Transferencia Internacional de Datos Personales

Fundamentos de su reglamentación y principios rectores

Por Eugenio Capriotti

Introducción [arriba]

En las últimas décadas se ha convertido en una cuestión evidentemente sensible el modo en que determinados sujetos administran datos personales[1] ajenos, asunto para nada irrelevante si se tiene en cuenta la fuerza y rapidez de internet y las nuevas tecnologías como potenciadores de los eventuales daños que un incorrecto manejo de los mismos puede causar a los derechos e intereses legítimos de las personas.

Por ello, le concierne al Estado garantizar un adecuado marco de protección de datos personales. Más aún en aquellas transferencias de datos que tengan por destino países sin legislación calificable, a criterio de la Dirección Nacional de Protección de Datos Personales (en adelante, DNPDP), como adecuada.

Mediante la Disp. 60/2016 la DNPDP precisó aquellos países que caben ser considerados como poseedores de una legislación adecuada en los términos del art. 12 de la Ley N° 25.326.

¿Cuáles son dichos países? El art. 3 de la mencionada Disposición enumera a los Estados miembros de la Unión Europea y miembros del Espacio Económico Europeo (EEE), Suiza, Guernsey, Jersey, Isla de Man, Islas Feroe, Canadá (sólo respecto de su sector privado), Andorra, Nueva Zelanda, Uruguay e Israel (sólo respecto de los datos que reciban un tratamiento automatizado).

En realidad, se trata, tácitamente, de un modelo de "lista blanca"[2] ya que es posible autorizar transferencias a países no enumerados pero que son adecuados según la UE. Se adopta este sistema pero sin adherir por escrito y estrictamente a la UE. Además, cabe agregar que de oficio la DNPDP podría realizar los estudios sobre otros países u organismos internacionales, o bien alguno de estos podría solicitar su adecuación.

Esto último podría servir para incluir nuevos países adecuados, o para retirar de la lista algunos. Por ejemplo, el Reino Unido, después de su salida de la Unión Europea (Brexit) podría eventualmente llegar a ser reevaluado para ver si es "adecuado". Pese a no estar en la UE, si mantiene su infraestructura de legislación y agencia independiente de protección de datos, podrá seguir siendo país adecuado a los fines de transferir datos personales.

Estados Unidos no está mencionado en la white list de la DNPDP porque en la práctica no tiene una ley general de protección de datos como el resto de los países europeos ni una agencia de protección de datos independiente. Tampoco aparecen mencionado países latinoamericanos tales como México o Colombia, excepto Uruguay que fue declarado país adecuado por la Comisión Europea.

Finalmente, la disposición mencionada aprobó dos contratos modelos, similares a los adoptados por la UE[3], para usar en la transferencia de datos a países con regímenes legales

no adecuados y reglamentó, además, la necesidad de solicitar autorización para usar un modelo diferente a los indicados.

El contrato de transferencia internacional de datos personales constituye el eje de análisis del presente trabajo: más precisamente, los recaudos que debe tomar el "exportador" de datos personales al vincularse con sujetos ubicados en países con una legislación de datos personales precaria o catalogable como insegura. Todo ello en virtud de una serie de elementos esenciales que se extraen de los modelos ofrecidos por la entidad.

Desarrollo [arriba]

I. Contrato de transferencia internacional

La DNPDP aprobó dos modelos, (i) uno para transferencia internacional de datos a otro responsable, que en la práctica constituye el caso típico de la casa matriz que centraliza datos de las subsidiarias locales mediante la cesión; (ii) el otro modelo es para la prestación de servicios, que podrá ser con la casa matriz o con un tercero que provee servicios y que, lógicamente, está fuera de país. La elección de uno u otro modelo repercute, en lo que le interesa al Importador, en el tipo de responsabilidad atribuible: solidaria o mancomunada[4].

