Cuestiones Internacionales: Transferencia internacional de datos. Ley aplicable y jurisdicción.

Por: Juan Antonio TRAVIESO

I. Introducción

Este trabajo tiene un contenido de presentación, historias y dilemas.

Traigo el saludo del Gobierno de Argentina que está luchando para reconstruir y sustentar una democracia estable en el estado de derecho, con una economía al servicio de todos. Tengo la esperanza de que la protección de datos personales sea un objetivo compartido con Uds., para lo que les ofrezco mi amistad y mi compromiso de seguir transitando los caminos comunes con la Unión Europea.

Luego de esta presentación que representa un honor y un compromiso personal e institucional, permítanme informarles sintéticamente, casi en lenguaje de email que en la Argentina se ha establecido la protección de datos personales en tres escalones. Un primer escalón está en la Constitución con la acción de habeas data (CN art. 43); un segundo escalón por el que el Parlamento por medio de una ley nacional ha desarrollado los alcances de la disposición constitucional (Ley 25326), y finalmente un Decreto del Poder Ejecutivo que ha reglamentado la norma citada (Decreto 1558/01).

Ahora vamos al punto del panel, que tiene relación estrecha con el proceso legislativo indicado, desde que reconocemos las fuentes en las Directivas de la Unión Europea como inspiradoras y orientadoras en la materia.

Soy básicamente un Profesor de Derecho Internacional y como tal, voy a proponer un esquema alrededor del derecho y de las propias obsesiones.

Por eso, en esta circunstancia, en pleno siglo XXI, con la globalización imperante, no vamos a comenzar por el futuro. Vamos a remontarnos al pasado con viejas historias, que se inician en 1902, hace solamente 100 años al comenzar una amistad. En ese marco quedará el dilema ético, mezcla de espejos de Borges que reflejan imágenes contradictorias. Por eso ofreceremos nuestro homenaje a Max Brod que traicionó la confianza, la intimidad y los datos personales como más adelante veremos.

II. Planteamiento del problema

La solución de los problemas que plantea la jurisdicción y la ley aplicable a un caso con elementos internacionales es siempre conflictiva. Esta presentación va a girar entre los conceptos de lege lata pero más en los de de lege ferenda.

Para el tema que nos convoca, postulamos la aplicación de la jurisdicción extraterritorial, esto es, la capacidad de un Estado para entender en el juzgamiento de una transferencia internacional de datos que ha ocurrido fuera de su territorio, bajo la condición de que los efectos de la misma hayan repercutido en él. Vemos con optimismo el desarrollo de nuestra disciplina que nos permite elaborar un esquema que deseamos compartir.

A partir de la Directiva 95/46/CE y de la sanción de numerosas legislaciones internas que rebalsan la Unión Europea, se abre un panorama para el derecho internacional de la protección de datos personales que genera varios interrogantes.

La transferencia de datos personales opera a nivel interno e internacional. A nivel interno el cuestionamiento queda superado pues el criterio de compatibilidad lo otorgan las legislaciones internas, que de una manera u otra, más general o particular han receptado el criterio del “nivel de protección equivalente” y “nivel de protección adecuada”. Por la novedad de la materia, proponemos elaborar en conjunto una ingeniería jurídica con el modelo de POPPER que implica diseñar el avión, mientras éste se halla en vuelo. Adelantamos que tenemos el hardware en protección de datos y estamos trabajando en el software de éstos, cuyo manual de funcionamiento es la Directiva 95/46/CE.

Si la transferencia irregular de datos se efectúa en Estados que son regidos por la Directiva 95/46/CE, o por alguna norma interna o internacional similar donde se requiera un nivel de protección equivalente o adecuado para la transferencia, y esos Estados ejerzan su jurisdicción sobre el caso, la solución no reviste mayores dificultades.[1]
La cuestión se presenta, cuando la transferencia internacional de datos produce sus efectos sobre otro Estado que no ha participado de ella, y los Estados que sí han participado no juzgan el caso.
Cabe preguntarse entonces si existe la posibilidad de aplicar sanciones a un responsable de una transferencia en un Estado que no ha ejercido su jurisdicción para juzgar el caso.
Adelantamos nuestra respuesta afirmativa en cuanto a la posibilidad de un Estado para juzgar transferencias de datos irregulares acaecidas en otro Estado.

III. El orden público internacional y la protección de datos personales
La protección de los datos personales en general, y conceptos tales como "datos sensibles o especiales"[2] y "nivel de protección adecuada"[3] en particular, comienzan a formar parte de la práctica generalmente aceptada como derecho por los Estados, con conciencia de obligatoriedad, muy cerca de constituir "*opinio Juris*". Prueba de ello es la gran cantidad de Estados que han sancionado normativas de protección de datos con contenidos similares o idénticos. Por tanto, podemos afirmar que asistimos a una extensión del contenido y aplicación del orden público internacional, que incorpora la protección de datos personales.
Frente a este nuevo marco, que obliga a elaborar un nuevo esquema en la forma de abordar el tema, se observa que el control relativo a la protección de datos personales no recae exclusivamente en el ámbito de la jurisdicción interna de los Estados.
Desde este enfoque, planteamos como punto de partida en el tema de la transferencia internacional de datos la aplicación de la ley y jurisdicción del lugar donde se producen los efectos de esa transferencia, y no la del lugar desde el cual se emitió la transferencia. La nueva realidad nos introduce en un ciberespacio transversal, que no es tierra de nadie[4]. Un punto de vista contrario, significaría que en ese ciberespacio, la jurisdicción sería virtual y el transmisor de datos y el receptor se hallarían fuera de cualquier regulación en un paraíso del laisses faire.
Por ese motivo es que es indispensable que el Estado pueda juzgar una transferencia internacional de datos consumada entre terceros países. Para que ello sea posible, la transferencia debe repercutir en el Estado que pretende juzgarla, por ejemplo, cuando la titularidad de los datos transferidos recae en sus propios nacionales. *In additionem*, se puede establecer un sistema instrumental que asegure, en una primera etapa con aprobación de los Estados, sistemas de jueces virtuales y arbitrajes "*on line*".

