BARATARIA
Revista Castellano-Manchega de Ciencias Sociales
Nº 19, pp. 37-56, 2015, ISSN: 1575-0825, e-ISSN: 2172-3184
DOI: http://dx.doi.org/10.20932/barataria.v0i19.24

LA DESPROTECCIÓN "INTERNACIONAL" DEL TITULAR DEL DERECHO A LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

THE "INTERNATIONAL" NON PROTECTION OF THE HOLDER OF THE RIGHT TO PROTECTION OF PERSONAL DATA

Alfonso Ortega Giménez
Universidad Miguel Hernández, Elche. España/Spain
alfonso.ortega@umh.es

Recibido/Received: 17/12/2014
Aceptado/Accepted: 27/04/2015

RESUMEN
El objeto de este estudio es analizar los diferentes mecanismos de protección a los que podría o debería tener acceso el titular del derecho a la protección de datos personales, ante una transferencia internacional de sus datos ilícita, con el fin de obtener una tutela adecuada, equilibrada y efectiva, en los distintos centros de producción normativa: superestructura jurídica internacional, sistemas de integración regional, y espacio transnacional. Análisis que revelará una situación que dista mucho de ser satisfactoria y que concluirá demostrando que el Derecho internacional privado es, claramente, la posibilidad más plausible para que el perjudicado obtenga una satisfacción a sus legítimos intereses.La

PALABRAS CLAVE
Protección de datos personales, desprotección, transferencia internacional de datos.

SUMARIO
1. Planteamiento. 2. Superestructura Jurídica Internacional. 2.1. ONU. 2.2. OCDE. 2.3. Conferencia Internacional de Autoridades de Protección y Privacidad. 3. Estructuras de carácter regional. 3.1. UE. 3.2. Consejo De Europa. 3.3. APEC. 4.1. CCI. 4.2. ISO. 5. Balance Final. 6. Bibliografía.

ABSTRACT
The purpose of this study is to analyze different protection mechanisms that could or should be accessed by the person entitled to the protection of personal data, to an international transfer of illegal data in order to obtain adequate protection, balanced and effective, in different centers of production rules: international legal superstructure regional systems integration and transnational space. Analyzes reveal a situation that is far from satisfactory and will conclude by demonstrating that private international law is clearly the most plausible explanation for the injured get a satisfaction to its legitimate interests possibility.

KEYWORDS
Data protection, non protection, international data transfer.

CONTENTS
1. Approach. 2. International Legal Superstructure. 2.1. UN. 2.2. OECD. 2.3. International Conference and Privacy Protection Authorities. 3. Structure of regional character. 3.1. EU. 3.2. Council of Europe. 3.3. APEC. 4.1. CCI. 4.2. ISO. 5. Final Balance. References.

1. PLANTEAMIENTO

El estudio el problema de la desprotección del titular de datos de carácter personal ante una transferencia internacional está conectado con el particular contexto tecnológico, social, económico e histórico en que tales transferencias se desarrollan. Si en cualquier época el intercambio de datos entre los diferentes países ha sido una realidad, hoy en día, su volumen y su importancia han adquirido un crecimiento rápido y exponencial, gracias a dos circunstancias que han cambiado radicalmente la percepción de la sociedad respecto a las transferencias internacionales de datos de carácter personal: por un lado, el perfeccionamiento de las tecnologías de la información y de la comunicación, que favorecen el flujo global y exponencial de información; y, por otro lado, la propia mundialización de las transferencias internacionales de datos de carácter personal.

En primer lugar, los avances tecnológicos -en particular, el desarrollo de Internet- facilitan considerablemente el tratamiento y el intercambio de información, permiten compartir recursos tecnológicos, centralizar determinadas actividades y procesos, y abaratar costes en la prestación de servicios por las propias empresas, fuera del país en el que se encuentran establecidas. Estos avances permiten que los datos de naturaleza personal, siempre útiles e interesantes para el desarrollo de cualquier actividad a gran escala, puedan hoy circular internacionalmente de manera rápida y ser almacenados indefinidamente.

En segundo término, las transferencias internacionales de datos personales, en áreas tales como los recursos humanos, los servicios financieros, la educación, el comercio electrónico o la investigación en el área de la salud, se han convertido en parte integral e integradora de la economía globalizada. Efectivamente, el flujo internacional de datos personales no sólo constituye una industria auxiliar respecto de empresas, entidades o personas que se dedican a realizar o utilizar las transferencias bancarias, las reservas de pasajes aéreos o el auxilio judicial internacional, sino en un sector económico creciente, en sí mismo considerado.

Es innegable que esta transformación cualitativa y cuantitativa en los flujos internacionales de datos personales ha hecho más eficientes a las empresas y ha coadyuvado al desarrollo de la Sociedad de la Información y a la mundialización de la actividad económica. Pero tales contribuciones no se han realizado sin costes, ya que han puesto en peligro la vida privada del titular de esos datos. A nadie escapa que, sin demasiadas dificultades técnicas, la información puede ser objeto de un tratamiento ilícito; esto es, de una transferencia internacional de datos personales sin consentimiento del interesado, concluyendo en una violación de sus derechos fundamentales constitucionalmente protegidos. De ahí la aparición de diversos expedientes reguladores, presentes en los distintos niveles de producción jurídica -supraestructura jurídica internacional, plataformas de integración regional, estados y entidades subordinadas– y la necesaria cooperación de autoridades al efecto de prevenir y combatir dichas violaciones.

El objeto de la protección de datos es proporcionar a su titular mecanismos de defensa adecuados y efectivos frente a la obtención o tratamiento ilícito de la información de naturaleza personal. Esto se logra mediante un juego contrapuesto de atribución de derechos para el titular de los datos y de imposición de obligaciones para aquellos que captan o procesan los mismos y/o ejercen un control sobre dicho tratamiento de datos. La búsqueda soluciones equidistantes en la satisfacción de los intereses legítimos implicados en las transferencias internacionales de datos no es fácil. En especial, debido a las diferencias palmarias existentes en el panorama comparado entre los distintos niveles de protección de los derechos y libertades de las personas y su intimidad.

La paulatina configuración de un mercado a escala mundial y la consiguiente multiplicación de transacciones económicas y relaciones derivadas de las mismas han ocasionado un aumento notable de los flujos transfronterizos de datos de carácter personal, entre distintos agentes públicos y privados, establecidos en diferentes estados. La necesidad de regular adecuadamente este fenómeno es innegable; del mismo modo en que no caben dudas acerca de la complejidad de dicha tarea, dada la difícil conciliabilidad de intereses tan dispares como la protección de la intimidad personal, las legítimas aspiraciones comerciales de las empresas involucradas en el tratamiento internacional de datos, y la libertad de información y comunicación. Tal variedad de intereses y su relevancia hacen aparecer relaciones que afectan a ramas tan distintas del ordenamiento jurídico como el Derecho Internacional Público, con la creciente celebración de acuerdos internacionales de cooperación entre autoridades de control; el Derecho Internacional Privado, con la multiplicación de situaciones derivadas del incumplimiento de un contrato internacional de tratamiento de datos personales, la cesión o transferencia no consentida de los mismos a escala mundial; el Derecho público, con el manejo de datos por parte de la Administración, o con la imposición de sanciones administrativas por el incumplimiento de la normativa aplicable en materia de protección de datos personales.

Como se acaba de exponer, la protección de datos de carácter personal puede ser contemplada desde posiciones muy distintas, en función de los intereses concurrentes -los derechos fundamentales de las personas vs. la consideración económica de la información personal y la diversidad de sistemas- o de las diferentes ramas del Derecho implicadas en la regulación de un fenómeno tan complejo. Esa complejidad no sólo ocupa y preocupa al común de la población, sino que presenta un innegable atractivo académico y práctico, que se explica por dos factores básicos.