De la lectura de las cláusulas de ambos modelos se puede concluir que el contrato tiene ciertos principios destinados a brindar un nivel adecuado de protección en la transferencia y que deben estar presentes en los contratos que se usen a la hora de apartarse de los modelos ofrecidos. Estos principios rectores son:

a) Identificación de las partes y lugar del tratamiento: se debe identificar al exportador y al importador de los datos, indicando la jurisdicción donde se ubicará el banco de datos;

b) Definición de términos: en referencia a la Ley N° 25.326, se exige una precisión de los conceptos de "datos personales", "datos sensibles", "tratamiento", "responsable" y "titular del dato"; la Identificación de la "autoridad" o "autoridad de control" con la DNPDP; una referencia al art. 25 de dicha Ley al hablar de la figura del "importador" o "encargado del tratamiento"; la indicación de la "legislación de protección de datos" como la Ley N° 25.326 y normativa reglamentaria; detallar la finalidad y la clase de datos personales que se transfieren, entre otros;

c) Características del tratamiento: las partes deben determinar la naturaleza y características de los datos personales a transferir, la forma en que las partes atenderán los pedidos del titular del dato o de la autoridad de control, las transferencias previstas a terceros, y la jurisdicción en que se radicarán los datos.

d) Designación de terceros beneficiarios: las partes deben designar a los titulares de los datos como terceros beneficiarios, con facultades para exigir el cumplimiento de las disposiciones de la Ley N° 25.326 relacionadas con el tratamiento de sus datos personales –sea ante el Importador como el Exportador y eventualmente subcontratistas– en particular lo relativo a los derechos de acceso, rectificación, supresión y demás derechos.[5] Igualmente, el Importador deberá aceptar que a DNPDP pueda ejercer sus facultades respecto del tratamiento de datos que asuma a su cargo, con los límites y facultades que le otorga la ley,

aceptando sus facultades de control y sanción, otorgándole a tales fines, en lo que resulte pertinente, el carácter de tercero beneficiario.

e) Responsabilidad: el alcance de la responsabilidad del importador encargado del servicio de tratamiento de datos siempre fue una cuestión que mucha inseguridad jurídica generó. Por un lado están quienes se inclinan por una solidaridad del cliente/exportador con el prestador/importador alegando que la prestación de este tipo de servicios supone una especie de cesión de datos personales[6].

Por otro lado, otro sector de la doctrina considera que, lejos de ser solidariamente responsables, el cliente (responsable del banco de datos) y el prestador tienen responsabilidades bien distintas bajo la Ley N° 25.326. "Como el acceso del prestador del servicio no supone la revelación de datos al mismo en los términos en que la norma concibe la cesión, hay que entender que los deberes impuestos a los cesionarios no le son aplicables a quienes traten datos por cuenta de terceros"[7].

El Exportador responderá por los daños que sufran los titulares de los datos como resultado del incumplimiento de las obligaciones pactadas en el contrato, sea por culpa propia o del Importador o subencargado del tratamiento. El titular del dato podrá reclamar asimismo al Importador y/o subencargado cuando el daño les sea imputable.

Este último criterio fue también confirmado en una opinión formal de la DNPDP dictada en Enero de 2014, mediante la cual dicho organismo confirma que la responsabilidad solidaria prevista para la cesión de datos (art. 11, de la Ley N° 25.326) no aplica al tratamiento de datos previsto en el art. 25 de la Ley N° 25.326[8].

f) Legislación aplicable y jurisdicción: El Importador deberá someterse, en lo relativo a la protección de los datos personales, a la Ley Nº 25.326, sus normas reglamentarias y disposiciones de la DNPDP. A su vez, la jurisdicción judicial y administrativa de Argentina entenderán en caso de conflicto vinculado a la protección de datos personales. Esta cláusula se impone en virtud del orden público[9] que tiene la norma (art. 44 de la Ley N° 25.326).

g) Cooperación con las autoridades de control: tanto el Exportador como el Importador deben prever y admitir la posibilidad de que la autoridad de control realice auditorias conforme a la Ley Nº 25.326, poniendo a disposición sus instalaciones de tratamiento de los datos. Tal sometimiento abarca también al subencargado. El Importador de datos informará sin demora al Exportador de datos en el caso de que la legislación existente aplicable a él o a cualquier subencargado no permita auditar al Importador ni a los subencargados.