IV.- La jurisdicción internacional en materia de protección de datos personales
Desde la Corte Permanente de Justicia Internacional se está sosteniendo una expansión de la extraterritorialidad, incluso en el derecho penal (caso Lotus).

---

[1] Directiva95/46/CE, art. 4.
[2] Directiva 95/46/CE, art. 8.
[3] Directiva 95/46/CE, art. 25.
[4] Perrit, Henry H., "*Jurisdiction in Cyberspace*", Villanova Law Review, 41 Vill.L.Rev. 1 (1996); y Henry H. Perrit, Jr. "*Jurisdiction in Cyberspace: The Role of Intermediaries*", Kahin and Nesson, pp. 164-202.

Este principio puede ser aplicado a la materia que nos ocupa. En efecto, la extraterritorialidad de la jurisdicción que propugnamos no impide la soberanía territorial de los Estados.

En esta época de globalización, la soberanía se reconstruye. La reconstrucción parte de los mismos estándares originales en cuanto al tema que estamos examinando, pues en la materia de protección de datos, es de interés de los Estados que afirmamos el sistema del nivel de protección adecuada, entender la jurisdicción soberana desde el punto de vista clásico replanteado. Los autores han entendido a la soberanía limitada por la ley internacional (Anzilotti[5]).

Tomando en consideración lo expuesto, podemos entender a la jurisdicción para juzgar una transferencia internacional de datos personales desde un triple punto de vista:

a) **jurisdicción territorial**: se trata básicamente del juzgamiento de hechos acaecidos dentro de un territorio de un Estado, por sus propios jueces.
b) **Jurisdicción extraterritorial**: consiste en la facultad que posee el Estado para juzgar hechos acaecidos en el territorio de otro Estado soberano. Este tipo de jurisdicción es la que se adopta en varios instrumentos internacionales,[6] que contienen el principio "juzgar o dejar juzgar" (*aut dedere aut iudicare*) que *mutatis mutandi* puede aplicarse al caso.
c) En tercer lugar, la **jurisdicción supranacional**, entendiéndose por tal el establecimiento de órganos que tienen facultades jurisdiccionales en dos niveles: jurisdicción especializada (Sala del Medio Ambiente en la Corte Internacional de Justicia) y jurisdicción general supranacional (Tribunal Internacional del Mar de Hamburgo y últimamente el Tribunal Penal Internacional).

A nivel comunitario, siempre de lege ferenda, la propuesta podría abarcar la constitución de una Sala especializada en protección de datos personales dentro de la Corte Europea de Derechos Humanos.

Siempre hay que tener en cuenta, que la arquitectura de la Disposición 95/46/CE prescribe la prevención,[7] esto es la prohibición de transferencia de datos que no respeten el art. 6 de la misma.[8]

V. Conclusiones

Estamos asistiendo al surgimiento de una nueva comunidad internacional dotada de un nuevo concepto de orden publico que, también "*mutatis mutandi*" podría incorporar un nuevo *jus cogens para la protección de datos personales, in statu nascendi*, que incorporaría entre sus postulados a la protección de los datos personales.[9]

Estamos convencidos que esto ya es posible en virtud del desarrollo actual del Derecho Internacional y Comunitario.

---

[5] Austro –German Custom Union Corte Permanete de Justicia (1931) Series A/b , Nro. 41 (2 W.C.R. 713).

[6] Por ejemplo, la Convención contra la Tortura (art. 5) y la Convención Interamericana contra la Corrupción (art. V).

[7] Directiva 95/46/CE, art. 25 inc. 4.

[8] En todos los caso en que existiera responsabilidad por daños derivados por incumplimiento de la protección de datos personales, podría aplicarse lo establecido en el Primer Informe sobre Responsabilidad internacional de QUENTIN BAXTER en el que el razonamiento se desarrollaba sobre la máxima latina "sic uture suo cum allieno suo", esto es, en síntesis que el que causa un daño debe repararlo, concepto que surge desde el famoso arbitraje del caso Trail Smelter y el desarrollo de CLYDE EAGLETON que afirmaba en una obra clásica acerca de la Responsabilidad de los Estados que el estado debe responder cuando causa daños sean directos o transfronterizos.

[9] La Carta de los Derechos Fundamentales de la Unión Europea ha establecido la protección de datos de carácter personal , los principios en el tratamiento de datos y el control por parte de una autoridad independiente (art.8)

Pero volvamos al siglo pasado como lo prometimos al principio. Nos falta el homenaje contradictorio y dilemático a Max Brod, por incumplir el deseo del amigo en su testamento. Max Brod afectó los derechos a la intimidad y datos personales, violó la confianza. Hizo mal, para hacer bien. ¿Quién tiene la calidad ética suficiente para juzgar si es más valiosa la obra de Kafka o su voluntad de destruirla? Y en nuestro caso ¿Es más valiosa también la obra, o los datos personales y la intimidad? Un litigio entre dos objetos culturales que hoy nos permite leer a Kafka, más allá de cualquier jurisdicción.