Primero, por el desarrollo global del comercio electrónico y demás servicios de la Sociedad de la Información. Resulta evidente que esta nueva configuración del marco económico y social redunda en un incremento de relaciones en las que está implicada la transferencia internacional de información sensible, con el consiguiente aumento de la litigiosidad y la creciente dimensión económica que está cobrando el libre tránsito de la información. El acceso y uso de la información por parte de empresas, administraciones e individuos, se ha convertido en un precioso bien intangible, causa y efecto a la vez de la progresiva integración económica y social. Como no podía ser de otro modo, dicha expansión supone afrontar la difícil tarea de compatibilizar los derechos fundamentales con las exigencias del comercio internacional, cuya liberalización -entronizada como principio rector por textos jurídicos fundamentales a escala mundial (OMC) o regional (UE, MERCOSUR, etc.)- es un límite básico a la hora de desarrollar expedientes reguladores. Segundo, por la presencia de empresas transnacionales que actúan a escala mundial, lo que en buena lógica supondría la necesidad de articular una respuesta tuitiva de los derechos del titular de datos de carácter personal también a escala global. No obstante, las dificultades teóricas y prácticas de tal empeño suponen que, de momento, nos debamos contentar con llegar a simples acuerdos de cooperación entre las distintas autoridades reguladoras. Así, en el seno de la UE, se van realizando esfuerzos de coordinación de la legislación de los Estados Miembros, de modo que dispensen una defensa "equivalente", sin perjuicio de reconocerles un margen de maniobra, que han de ejercer de conformidad con el Derecho de la UE y dentro de los límites de la propia Directiva 95/46/CE.

La ausencia de una tan deseable como, por el momento, irrealizable regulación verdaderamente internacional de las transferencias internacional de datos de carácter personal

y el carácter potencialmente limitado de las experiencias reguladoras regionales, convierten a los sistemas nacionales de Derecho internacional privado en el último refugio del titular de datos de naturaleza personal, enfrentado a una violación de sus derechos.

En primer lugar, las soluciones uniformes se ven dificultadas por las distintas calificaciones que reciben las diferentes categorías de datos personales y por el carácter dinámico del comercio internacional, poco favorable a la esclerotización que siempre supone la regulación de un determinado sector. Los logros más fundamentales, al menos por el momento, consisten en las acciones concertadas entre diferentes sistemas jurídicos, que permiten, además de la consecución de economías de escala sobre los costes de circulación internacional de la información, un aumento de la seguridad jurídica, impidiendo la constitución de "paraísos de datos" y la deslocalización de actividades informáticas.

En segundo lugar, la especial volatilidad de las transferencias internacionales de datos complica extraordinariamente la definición del derecho sustantivo aplicable. Las características de los flujos de información y el carácter abierto de las redes posibilitan el acceso a los datos, así como su recopilación y tratamiento simultáneo en y desde varios países, por lo que distintos estados podrán reclamar competencia jurisdiccional y/o normativa para definir los términos y las condiciones de las prácticas apropiadas en el ámbito del tratamiento de la información sensible.

La potencial pluralidad de ordenamientos jurídicos implicados en la protección de la correcta circulación internacional de datos de naturaleza personal y la existencia en sí de transferencias internacionales de tales datos, consecuencia del creciente carácter internacional de las relaciones personales y comerciales, exige la intervención del Derecho internacional privado; pero no una intervención cualquiera. Como se expondrá a lo largo de este trabajo, se trata tanto de describir, analizar y comparar el sistema vigente, cuanto de explorar la virtualidad de dicho sistema frente a un problema jurídico específico: la tutela eficaz y adecuada del perjudicado por un tratamiento ilícito de sus datos de carácter personal, derivado de una transferencia internacional. Esta visión particular y tuitivamente orientada exige una metodología especial, que no parte de la tradicional exposición de las cuestiones clásicas del Derecho internacional privado, sino del problema en sí: la desprotección del titular de datos de carácter personal. Para demostrar tal estado deficitario, muchas de las páginas que siguen se servirán de contribuciones de otras disciplinas jurídicas (Derecho económico internacional, Derecho internacional público o Derecho de la UE) para acabar concluyendo como las transferencias internacionales de datos de carácter personal ilícitas constituyen un auténtico desafío para el Derecho internacional privado.

A continuación, vamos a analizar los diferentes mecanismos de protección a los que podría o debería tener acceso el titular del derecho a la protección de datos personales, para obtener una tutela adecuada, equilibrada y efectiva en los distintos centros de producción normativa: superestructura jurídica internacional, sistemas de integración regional, y espacio transnacional. Análisis que revelará una situación que dista mucho de ser satisfactoria y que concluirá demostrando que el Derecho internacional privado es, claramente, la posibilidad más plausible para que el perjudicado obtenga una satisfacción a sus legítimos intereses.

2. SUPERESTRUCTURA JURÍDICA INTERNACIONAL

A partir del Acuerdo General sobre Aranceles Aduaneros y Comercio de la OMC es innegable la tendencia creciente a la institucionalización en la regulación de los intercambios

comerciales internacionales. Eso da como resultado la creación de instituciones internacionales de cooperación de muy distinto signo.

El presente apartado tiene por objeto identificar las iniciativas normativas provenientes de aquellas instituciones internacionales que se han ocupado de la protección de datos personales de los particulares, con el fin de determinar si les ofrecen una tutela adecuada, equilibrada y efectiva en caso de tratamiento ilícito internacional de sus datos personales. En particular, nos vamos a detener en las siguientes instituciones: 1) la ONU; 2) la OCDE; y 3) la CONFERENCIA Internacional de Autoridades de Protección y Privacidad; en la medida en que otras instituciones internacionales como la OMC o la OIT, a pesar de que su ámbito de competencia y las necesidades de sus objetivos requerirían actuar en este ámbito, a día de hoy, no lo han hecho.

2.1. ONU

A pesar de que el derecho a la intimidad puede ser concebida de forma distinta dependiendo del entorno cultural en el que nos encontremos, no podemos ignorar la existencia de un denominador común en todas las legislaciones y ordenamientos jurídicos: el hecho de entenderla como el "respeto a la protección personal y familiar" de todo individuo. Buena prueba de ello es el reconocimiento que de la misma hacen los textos internacionales, como la "Declaración Universal de los Derechos Humanos de 1948" o el "Pacto Internacional de Derechos Civiles y Políticos de 1966", que sitúan siempre su protección en la esfera de la vida privada.

Si bien es cierto que ese concepto ha sido válido y útil durante muchos años, no podemos ignorar que en algunos ámbitos, como el que nos ocupa, la realidad social va por delante de las normas. Debido al continuo avance de la técnica y la informática ha sido necesario dotar de una cierta autonomía al derecho a la protección de datos personales. Y es que, aunque los instrumentos tradicionales le han dispensado una cierta protección bajo el amparo del derecho a la intimidad, la naturaleza y especificidad de los derechos perjudicados demanda una mejor (y mayor) cobertura. A esta demanda han respondido el conjunto de directrices para la regulación de los archivos de datos personales informatizados, adoptadas por Resolución 45/95, de 14 de diciembre de 1990, de la Asamblea General de Naciones Unidas ("Directrices para la regulación de los archivos de datos personales informatizados"). En virtud de la misma, los procedimientos para aplicar las normas relativas a los archivos de datos personales informatizados se dejan a iniciativa de cada Estado, con sujeción a una serie de orientaciones, entre las que cabe destacar la relativa a ciertos principios que deberían observarse en las legislaciones nacionales: legalidad y lealtad, de exactitud, de especificación de la finalidad, de accesibilidad.

2.2. OCDE

La adopción de recomendaciones elaboradas por organizaciones como la OCDE, especialmente en lo relativo a la creación de marcos internacionales que permitan impulsar el respeto al derecho a la protección de datos en el contexto de las transferencias internacionales de datos, supone un positivo avance de cara a lograr este objetivo.

Es de destacar la Recomendación de 23 de septiembre de 1980 del Consejo de la OCDE relativa a las líneas directrices concernientes a la protección de la intimidad y los flujos transfronterizos de datos de carácter personal, que introdujo importantes reformas en sus legislaciones estatales con el fin impedir el almacenamiento ilícito de datos personales y su revelación no autorizada. Esta situación provocó con el tiempo una lógica preocupación por

proteger la intimidad de los ciudadanos, lo que dio lugar a un desarrollo asimétrico de normas nacionales y, por consiguiente, un inevitable obstáculo a la libre circulación transfronteriza de datos.

