittorio, *Informática y Derecho*. Bogotá, Temis, 1988, pp. 35 y ss.
[v] Pérez Luño, Antonio Enrique "Los derechos humanos en la sociedad tecnológica", en Lozano Mario *et al., Libertad informática y leyes de protección de datos personales*, Madrid, CEC, 1989, p. 140.
[vi] Pérez Luño, Antonio Enrique, *Manual de Informática y Derecho*, Barcelona, Ariel, 1996, p. 72.
[vii] En la versión dada por el Tratado de Maastricht; de 7 de febrero de 1992 y el Tratado de Ámsterdam, de 2 de octubre de 1997, y modificado por el Tratado de Niza firmado el día 26 de febrero de 2001.
[viii] Artículos 95 (armonización del mercado interior), 81 y 82 (referentes a la competencia), 47 y 48 (derecho de establecimiento y servicios) del TCE.
[ix] Artículos 163 – 172 del TCE.
[x] Artículo 157 del TCE.
[xi] Artículos 154 – 156 del TCE.
[xii] Villanueva, Ernesto y Luna Pla, Issa (ed.), *Derecho de acceso a la información pública. Valoraciones iniciales*, México, Universidad Nacional Autónoma de México, 2004, p. 89.
[xiii] Banisar, David, y Davis, Simon, *Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection, and Surveillance Laws and Developments*, Illinois, J. Marshall, Computer & Info, 1999, pp. 11- 12.
[xiv] Hasta hoy son 45 Estados contratantes del Convenio, entre los cuales se encuentran todos los países miembros de la Unión Europea. Para garantizar los preceptos contenidos en el CDE, fue creado el Tribunal Europeo de los Derechos del Hombre con sede en Estrasburgo artículo 19 de la CEDH.
[xv] A partir de mayo de 2004, la UE incrementó de 15 a 25 Estados miembros.
[xvi] Artículo 249 del TCE.
[xvii] Artículo 249 del TCE.
[xviii] Bennett, J. Colin, "Convergence revisited: Toward a Global Policy for the Protection of Personal Data?", in *Technology and Privacy: The New Landscape*, New York, Aspen Publishers, 1999, p. 689.
[xix] Solove, David J. y Rotemberg, Mark, *op. cit.*, p. 688.
[xx] Arts. 25 y 26 de la Directiva 95/46/CE.
[xxi] También llamada "Grupo del artículo 29".
[xxii] "Comité del artículo 31".
[xxiii] Heredero Higueras, Manuel, *La Directiva Comunitaria de Protección de Datos de Carácter Personal*, Pamplona, Aranzadi, 1997, p. 88.
[xxiv] Véase el artículo 26 de la Directiva 95/46/CE.
[xxv] Para un estudio detallado de este tema véase Argüello Téllez, Fernando, "Protección de Datos Personales: La Directiva Comunitaria, su Influencia y Repercusiones en Latinoamérica", *Protección de Datos de Carácter Personal en Iberoamérica (II Encuentro Iberoamericano de Protección de Datos, La Antigua – Guatemala, 2-6 de junio de 2003)*, Valencia, Tirant Lo Blach, 2005, pp. 69 y ss, en concreto p. 77.
[xxvi] Sin embargo, ambas partes podrán ser eximidas de responsabilidad si demuestran que ninguna de ellas es resposable.
[xxvii] Característica importante si consideramos que la Comisión se pronunció admitiendo como compatible con el artículo 25.6 la posibilidad de que existieran decisiones de adecuación sectoriales, aunque el enunciado del mismo hable únicamente de países.
[xxviii] Que en terminos de la Directiva 95/46/CE serían: derecho de información, consentimiento, comunicación a terceros, seguridad, calidad de datos, derecho de acceso y recursos, responsabilidad y sanciones, pero con un contenido más restringido.
[xxix] Las FACs son quince y se refieren a los datos especialmente protegidos, excepciones relativas al ejercicio del periodismo, responsabilidad subsidiaria de los proveedores de Servicios de Internet o telecomunicaciones, excepciones a los principios de notificación, opción y acceso para los bancos de inversiones y los bancos de auditoria, la función de las autoridades de protección de datos europeas, condiciones y compromisos adquiridos a través de la autocertificación, verificación del cumplimiento de Puerto Seguro, alcance del derecho de acceso, condiciones especiales referentes a los datos de Recursos Humanos transferidos desde la Unión Europea, regulación contractual de los tratamientos por cuenta de terceros, resolución de litigios y ejecución, precisiones sobre el derecho de opción, transferencia de información sobre viajes, transferencia de datos relativos a productos médicos y farmacéuticos y, finalmente, sobre la información extraída de registros públicos e información de dominio público.
[xxx] Si consideramos la Land de Hesse Alemana de 1970 como primera legislación en materia de protección de datos personales, aunque no tenía el carácter de ley estatal, y la primer disposición en esta

materia en Latinoamérica la encontramos en el artículo 5 LXXII de la Constitución brasileña de 1988, que menciona una acción de protección de la información personal como *habeas data*.

[xxxi] Otón Sidou, J. M., *Las nuevas figuras del derecho procesal constitucional brasileño: mandado de injunçao y habeas data*", trad. de Héctor Fix-Zamudio, *Boletín Mexicano de Derecho Comparado,* año XXIV, núm. 70, enero-abril de 199, pp. 180 y 181. Para Juan F. Armagnague, la expresión habeas data "ha tomado parte del latín y parte del inglés, "habeas viene del latín y significa *conserva y guarda tú*... del inglés proviene data, un sustantivo plural que se traduce como *información* o *datos*, por lo cual, en una acepción literal, habeas data se define como *conserva o guarda tus datos*", Armagnague, Juan F., *Derecho a la información, habeas data e Internet*, Buenos Aires, Ediciones la Roca, 2002, p. 325.

[xxxii] Palazzi, Pablo A., *La Transmisión Internacional de Datos Personales y la Protección de la Privacidad. Argentina, América Latina, Estados Unidos y la Unión Europea*, Buenos Aires, Ad Hoc, pp. 99 y ss.

[xxxiii] Argentina, Brasil, Colombia, Ecuador, Guatemala, Paraguay, Perú y Portugal.

[xxxiv] Véase el Capítulo IV de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental mexicana.