h) Subtratamiento de datos: El contrato de considera intuitu personae debido a la sensibilidad de los datos y la importancia que detenta la figura del Importador a la hora de inspirar confianza y seguridad en su tratamiento. Es por ello que el Importador de datos no podrá subcontratar ninguna de sus operaciones de procesamiento llevadas a cabo en nombre del Exportador de datos sin previo consentimiento por escrito. En tal caso, el subencargado tendrá que asumir iguales obligaciones que el Importador, en lo que resulte compatible. El Importador de datos seguirá siendo plenamente responsable frente al Exportador de datos del cumplimiento de las obligaciones del subencargado del tratamiento de datos con arreglo a

dicho acuerdo. Este requisito puede verse satisfecho mediante contrato entre Importador y subencargado en el cual este último es cosignatario del contrato.

i) Obligaciones una vez finalizada la prestación de los servicios de tratamiento de los datos personales: tanto el Importador como el subencargado deberán devolver todos los datos personales transferidos y sus copias, o bien destruirlos por completo y certificar esta circunstancia al Exportador, a menos que la legislación aplicable al Importador le impida devolver o destruir total o parcialmente los datos personales transferidos, verificando que dicho plazo de conservación no sea contrario a los principios de protección de datos personales aplicables, y en caso afirmativo se notificará a la autoridad de control[10].

II. Obligaciones del Exportador de datos

Las principales obligaciones del Exportador vienen de la mano de la necesidad de hermetismo en el tratamiento de datos frágiles. La recopilación, el tratamiento y la transferencia de los datos personales se deben efectuar de conformidad con la Ley N° 25.326 y procurar haber informado a los titulares de los datos que su información personal podía ser transferida a un tercer país con niveles inferiores de protección de datos.

Se destaca la necesidad de contratar un seguro de responsabilidad para eventuales perjuicios ocasionados con motivo del tratamiento previsto, en caso de que el Importador no resulte tener solvencia económica acreditada.

En caso de subcontratación, el subencargado deberá contar con la conformidad previa expresa del Exportador y que proporcionará por lo menos el mismo nivel de protección de los datos personales y derechos de los titulares de los datos que los pactados con el Importador, celebrando un contrato a tales fines, y quien estará también bajo las instrucciones del Exportador.

Finalmente, corre con la obligación de poner a disposición de los titulares de los datos, y entregar a petición de estos, una copia de las cláusulas que se relacionen al tratamiento de sus datos personales, derechos y garantías, así como una copia de las cláusulas de eventuales contratos de servicios de subtratamiento de datos que se suscriban.

III. Obligaciones del Importador de datos

El Importador se obliga a tratar los datos personales transferidos solo en nombre del Exportador de datos, de conformidad con sus instrucciones y las cláusulas del contrato, en un marco de absoluta confidencialidad. En caso de que no pueda cumplir estos requisitos, tendrá que informar de ello al Exportador de datos, en tal caso este estará facultado para suspender la transferencia de los datos o rescindir el contrato.

Naturalmente debe garantizar las medidas de seguridad y confidencialidad necesarias y efectivas verificando que no sean inferiores a las dispuestas por la normativa vigente, Disposición DNPDP Nº 11/06, de manera tal que garanticen el nivel de seguridad apropiado a los riesgos que entraña el tratamiento y a la naturaleza de los datos que han de protegerse.

Adicionalmente, debe informar al Exportador de datos en forma inmediata en caso de tener conocimiento de la existencia de alguna disposición que impida el cumplimiento de las

obligaciones, garantías y principios de la Ley Nº 25.326 y demás obligaciones previstas en el contrato, en cuyo caso el Exportador podrá suspender la transferencia.

La DNPDP se reserva la facultad de tener a su disposición, mediante expresa solicitud, las instalaciones de tratamiento de datos del Importador, sus ficheros y toda la documentación necesaria para el tratamiento, a efectos de revisión, auditoría o certificación.

No cederá ni transferirá los datos personales a terceros excepto que: i) se establezca de manera específica en el contrato o resulte necesario para su cumplimiento, verificando en ambos casos que el destinatario se obligue en iguales términos que el Importador en el presente y siempre con el conocimiento y conformidad previa del Exportador, o ii) la cesión sea requerida por ley o autoridad competente, en la medida que no exceda lo necesario en una sociedad democrática. Al recibir la solicitud señalada, el Importador deberá de manera inmediata verificar que la autoridad solicitante ofrezca garantías adecuadas de cumplimiento de los principios de la Ley Nº 25.326. En caso que la autoridad no otorgue u ofrezca las garantías indicadas, prevalecerá la ley argentina, por lo que el Importador procederá a suspender el tratamiento en dicho país reintegrando los datos al Exportador según las instrucciones que este le imparta y notificando este último a la autoridad de control.