Por esta y otras razones, en el seno de la OCDE se han elaborado todo un conjunto de directrices que armonizan la normativa nacional relativa a la intimidad y tratan de impedir interrupciones en la circulación internacional de datos. Estas directrices son, en buena medida, resultado de los trabajos realizados por el subgrupo de la OCDE de Bancos de Datos en el Sector Público, el cual comenzó a articular soluciones políticas en este sentido, constituyendo, en 1978, un Grupo de Expertos encargado de estudiar esta problemática. Las directrices mencionadas se llevaron a cabo a través de tres instrumentos internacionales: a) la Recomendación de 23 de septiembre de 1980 en la se que insta a los Estados miembros a tener en cuenta en su legislación interna; b) las "Directrices sobre la protección de la intimidad y los flujos transfronterizos de datos de carácter personal"; y c) la Declaración de 11 de abril de 1985 "sobre flujos transfronterizos de datos". Las directrices recogidas en estas declaraciones y recomendaciones representan un consenso sobre principios básicos que en muchos casos se han incorporado a las legislaciones nacionales existentes, sirviendo de fundamento para aquellos países que todavía no disponen de este tipo de regulación. Entre estos principios destacan: el principio de limitación de la recogida de datos, el de calidad de datos, el de especificación del fin, de seguridad, transparencia, participación del individuo y el de responsabilidad. Todos ellos han sido reafirmados, si bien de forma implícita, en posteriores declaraciones e instrumentos internacionales realizados en el marco de la OCDE, como puede deducirse de la Recomendación relativa a las directrices de política criptográfica, adoptada por el Consejo de la OCDE el 2 de marzo de 1997, o la Declaración Ministerial relativa a la protección de la intimidad en las redes globales adoptado por el Grupo de Trabajo sobre Seguridad de la Información e Intimidad en Ottawa el 7 y 9 de octubre de 1998.

2.3. Conferencia internacional de autoridades de protección y privacidad

Nos referimos a la denominada *Resolución de Madrid*: "Estándares Internacionales sobre Datos Personales y Privacidad". Se trata de la Resolución relativa a la urgente necesidad de proteger la privacidad en un mundo sin fronteras, y de alcanzar una propuesta conjunta para el establecimiento de estándares internacionales sobre privacidad y protección de datos personales, aprobada en la 31ª Conferencia internacional de Autoridades de protección de datos y privacidad, celebrada en Madrid, del 4 al 6 de noviembre de 2009.

Señala la *Resolución de Madrid* que debemos apostar por un enfoque común, por el diálogo transatlántico entre la conjunción privacidad-seguridad y optar por el establecimiento de unos estándares comunes; y, más aún en una sociedad como la actual, en la que el desarrollo de las herramientas que proporciona la sociedad de la información y las tecnologías de la información y las telecomunicaciones dan lugar a un marco enteramente globalizado, en el que son comunes los flujos de datos entre los distintos Estados, siendo dichos flujos necesarios para el funcionamiento de la sociedad tal y como es hoy concebida.

Eso sí, hasta tanto se desarrollen estas iniciativas es preciso atender con especial sensibilidad a los flujos internacionales de datos, para que se permitan su transferencia desde entornos geográficos con niveles de protección adecuados a otros que carezcan de ellos, garantizándose la protección del titular del derecho a la protección de datos derivada de una transferencia internacional de datos de carácter personal ilícita.

La superación de fronteras físicas y temporales requiere, ineludiblemente, de un instrumento normativo común, con el que se logre el mayor consenso posible internacional.

No se trata de abandonar los sistemas jurídicos tradicionales, ni la fuerza de las leyes, sino de adaptar el sistema para que su aplicación y control sean lo más inmediato y factible posible. Es, por tanto, una adaptación multirregional y multidisciplinar del Derecho en materia de transferencia internacional de datos.

Es necesaria, pues, cierta coordinación en el ámbito mundial en materia transferencia internacional de datos personales, con el fin último de garantizar la protección del titular del derecho a la protección de datos ante el tratamiento ilícito internacional de sus datos de carácter personal.

Así las cosas, en mi opinión, las iniciativas que emanan de organizaciones intergubernamentales de alcance global estudiadas son claramente insuficientes para garantizar el derecho a la protección de datos de carácter personal. Las normas emanadas de estas instancias internacionales o bien no son directamente invocables por los particulares (perjudicados) o bien carecen de una traducción adecuada al plano práctico. El titular del derecho a la protección de datos sigue encontrándose en una evidente situación de inferioridad jurídica, que le sitúa al borde de la desprotección.

3. ESTRUCTURAS DE CARÁCTER REGIONAL

A pesar de que las distintas organizaciones internacionales están englobadas bajo una misma rúbrica (estructuras de carácter regional) los niveles de integración son muy distintos.

Una vez abordadas las iniciativas en materia de protección de datos personales provenientes de la superestructura jurídica internacional, en este segundo apartado nos ocuparemos de analizar los distintos intentos normativos de las organizaciones de integración regional que tienen como objetivo la protección del titular del derecho a la protección de datos de carácter personal; en particular, los provenientes de: 1) la UE; 2) el Consejo de Europa; y 3) la APEC.

3.1. UE

La regulación del tratamiento de datos personales en los Estados miembros de la UE se ha caracterizado por el alto grado de homogeneidad entre las normas existentes sobre la materia en cada uno de dichos Estados –consecuencia lógica de la transposición de la Directiva 95/46/CE–. No obstante, no podemos olvidar que cada Estado miembro tiene un margen de maniobra en la materia y que, además, se verá influenciado por diferentes factores políticos, culturales y sociológicos a nivel interno que provocarán pequeñas diferencias entre las legislaciones de unos y otros Estados.

El reconocimiento del derecho a la protección de datos de carácter personal, aunque es relativamente reciente en todos los Estados miembros de la UE, nos permite, hoy día, distinguir tres grandes grupos de Estados:

a) El grupo de aquellos Estados miembros en los que el texto constitucional reconoce expresamente un derecho a la protección de datos personales. Así ocurre en Suecia, Portugal, Eslovaquia, Eslovenia, Hungría y Polonia.

b) El grupo de los Estados en los que el texto constitucional no reconoce expresamente un derecho a la protección de datos personales, pero sí contiene disposiciones sobre la materia que han permitido al Tribunal Constitucional reconocer dicho derecho fundamental. Este es el caso de España, Países Bajos, Finlandia y Lituania.

c) El grupo de los Estados en los que en el texto constitucional no existe ninguna referencia a la protección de datos personales y el Tribunal Constitucional ha reconocido la existencia del derecho a la protección de datos personales como parte integrante, como nuevo contenido, de otro derecho fundamental, sí reconocido expresamente en la Constitución, ya sea el derecho a la intimidad o a la vida privada, ya sea al libre desarrollo de la personalidad y la dignidad humana.

Fue a partir de 1970 cuando los diferentes países europeos fueron abordando la tarea de regular el tratamiento de datos personales para tratar así de hacer frente a los potenciales peligros que los desarrollos tecnológicos representaban para la vida privada de las personas. Así, se han sucedido tres generaciones de leyes de protección de datos:

1) Las leyes de primera generación, surgidas tras la aprobación de la Ley del Land de Hesse, se caracterizaron por exigir una autorización previa para la creación de ficheros de datos y por crear autoridades de control encargadas de supervisar el tratamiento de datos.

2) Las leyes de segunda generación, elaboradas tras la aprobación del Convenio 108 sobre Protección de Datos del Consejo de Europa, se caracterizaron por una tendencia a la simplificación, por el abandono de los mecanismos previos de control y por la búsqueda de la autorregulación, de un equilibrio entre la protección de los derechos de los ciudadanos y el desarrollo de las nuevas tecnologías.

3) Tras la aprobación de la Directiva 95/46/CE -que nació con dos claros objetivos: evitar intromisiones ilegítimas en la vida de las personas y asegurar la consecución del mercado interior y la libre circulación de datos sin restricciones injustificadas entre los Estados miembros (artículo 1)-, las leyes de tercera generación se caracterizan por armonizar la libre circulación de datos y la defensa de los derechos de las personas, incrementando las medidas de seguridad; estas leyes, a diferencia de las anteriores, ya no se centran tanto en el uso de la informática como en la protección del individuo frente a la acumulación de datos personales.

La consolidación definitiva en la UE del derecho a la protección de los datos personales viene representada por la Carta de los Derechos Fundamentales de la UE (*DOUE* C 303, de 14 de diciembre de 2007, y C 83, de 30 de marzo de 2010), que reconoce el "Respeto de la vida privada y familiar" (artículo 7) y el derecho a la "Protección de datos de carácter personal" (artículo 8), al dotar al derecho a la protección de datos de una configuración legal expresa.

El artículo 7 señala que "Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones". Los derechos garantizados en el artículo 7 corresponden a los que garantiza el artículo 8 del CEDH. A fin de tener en cuenta la evolución técnica, se ha sustituido la palabra correspondencia por la de "comunicaciones". De conformidad con lo dispuesto en el apartado 3 del artículo 52, este derecho tiene el mismo sentido y alcance que el artículo correspondiente del CEDH.

El artículo 8 señala que "1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan. 2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que le conciernan y a obtener su rectificación. 3. El respeto de estas normas estará sujeto al control de una autoridad independiente". Este artículo se basa en el artículo 286 del Tratado constitutivo de la Comunidad Europea y en la Directiva 95/46/CE, así como en el artículo 8 del CEDH y en el Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, de 28 de enero de 1981, ratificado por todos los Estados miembros. El derecho a la protección de los

datos de carácter personal se ejerce en las condiciones establecidas por la Directiva antes mencionada y puede limitarse en las condiciones establecidas por el artículo 52 de la Carta.

La Carta distingue entre el tradicional derecho "al respecto de la propia vida privada y familiar" y el "derecho a la protección de datos personales". El primero está mencionado en el artículo 7, que en resumen reproduce el esquema del artículo 8 del Convenio Europeo de Derechos Humanos. El segundo, recogido en el artículo 8 de la Carta, consagra el carácter autónomo del derecho fundamental, distinto del derecho a la tutela de la vida privada. Y es importante resaltar que, caso único en el entero texto de la Constitución Europea, al derecho a la protección de datos personales se dedica un artículo especifico también en la primera parte (articulo 51). Este nuevo derecho fundamental no puede ser enmarcado en el esquema de "ser dejado solo", sino que se concreta en la atribución a cada uno del poder de "gobernar" la circulación de las informaciones que le conciernen. Se transforma así en elemento capital de la libertad del ciudadano en la sociedad de la información y de la comunicación.

Se ha individualizado, en su artículo 8, un novedoso derecho: el derecho a la protección de datos de carácter personal; que pasa a formar parte del orden público europeo y de los derechos de sus ciudadanos. Éste es uno de los derechos fundamentales que se explicitan con mayor amplitud y que aparece deslindado, con claridad meridiana, de otros como el respeto a la vida privada y familiar. Así, la privacidad ha entrado en la categoría de los derechos humanos en la medida que garantiza libertades ulteriores como la de obtener trabajo, un crédito o de optar o acceder a determinados servicios: en definitiva, devuelve al individuo (persona física) el control sobre su entorno y garantiza la sostenibilidad del desarrollo.

A. Iniciativas legislativas

Recientemente, el Parlamento Europeo y la Comisión han optado por una revisión de la Directiva 95/46/CE. Lo ha hecho a través de un Reglamento: "Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos" (Reglamento General de Protección de Datos, de 25-01-2012. *COM (2012) 11 final*.), norma general y directamente aplicable sin necesidad de transposición; el objetivo es claro: logar la uniformidad legislativa. Establece un conjunto de normas sobre protección de datos válido para toda la UE: control de los ciudadanos sobre sus datos personales, protección de datos adaptada al mercado único digital, y protección de datos en un contexto de mundialización. Ello deriva de la propia asunción de la figura del Reglamento como instrumento jurídico único. Sin embargo, su base jurídica está, cuanto menos, en entredicho: reconocerle valor jurídico a la Carta de los Derechos Fundamentales no ha sido otra cosa que atribuirle valor normativo a aquello que ya se venía aplicando como principio general del Derecho. Pero es más, el artículo 6.1 del TFUE es muy claro: las "disposiciones de la Carta no ampliarán en modo alguno las competencias de la Unión tal como se definen en los Tratados". La Comisión europea propone como fundamento el artículo 16.2 del TFUE, que parece atribuir una competencia específica al Parlamento Europeo y al Consejo que establecer "con arreglo al procedimiento legislativo ordinario, las normas sobre protección de las personas físicas respecto del tratamiento de datos de carácter personal por las instituciones, órganos y organismos de la Unión, así como por los Estados miembros". Aunque, se trata de una atribución limitada al "ejercicio de las actividades comprendidas en el ámbito de aplicación del Derecho de la Unión, y sobre la libre circulación de estos datos", ello explica que la

Propuesta de Reglamento se acompañe de la Propuesta de una Directiva relativa al ámbito judicial y policial.

Se proporcionan refuerzos a las autoridades nacionales independientes de protección de datos para que efectúen una mejor aplicación de las normas de la UE en su territorio. Paralelamente, se acentúan sus atribuciones, al asumir con carácter general la potestad de multar a las empresas que quebranten las normas de protección de datos de la UE, sanciones que pueden suponer hasta un millón de euros o un 2% del volumen de negocios anual global de una empresa. A su vez, se eliminan requisitos administrativos innecesarios, como los de notificación a las empresas. En lugar de la disposición actual, que obliga a todas las empresas a notificar todas las actividades de protección de datos a los supervisores de protección de datos, el Reglamento intensifica la responsabilidad y la obligación de rendir cuentas de todos aquellos que procesen datos personales. Por ejemplo, las empresas y organizaciones deberán notificar a la autoridad nacional de control toda violación de datos grave lo antes posible.

En cuanto al marco de protección de los ciudadanos, los principios normativos y los derechos Arco se refuerzan en tres sentidos:

1º) Para los casos en que el tratamiento de los datos exija el consentimiento del interesado, deberá dejarse claro en la normativa nacional que dicho consentimiento ha de obtenerse explícitamente y no presuponerse. Se trata de una mejora necesaria respecto de la situación actual, en la que se permiten categorías de consentimiento cuya concurrencia no siempre es de fácil determinación. Así, y como ejemplo de ello, conforme a los artículos 6 y 7 de nuestra LOPD el consentimiento puede ser tácito o expreso, lo cual no deja de plantear problemas. Respecto del consentimiento tácito, por su difícil concreción, más aún si, como exige la LOPD de manera un tanto incongruente, ha de ser además de tácito, inequívoco. En cuanto al segundo, porque se distingue entre consentimiento expreso escrito y no escrito, subcategorías que, de nuevo, son de complicada definición.

2º) Se regula el derecho a la portabilidad de los datos, es decir, se permite que los ciudadanos tengan un acceso más fácil a sus propios datos. Ello conlleva el poder transferir sus datos personales de un proveedor de servicios a otro con mayor facilidad, aspecto que aumenta además la competencia entre servicios.

3º) Muy en boga en los últimos tiempos e íntimamente relacionado con el núcleo del derecho de protección de datos, esto es, la disponibilidad efectiva sobre los datos personales protegidos, se introduce el "derecho al olvido". A través del mismo se pretende ayudar a los ciudadanos a gestionar mejor los riesgos inherentes a la protección de datos en línea, permitiendo a los usuarios borrar sus datos cuando no existan razones legítimas para conservarlos.

En lo relativo al ámbito geográfico de aplicación, deberán aplicarse las normas de la UE a toda empresa activa en el mercado de la UE que ofrezca sus servicios a ciudadanos de la Unión y procese datos personales en terceros países. Del mismo modo, los ciudadanos podrán dirigirse a la autoridad de protección de datos de su país, incluso cuando sus datos sean tratados por una empresa ubicada fuera de la UE.

Con respecto a la protección del titular del derecho a la protección de datos derivada de una transferencia internacional de datos de carácter personal ilícita el futuro Reglamento plantea una novedad relevante: si bien el artículo 3 mantiene el criterio territorial vinculado al concepto "establecimiento" para responsables o encargados de tratamiento ubicados geográficamente en la UE, incluye un nuevo criterio de "tratamientos relacionados con oferta de bienes o servicios a ciudadanos de la UE" o destinados a "monitorizar su conducta" para responsables sin establecimiento en la UE. De esta forma, la protección de los datos de los ciudadanos deberá extenderse a la transferencia internacional de datos desde la UE a terceros

estados, con independencia de la ubicación geográfica de una empresa o de su centro de tratamiento de datos. En el contexto de globalización actual, se exige una mejora de los actuales mecanismos de transferencia internacional de datos a terceros estados, a fin de facilitar el flujo transfronterizo de datos de carácter personal.