Conclusión [arriba]

No cabe duda de que la regulación impartida por la DNPDP es muy bienvenida y útil en nuestra legislación argentina; amen de la importancia que reviste en un mundo globalizado la exportación de datos de manera segura y eficaz.

Sin ser muy rebuscado y para poder ejemplificar, este régimen repercute directamente en nuestra cotidianeidad cuando se utilizan “servicios en la nube”, donde todo el contenido ‘en la nube’ está compuesto por datos personales[11].

Sólo se pueden realizar, libremente y sin autorización alguna, las transferencias que tengan como destinatario un país que ofrezca un nivel de protección equiparable al que se presta en la Ley N° 25.326. Por tanto, el factor clave en la realización de un movimiento internacional de datos es la evaluación del nivel de protección que ofrece el país destinatario. El exportador de los datos debe comprobar si este nivel de protección es equiparable al que se ofrece en la Ley, y de no ser así, deberá recurrir a los principios de las clausulas tipo, al menos.

La nueva Disposición resulta ser más que necesaria a los fines de garantizar la protección de los titulares de esos datos, que hasta no hace mucho tiempo se hallaban sin defensas ex-ante de ocurrido el daño y que resultaban ineficaces dada la internacionalidad del contrato y su desregulación local.

Los principios formulados resultan atinados y aceptables en el mercado de tratamiento informático de datos mundial, ya que los mismos fueron inspirados en el régimen de la Unión Europea, fuente máxima de consulta en la materia.

Cabe concluir la exposición advirtiendo, nuevamente, la importancia del tema a punto tal que las violaciones a estos principios de raigambre internacional son consideradas, con toda razón, como “infracciones muy graves” según la Disposición 9/15 de la DNPDP[12]. Pasibles

de ser aplicables hasta seis apercibimientos, suspensiones, clausura o cancelación del archivo, registro o banco de datos del Exportador y multas de hasta $100.000.

Notas [arriba]

[1] De acuerdo con el concepto amplio de nuestra legislación —que sigue al de la Unión Europea en la materia— se entiende a los datos personales como la “Información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables” (Ley N° 25.326, art. 2º).
[2] Palazzi, Pablo A., Transferencia internacional de datos personales. Nueva regulación de la Dirección Nacional de Protección de Datos Personales. LA LEY AR/DOC/3904/2016.
[3] Decisión 2001/497/CE del 15 de junio de 2001 y la Decisión 2010/87/UE del 5 de febrero de 2010; especialmente esta última en cuanto establece cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países, de conformidad con la Directiva 95/46/CE.
[4] Disp. 60/2016, Cláusula 5 del Anexo I para el caso de cesión; y cláusula 6 del Anexo II para el caso de prestación de servicios.
[5] Derechos contenidos en el Capítulo III, arts. 13 a 20 de la Ley N° 25.326.
[6] El art. 11 inc. 4 de la Ley N° 25.326 indica que "...el cesionario quedará sujeto a las mismas obligaciones legales y reglamentarias del cedente, y éste responderá solidaria y conjuntamente por la observancia de las mismas ante el organismo de control y el titular de los datos de que se trate".
[7] Tanús, Gustavo D., El contrato de prestación de servicios de tratamiento de datos personales (el outsourcing de datos). SJA 28/4/2004; JA, 2004-II-1445.
[8] Nota de la DNPDP 32/2014, de enero de 2014.
[9] Frene, Lisandro, Tratamiento informatizado de datos personales. LA LEY 22/08/2013, 1 • Sup. Act. 22/08/2013, 1.
[10] Conforme surge del inciso K de la Cláusula 4 inserta en el Anexo I de la Disposición N° 60 - E/2016.
[11] Travieso, J. A., La protección de datos personales: problemas y sistemas. LA LEY 08/04/2014, pág. 1.
[12] Conforme punto 3.I) “Transferir datos personales de cualquier tipo a países u organismos internacionales o supranacionales que no proporcionen niveles de protección adecuados, salvo las excepciones legales previstas en el art. 12, inciso 2, de la Ley N° 25.326, sin haber cumplido los demás recaudos legales previstos en la citada ley y su reglamentación”.