B. Cooperación de Autoridades

Cuando hablamos de Cooperación entre Autoridades nos estamos refiriendo a un caso concreto: el de las Normas o Reglas Corporativas Vinculantes (BCR: *Binding Corporate Rules*). Su objetivo es claro: flexibilizar los flujos de datos entre empresas de grandes corporaciones multinacionales. Las empresas multinacionales necesitan que la información pueda fluir entre sus diferentes sedes. Para ello hay que efectuar, en muchas ocasiones, una transferencia internacional de datos personales.

Se trata de códigos de buenas prácticas basados en las normas de protección de datos europeas y aprobadas al menos por una Autoridad de control, que dichas empresas multinacionales elaboran de manera voluntaria y suscriben a fin de asegurar las salvaguardias necesarias para determinadas categorías de transferencias internacionales de datos personales entre empresas que forman parte del mismo grupo de sociedades y están vinculadas por esas normas.

Las BCR son un conjunto de normas o reglas de procedimiento interno que rigen las transferencias internacionales de datos de carácter personal en el seno de grupos multinacionales de empresas. Se trata de un instrumento potenciado por la UE, enfocado a remover los obstáculos a la libre circulación de datos personales entre países, y a flexibilizar los movimientos internacionales de datos personales entre un grupo de empresas multinacionales con filiales establecidas incluso fuera del EEE.

De esta manera, las normas corporativas vinculantes se configuran como un instrumento que permite a las empresas ofrecer garantías para poder llevar a cabo transferencias de datos hacía terceros países. En concreto, el Grupo de Trabajo del artículo 29, en su documento de trabajo WP 108, recoge un modelo de *checklist* para la aprobación de dichas normas corporativas vinculantes, y en otro documento de trabajo (WP 107), establece un procedimiento de cooperación para la emisión de posiciones comunes sobre las garantías proporcionadas por dichas reglas corporativas que permitan a las empresas transferir datos.

Las BCR, que constituyen un instrumento positivo, alternativa a las cláusulas contractuales tipo, responden a la lógica de los contratos, pero en un planteamiento multilateral que exige el establecimiento de mecanismos de cooperación internacional entre las Autoridades nacionales de protección implicadas. Se sigue un modelo, que podríamos denominar de "integración intermedia". Supone la solicitud conjunta de las BCR ante una sola autoridad, pero la autorización debe ser emitida por cada una de las Autoridades nacionales de protección implicadas. Supone un grado de cooperación intermedio entre las Autoridades nacionales de protección.

El mecanismo es muy sencillo: a) uno de los miembros del grupo se erige en responsable de la solicitud y asume la iniciativa; b) este representante, que asume el liderazgo, debe presentar una sola solicitud de BCR a la Autoridad nacional de protección que considere la más adecuada *leading authority*); y, c) se presenta una sola solicitud que debe contener la mención de cada una de las Autoridades nacionales que debe prestar su autorización.

El procedimiento de cooperación comienza en este momento: la autoridad nacional de protección directora del proceso reenvía las BCR a las otras Autoridades nacionales de protección implicadas para que realicen las alegaciones que estimen oportunas. Cuando éstas

han sido realizadas, se comunica a la autoridad a cargo para que el grupo aporte las modificaciones necesarias; en ese caso, la versión inicial se consolida; aunque, como la última palabra la tiene cada una de las Autoridades implicadas, una puede estar conforme y otra exigir modificaciones para que las BCR se ajusten a su legislación nacional.

Este modelo presenta un atractivo frente a los contratos: sólo es necesario presentar las BCR para su aprobación ante una Autoridad nacional, mientras que los contratos deben ser presentados ante cada una de ellas, pero menos intenso, pues aunque las BCR se solicitan conjuntamente deben ser aprobadas por cada una de las Autoridades nacionales de protección implicadas.

Sin duda alguna, las BCR no sustituyen a las cláusulas contractuales tipo aprobados por la Comisión Europea, puesto que cada instrumento tiene sus propios propósitos. No son sino una alternativa a las cláusulas contractuales tipo que pueden suscribirse entre exportador e importador para la regulación de una transferencia internacional, que suponga una cesión de datos, cuando el destinatario de los datos está ubicado en un país fuera de la UE y que no goza de un nivel de protección adecuado.

Deben ser vistas como un instrumento que facilite las transferencias internacionales de datos personales, garantice la aplicación de la normativa sobre protección de datos, y se convierta en un instrumento propicio para fomentar el desarrollo y aplicación de unos estándares internacionales comunes.

Las BCR constituyen una suerte de *safe haven* entre empresas de un mismo grupo. El elemento clave de las BCR es que las mismas son vinculantes, tanto hacia dentro como hacia fuera. Hacia "dentro" (obligatoriedad interna) requiere de mecanismos legales corporativos y psicología corporativa de cumplimiento que se garantiza con una formación adecuada del personal. Hacia "fuera" (obligatoriedad externa), es decir, que la política de privacidad de la compañía se dé a conocer con total transparencia y que se haga con un acto de publicidad por parte de la empresa.

El Grupo de Trabajo del artículo 29, en los últimos tiempos, se ha concentrado en la mejora de las autorizaciones basadas en las BCR, habiéndose producido dos avances de interés:

- El primero de ellos tiene que ver con la aprobación por el Grupo de Trabajo del artículo 29 de tres Documentos de Trabajo (WP153, 154 y 155) que pretenden aclarar y complementar el régimen establecido por anteriores Documentos: en particular, por los WP 74 y 108.

- El segundo de los hitos destacados que merece una mención tiene que ver con la adopción de un acuerdo entre diversos Estados Miembros de la UE para el reconocimiento mutuo de sus decisiones en materia de BCR. Este acuerdo surge como respuesta a las dificultades del procedimiento de coordinación existente. El problema que se pretende paliar es el largo tiempo que media entre que una empresa solicita la autorización de una BCR y el logro de la decisión final. El acuerdo supone que cuando una empresa solicite autorización para una BCR ante la *Leading authority*, la decisión que ésta adopte será aceptada por las demás Autoridades participantes. El mecanismo no se configura como un acuerdo de contenido jurídico, sino como un compromiso político, que no altera la necesidad de iniciar procedimientos nacionales de acuerdo con lo establecido por las diferentes legislaciones nacionales, ni tampoco modifica la necesidad de que las BCR se ajusten a las especificidades que tales legislaciones puedan determinar.

En definitiva, las BCR se configuran, hoy día, como una alternativa contractual, de carácter multilateral, para la transferencia internacional de datos a terceros Estados. Se trata de reglas uniformes para el tratamiento de datos dentro de un grupo de empresas, aplicables a

las sedes implicadas en la transferencia, que implica la cooperación entre las Autoridades nacionales de dichas sedes.

Aunque el legislador europeo quiere darle un impulso a las BCR, convirtiéndolas en un instrumento habitual en todos los grupos multinacionales, y buena prueba de ello es que la Propuesta de Reglamento pretende convertirlas en el estándar que empleen los grupos multinacionales en el futuro, la obligatoriedad externa que se predica de las BCR, en la práctica plantea (y seguirá planteando), a nuestro modo de ver, tres problemas capitales para la protección del titular del derecho a la protección de datos de carácter personal ante el tratamiento ilícito internacional de sus datos personales: a) su carácter vinculante; b) el favorecimiento del *forum shopping*; y, sobre todo, c) la articulación de conflictos de competencia entre Autoridades de control. Veamos cada uno de ellos:

a) Su carácter vinculante: no podemos ocultar nuestras dudas sobre el carácter vinculante de las BCR, pues sólo son un mínimo nivel de protección: no son más que meras "declaraciones unilaterales de voluntad"; y es que, salvo algún caso aislado expresamente reconocido por la ley, la voluntad unilateral que se estima vinculante para quien la declara es la que va acompañada del consentimiento del que la recibe, por lo que en realidad se trata de un control unilateral, con obligaciones para una sola de las partes. Por eso, en la Ley española (RLOPD) se acepta la posibilidad de dar una autorización a solicitudes en que se aporte como garantía la existencia de unas normas corporativas vinculantes, pero siempre bajo el cumplimiento de unos requisitos concretos legalmente establecidos (artículo 70.4 del RLOPD).

b) El favorecimiento del *forum shopping*: las BCR implican que el grupo empresarial acepte que el posible perjudicado pueda elegir entre: a) la jurisdicción del Estado origen de la transferencia (lugar en que se encuentre el perjudicado); o, b) la del Estado en que se han delegado responsabilidades en protección de datos cometa -p. ej., el lugar donde se haya cometido la infracción- (WP 74, de 3 de junio de 2003), lo que, en la práctica, está favoreciendo el *forum shopping*.

El posible perjudicado (exportador o importador de los datos), consciente de que una misma situación privada internacional puede ser resuelta de manera distinta según sea planteada ante tribunales de un país o de otro país, podría acudir a las Autoridades de un país determinado con el fin de lograr un concreto resultado jurídico que favorezca sus intereses. Si las posibilidades del perjudicado se redujeran a una y sólo a una, cualquiera que sea el Estado miembro cuya autoridad deba pronunciarse al respecto, se evitarían evasiones de las legislaciones más restrictivas, no dando pie a prácticas de *forum shopping*, en caso de litigios derivados de la aplicación de una BCR, como consecuencia de un tratamiento ilícito internacional de datos de carácter personal.

c) La articulación de conflictos de competencia entre Autoridades de control: aunque la decisión de aceptación o no de las BCR será adoptada por consenso entre todas las Autoridades de control implicadas, no resulta posible la adopción de una decisión única al término del procedimiento de adopción de las BCR, al no caber el reconocimiento mutuo de las decisiones de las Autoridades. Se pueden plantear varios escenarios conflictuales: por un lado, uno, puede darse el caso de que una de las Autoridades de control participantes en el proceso de adopción de las BCR se declare competente en caso de incumplimiento de la misma, aún no siendo la Autoridad de control elegida en la BCR (*Leading authority*); es más, puede darse el caso de que la autoridad de control llegue a extralimitarse en el ejercicio de sus funciones de control; y, por otro lado, dos, es posible la disparidad de criterios de las Autoridades de control de los Estados miembros; p. ej., a la hora de determinar cuándo un

Estado tiene un "nivel de protección adecuado", o, en su caso, que existan requisitos adicionales en cada país, como la notificación o diligencias administrativas, que habrá que cumplir también.

3.2. Consejo de Europa

El Consejo de Europa es una organización internacional de ámbito regional destinada a promover, mediante la cooperación de los estados de Europa, la configuración de un espacio político y jurídico común en el continente, sustentado sobre los valores de la democracia, los derechos humanos y el imperio de la ley.

Tenemos como referente normativo el Convenio 108/81/CE, del Consejo de Europa, de 28 de enero de 1981, para la "protección de las personas con respecto al tratamiento automatizado de datos de carácter personal" (*BOE* núm. 274, de 15 de noviembre de 1985).

El Convenio 108/81/CE se presenta con un objetivo claro, que se establece en su artículo 1: garantizar a toda persona física el respeto de sus derechos y libertades fundamentales y en especial de su derecho a la intimidad, con relación al tratamiento automático de los datos de carácter personal que le conciernen (protección de datos).

La idea que subyace es buscar el equilibrio entre la protección de datos relativos a las personas y la libre circulación de las informaciones a través de las fronteras. El Convenio 108/81/CE "busca compatibilizar la protección del derecho a la intimidad personal con la liberalización de los flujos de datos entre los Estados parte *ius communicationis*"; se trata de un instrumento jurídico que carece de aplicabilidad directa, ya que mientras un Estado firmante del mismo no dicte las normas de desarrollo oportunas, éste no podrá ser aplicado directamente por los Tribunales. Además, se trata de una "norma de mínimos", que opera a modo de "postulados generales", pues permite, en su artículo 12, que los Estados parte en el mismo puedan llegar a tener un "Derecho distinto" sobre la materia, esto es, aunque la regla general es la "libre circulación de datos personales entre los Estados parte", estos pueden fijar limitaciones a la misma, mediante su normativa de desarrollo.

Son varios los principios sobre los que se sustenta el Convenio: a) el Principio del consentimiento, según el cual la finalidad justificativa de la creación de un fichero de datos debe estar definida y predeterminada antes de su puesta en funcionamiento; b) el Principio de lealtad, que implica que la recogida de datos debe realizarse de una forma lícita; c) el Principio de calidad, según el cual el responsable de los datos debe comprobar la exactitud de los datos recopilados y su actualización; d) el Principio de publicidad, que obliga a la existencia de un registro público de los ficheros automatizados; e) el Principio de control, que supone que cualquier persona tiene derecho a conocer si los datos que le conciernen son objeto de tratamiento informatizado y, si así fuera, a obtener copias de ellos, e incluso a su rectificación si fueran erróneos o inexactos; y, f) el Principio de seguridad y confidencialidad en el tratamiento de los datos, según el cual se debe establecer medidas de seguridad para que los ficheros de datos estén protegidos.

La relación existente entre la comentada revisión de la Directiva 95/46/CE y la del Convenio 108/81/CE, del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal es una realidad. Al cumplirse los 30 años de su adopción en 1981, se iniciaron los trabajos preparatorios de la revisión del Convenio 108 del Consejo de Europa, aunque ésta se lanzó formalmente a finales de 2010 con la aprobación por el Comité de Ministros de una "Resolución sobre la Protección de Datos y la Privacidad en el Tercer Milenio".

En 2011, el Consejo de Europa publicó una hoja de ruta con los hitos principales en lo relativo al proceso de modernización del Convenio 108. En noviembre de 2011, el

Secretariado publicó una primera propuesta de texto articulado, para su presentación y primera discusión general en la reunión plenaria del Comité Consultivo de Protección de Datos (T-PD), que se celebró ese mismo mes de noviembre.

Existe un consenso unánime sobre la necesidad de que ambos procesos sean coherentes. Pero el hecho de que la propia Comisión haya manifestado su intención de negociar el texto del Convenio en ejercicio de las competencias de la UE en la materia (para lo que tendrá que pedir el correspondiente mandato al Consejo de la UE), parecen indicar que el proceso se verá ralentizado. Por otra parte, se da también la circunstancia de que el Consejo de Europa no se ha decantado aún por un instrumento de modificación de entre varias opciones posibles (protocolo adicional, protocolo de modificación o convenio revisado), lo que indudablemente influirá en el cumplimiento de los plazos marcados.

3.3. APEC

La APEC se presenta como un Foro multilateral, creado en 1989, con el fin de consolidar el crecimiento y la prosperidad de los países del Pacífico, que trata temas relacionados con el intercambio comercial, coordinación económica y cooperación entre sus integrantes.

Merece nuestra atención el Marco de Privacidad de APEC que promueve un acercamiento flexible a la protección de la privacidad de la información en las Economías Miembro de APEC, evitando la creación de barreras innecesarias para los flujos de información (2005), que fue desarrollado y aprobado en 2004, con unos objetivos claros: impulsar la apropiada protección de la información personal, prevenir la creación de barreras innecesarias al flujo de información, promover que empresas multinacionales utilicen métodos uniformes para recabar y procesar datos personales, y facilitar esfuerzos nacionales e internacionales para exigir la protección de datos personales.

Así las cosas, es evidente que los intentos de estas organizaciones de integración regional (UE, Consejo de Europa, APEC) no han logrado en la práctica una protección adecuada, eficaz y equilibrada del titular del derecho a la protección de datos de carácter personal ante un tratamiento ilícito internacional.

Los intentos de estas organizaciones de integración regional se enfrentan a una doble dificultad, generada por la naturaleza propiamente internacional del problema: por un lado, la capacidad para llegar a soluciones *ad intra* -armonizando (Directiva) o uniformizando (Reglamento) legislaciones, o *ad extra* procurando la coordinación de autoridades-; y, por otro lado, no puede prescindir del diálogo con otros sistemas. Un rearme proteccionista interior puede penalizar al mercado regional en el plano de la competencia internacional o generar el recurso a los paraísos de datos.

4. INICIATIVAS EN EL ESPACIO TRANSNACIONAL

Un último fenómeno normativo que puede alcanzar cierta importancia en la materia que nos ocupa son las iniciativas procedentes del denominado "Derecho transnacional". En especial, el análisis se centrará en el protagonismo de las organizaciones creadas por los operadores del comercio internacional que codifican dicho ordenamiento jurídico espontáneo, profesional, cuyo objeto es regular las relaciones comerciales internacionales en el ámbito concreto de la protección del titular del derecho a la protección de datos.

Tales iniciativas normativas vendrían protagonizadas por los siguientes organismos de carácter privado que se han ocupado específicamente del problema: 1) la CCI; y 2) la ISO.

4.1. CCI

Debemos destacar una iniciativa: la Propuesta de la CCI que pretende modificar la Decisión de la Comisión Europea 2002/16/CE, sobre cláusulas contractuales tipo que amparan las transferencias a prestadores de servicios en terceros países (*DO* 2002 l 6/52).

La Propuesta debe ser acogida favorablemente en la medida en que permite, con garantías, posibilitar que los prestadores de servicios puedan contratar a otras entidades para la ejecución de los servicios cuya prestación fue inicialmente asumida por ellos. Dicha Propuesta se dirige de forma prioritaria a permitir la subcontratación de servicios por parte de un encargado del tratamiento, entre empresas ubicadas en terceros países que no garanticen un nivel de protección adecuado. Lo que, en la práctica, puede suponer que los fenómenos de deslocalización de actividades empresariales desde Europa se incrementen.

Es por ello que, partiendo de las garantías que deben exigirse en las transferencias internacionales de datos de carácter personal a países que carecen de un nivel de protección adecuado, debemos formular una observación dirigida a mantener la neutralidad entre las empresas que operan en el ámbito de la UE y las ubicadas en terceros Estados, en relación con el fenómeno de la subcontratación.

A mi modo de ver, el documento presenta una omisión relevante puesto que se limita a incorporar cláusulas contractuales que garanticen la protección de datos personales cuando el prestador de servicios (importador de los datos en un tercer país), subcontrata a otra empresa ubicada asimismo en un país tercero y no da respuesta a la posibilidad de que un prestador de servicios ubicado en la UE pueda subcontratar con garantías adecuadas con entidades en terceros países. La citada omisión podría suponer, en la práctica, que los efectos de las modificaciones propuestas no sean neutrales al permitir una mayor flexibilidad al prestador de servicios establecido en un tercer país frente al establecido en la UE, teniendo en cuenta que en el primero de los casos los riesgos asociados al tratamiento de datos pueden ser superiores al prestarse todos los servicios contratados o subcontratados en países donde, salvo en virtud de las cláusulas contractuales tipo, no es de aplicación la Directiva 95/46/CE.

Por tanto, esta falta de neutralidad puede incentivar fenómenos de deslocalización de actividades empresariales en la UE más intensivos de los que resultarían si se contemplaran unas cláusulas contractuales tipo que permitieran, al menos, que la actividad del primer prestador de servicios contratado por el responsable del tratamiento que subcontrata a empresas en un tercer país, estuviera ubicada en la UE. En tal caso, las modificaciones de la Decisión 2002/16/CE propuestas por la CCI, como concreción del sistema de garantías de la Directiva 95/46/CE, operarían como un instrumento normativo discriminatorio en contra de actividades empresariales en la UE, quedando, en última instancia, quedando, en última instancia, en cierto modo, desprotegido el titular del derecho a la protección de datos de carácter personal ante el tratamiento ilícito internacional de sus datos de carácter.

4.2. ISO

La Organización Internacional de Normalización o ISO es el organismo encargado de promover el desarrollo de normas internacionales de fabricación (tanto de productos como de servicios), comercio y comunicación para todas las ramas industriales a excepción de la eléctrica y la electrónica. Su función principal es la de buscar la estandarización de normas de productos y seguridad para las empresas u organizaciones (públicas o privadas) a nivel internacional.

Las normas que, actualmente, están siendo elaboradas por el nuevo grupo de trabajo de la ISO son tres: 1) la norma ISO 24760-1:2011 (“marco para que la gestión de información sobre la identidad se realice de manera segura, fiable y respetuosa de la privacidad”), que

define los términos para la gestión de identidades y especifica los conceptos básicos de la identidad y la gestión de la identidad y sus relaciones; 2) la norma ISO 29100:2011 ("marco sobre privacidad que define los requisitos de privacidad para el procesamiento de información de carácter personal en cualquier sistema de información de cualquier jurisdicción"), que proporciona un marco de privacidad al especificar una terminología común sobre la privacidad, definir los actores y sus roles en el procesamiento de información personal identificable, describir las consideraciones de privacidad salvaguardar, y proporcionar referencias a los principios de privacidad conocidos de tecnología de la información; y 3) la norma ISO 29101:2013 ("marco de referencia sobre la privacidad que establece las mejores prácticas para la implementación técnica uniforme de los principios de privacidad"), que define un marco de arquitectura de privacidad que especifica la preocupación por los sistemas (TIC) que procesan la información de identificación personal de la información y tecnología de comunicación, las listas de componentes para la aplicación de estos sistemas, y ofrece vistas arquitectónicas contextualizar estos componentes.

Las iniciativas en el espacio transnacional (CCI, ISO) son, en principio positivas, pero no son suficientes, desde la perspectiva tuitiva, para la protección del titular del derecho a la protección de datos. Tienen como destinatarios a las empresas de la industria de tratamiento internacional de datos (causantes del daño en un tratamiento ilícito internacional de datos). Consecuentemente, el perjudicado no tiene posibilidad de invocarlas.

5. BALANCE FINAL

Cualquier economía moderna tiene la necesidad de poder transmitir datos de carácter personal hacia el exterior. Si bien el perjudicado por un tratamiento ilícito internacional de sus datos se encuentra en una clara situación de inferioridad jurídica, que le sitúa al borde de la desprotección, la solución no puede venir por el bloqueo radical de los datos personales del perjudicado hacia el exterior.

Los retos que plantea la mundialización requieren herramientas y mecanismos flexibles que garanticen una protección adecuada, equilibrada y eficaz, sin fisuras jurídicas de los datos personales. Desde la superestructura jurídica internacional y las estructuras de carácter regional se deben promover la adopción de unas normas de protección de datos exigentes e interoperables en todo el mundo.

El estudio de los mecanismos y reglas de protección vigentes en los distintos niveles de producción normativa -superestructura jurídica internacional, sistemas de integración regional, realizaciones del denominado "derecho transnacional"-, arroja un balance claro: el marco jurídico existente es a todas luces insuficiente para garantizar el derecho fundamental a la protección de datos ante un tratamiento lícito internacional.

Las normas emanadas de las instancias internacionales y de las organizaciones de integración regional, a pesar de que han establecido límites a las transferencias internacionales de datos para evitar que la legislación interna de un país en la materia pueda ser burlada mediante la transferencia a otro país en donde la legislación sea menos exigente (o incluso que no exista legislación alguna en este campo), no tienen como objetivo principal la protección del titular del derecho a la protección de datos de carácter personal, sino cumplir con los objetivos de sus tratados. Por lo general, no son normas directamente invocables por los particulares, sino que son normas dirigidas a los estados.

Otro tanto cabe decir de las posibles soluciones que provengan del espacio transnacional: o bien se trata de códigos de conducta, recomendaciones, instrumentos de *soft law*, que tienen como destinatarios a las empresas de la industria de tratamiento internacional de datos; o bien ofrecen mecanismos alternativos de resolución de controversias pensados desde y para la defensa de los intereses de esas misma empresas.

Lo deseable sería la aprobación de una normativa que permita esclarecer responsabilidades en los flujos internacionales de datos derivados de las necesidades empresariales, reducir los costes de cumplimiento con la normativa, facilitar a los titulares del derecho a la protección de datos instrumentos efectivos de protección de sus derechos, y dotar de mayor eficacia a los reguladores y minimizar las cargas administrativas.

Mientras eso llega, a día de hoy, la normativa de Derecho internacional privado es, de lejos, la más manifiestamente mejorable siempre desde un punto de vista tuitivo.

El estudio de los mecanismos y reglas de protección vigentes en los distintos niveles de producción normativa -superestructura jurídica internacional, sistemas de integración regional, realizaciones del denominado "derecho transnacional", Derecho internacional privado- arroja un balance claro: el marco normativo existente es a todas luces insuficiente para garantizar el derecho a la protección de datos, ya que se encuentra fragmentado en unidades nacionales de regulación, custodiadas por autoridades de protección independientes. El titular del derecho a la protección de datos se encuentra en una evidente situación de inferioridad jurídica, que le sitúa al borde de la desprotección frente al superior conocimiento técnico y poder económico de los infractores.

Las normas emanadas de las instancias internacionales (ONU, OMC, OCDE) o bien no son directamente invocables por los particulares o bien carecen de una traducción adecuada al plano práctico. Por supuesto que sería deseable lograr un gran acuerdo internacional, cuyo objetivo principal fuese la protección del titular del derecho a la protección de datos de carácter personal, sin que ello supusiese una carga excesiva al libre flujo de datos, que afectase negativamente a las relaciones comerciales internacionales. La apuesta debería ser, al tiempo, ambiciosa y equilibrada. Ambiciosa, porque partimos de la inexistencia de experiencias concretas en este campo; lo que implicaría buscar el foro más adecuado para su discusión y adopción, así como el mecanismo jurídico con la mayor proyección más universal posible. Equilibrada, porque hay que conjugar intereses legítimos de muy variada naturaleza y contrapuestos: por un lado, el derecho fundamental a la protección de datos de carácter personal y, por otro, las necesidades del comercio electrónico y los pactos internacionales de liberalización de los intercambios comerciales transfronterizos.

En cualquier caso, el contenido mínimo de ese instrumento legislativo universal y vinculante debería: a) establecer y llevar a la práctica los principios comunes existentes en materia de protección de datos y los límites a la libre circulación de información de carácter personal; b) reforzar la cooperación internacional entre las autoridades de protección de datos; y c) contemplar mecanismos de resolución de controversias adecuados y coercitivos. De momento, la agenda de las distintas organizaciones internacionales y la experiencia jurídica comparada no parecen contemplar nada parecido a tal emprendimiento.

Por su parte, los intentos de las organizaciones de integración regional (Consejo de Europa, APEC, UE) se enfrentan a una doble dificultad. Por una parte, la capacidad para llegar a soluciones *ad intra* -armonizando (Directiva) o uniformizando (Reglamento) legislaciones, o procurando la coordinación de autoridades (Convenios internacionales)- no puede prescindir, dada la naturaleza propiamente internacional del problema, del diálogo con otros sistemas. Por otra, las soluciones tradicionales de Derecho internacional privado no sólo no son del todo adecuadas para funcionar en una perspectiva *ad extra* -normas de

competencia judicial internacional que discriminan entre demandados domiciliados dentro o fuera del sistema regional, particularismos, problemas de alegación y prueba del derecho extranjero, etc.-, sino que tampoco resultan satisfactorias para proteger a la parte débil. Ello resulta manifiesto si se tiene en cuenta el establecimiento del domicilio del demandado como foro general (*verbi gratia*, foro del infractor), o la difícil precisión de los fueros especiales aplicables en la materia (*forum delicti commissi*), especialmente cuando el perjuicio se produce a escala mundial. Todo ello conduce a que el titular perjudicado por un tratamiento transfronterizo ilícito de sus datos personales, se sienta evidentemente desincentivado para reclamar en sede extracontractual.

Tampoco las posibles soluciones que provengan del denominado "derecho transnacional" ofrecen un balance esperanzador para el perjudicado. Sus realizaciones más notables consisten en códigos de conducta, recomendaciones, instrumentos de *soft law*, etc., que tienen como destinatarios a las empresas de la industria de tratamiento internacional de datos, o en sistemas alternativos de resolución de controversias, pensados desde y para la defensa de esas mismas empresas, prescindiendo del necesario contrapeso de intereses.

Establecida la necesidad de buscar mecanismos jurídicos que corrijan la posición de inferioridad del titular del derecho a la protección de datos, es preciso partir de la complejidad de la tarea. La importancia de los intereses en presencia -derechos fundamentales de la persona perjudicada, del comercio internacional en general y de la industria de tratamiento de datos, en particular- exige una ponderación entre lo deseable y lo posible. Desde la primera de esas coordenadas, no cabe duda de que un problema que nace y se desarrolla en un ámbito deslocalizado y potencialmente mundial exigiría, como solución ideal, soluciones igualmente internacionales. Sin embargo, al menos de momento, tal aspiración está lejos de poder ser colmada por cualquiera de los centros de producción normativos analizados. Es más, de ser abordada, ni siquiera lo sería sin grandes costes, en términos de recursos y de la experiencia jurídica precisa para la elaboración de normas aceptables que obtengan un consenso representativo y efectivo. Desde la segunda de las directrices antes apuntadas, el titular del derecho a la protección de sus datos de carácter personal no requiere una tutela absoluta o a cualquier precio. Un planteamiento excesivamente estricto impediría respetar los compromisos adquiridos internacionalmente y las necesidades legítimas del comercio internacional (ONU, OMC, OCDE) y de la realidad de las redes mundiales de telecomunicación. Una protección a ultranza amenazaría con crear un foso entre la legislación y la práctica, tan perjudicial para la tutela del derecho a la protección de datos de carácter personal cuanto para la industria que los trata. La protección que aquí se reclama debería reunir, en línea de principios, las siguientes características: tutela adecuada, equilibrada y efectiva. Adecuada o, en términos jurídicos, fácilmente accesible. Equilibrada, es decir, que pondere los intereses en juego y no acabe por morir de éxito debido a una eventual tentación sobreprotectora. Efectiva, en fin, traducible en una satisfacción que generalmente consistirá en una indemnización económica, dado lo irreparable del daño por otras vías.

A día de hoy, para obtener esa compensación ante la violación de un derecho fundamental, el Derecho internacional privado se presenta como el sistema normativo más manifiesta y sencillamente mejorable; ya sea reinterpretando a favor del perjudicado las normas vigentes de competencia judicial internacional y derecho aplicable; ya sea reformando en sentido tuitivo dicha normativa. En el sector del reconocimiento y ejecución de decisiones no se presentan peculiaridades dignas de estudio particular en este ámbito, por lo cual no han sido objeto de análisis particular.

Con el instrumental jurídico vigente en la mano, parece razonable llevar a cabo una interpretación de los foros de competencia judicial internacional con el fin de que se garantice un correcto equilibrio entre los distintos intereses en presencia y el sistema responda, por un lado, al principio de proximidad y, por otro, prevea una protección eficaz del titular del derecho a la protección de datos de carácter personal, derivada de una transferencia internacional ilícita. Ahora bien, aun forzando al máximo las posibilidades hermenéuticas del sistema -en el sentido más favorable de la víctima que se quiera (*forum damni*)- los criterios de competencia judicial internacional vigentes no son adecuados para procurar una protección adecuada, equilibrada y eficaz del perjudicado por una transferencia internacional ilícita de información personal sensible.

BIBLIOGRAFÍA

CARRASCOSA GONZÁLEZ, J. (1997). "Circulación internacional de datos personales informatizados y la Directiva 95/46/CE, en *Actualidad Civil*, 23: 509-539.

CARRASCOSA GONZÁLEZ, J. (1992). "Protección de la intimidad y tratamiento automatizado de datos de carácter personal en Derecho Internacional Privado", en *Revista Española de Derecho Internacional*, XLIV, 2: 417-441.

ESTADELLA YUSTE, O. (1995). *La protección de la intimidad frente a la transmisión internacional de datos personales*. Madrid: Tecnos.

GUERRERO PICÓ, Mª C. (2006). *El impacto de Internet en el Derecho fundamental a la protección de datos de carácter personal*. Navarra: Aranzadi, Cizur Menor.

MARTÍN y PÉREZ DE NANCLARES, J. (2008). "Comentario al artículo 8. Protección de Datos de Carácter Personal", en *Carta de los Derechos Fundamentales de la Unión Europea*. Madrid: Fundación BBVA, pp. 223-243.

ORTEGA GIMÉNEZ, A. (2014). *La (des)protección del titular del derecho a la protección de datos derivada de una transferencia internacional ilícita en derecho internacional privado español*. Tesis doctoral. Alicante: Universidad de Alicante.

SANCHO VILLA, D. (2010). *Negocios internacionales de tratamiento de datos personales*. Navarra: Civitas, Cizur Menor.

Breve currículo:

Alfonso Ortega Giménez
Doctor en Derecho. Profesor de Derecho internacional privado en la Universidad Miguel Hernández de Elche; Subdirector Académico del Master en Comercio Internacional, organizado por la Universidad de Alicante. Director del Observatorio de la Inmigración de la ciudad de Elche y Vocal del Observatorio Valenciano de la Inmigración. Consultor de Derecho internacional privado de la Universitat Oberta de Catalunya (UOC). Consejero académico de PELLICER & HEREDIA ABOGADOS y miembro del Consejo Asesor de la Revista *Economist & Jurist*. Miembro de la Red Española de Política Social (REPS). Autor de diferentes artículos, notas, recensiones y comentarios publicados en Revistas científicas, técnicas y de divulgación, españolas y extranjeras; ha participado, como coordinador y/o autor, en más de 60 libros.