LA PROTECCIÓN DE DATOS PERSONALES: UNA HERRAMIENTA PARA PROMOVER LA INVERSIÓN

Héctor Figari Costa[*]

María del Carmen Quiroz Ochoa[**]

La celeridad en las operaciones empresariales es una de sus características más resaltantes. Esto se ha dado como consecuencia de la expansión de las empresas y del desarrollo de la tecnología de la información. Sin embargo, no debemos perder de vista que el derecho a la intimidad de las personas puede ser vulnerado, al compartirse información reservada y privada sin la autorización de su titular. El presente artículo tiene como objetivo determinar si nuestra Ley de Protección de Datos Personales cumple con los estándares internacionales y si, sobre todo, otorga seguridad a los privados.

Los autores sostienen que la Ley de Protección de Datos Personales cumple con la mayoría de requisitos internacionales y otorga la seguridad del caso pero que aún le falta implementar ciertos aspectos. Por ejemplo, delimitar y especificar las sanciones que se han tipificado, que la Autoridad Nacional de Protección de Datos Personales cuente con recursos presupuestarios, que el Reglamento coadyuve al desarrollo de dicha ley, entre otros. Lo central, señalan los autores, es poder brindar seguridad a las personas, sean naturales o jurídicas, y así promover la inversión privada.

[*] Abogado. Magíster en Derecho (LL.M) por la Universidad de Northwestern. Beneficiario de la beca A.L. Raymond Fund Scholarship. Cursos de postgrado "Instituciones Jurídicas del Mercado" y "Derecho de la Electricidad, el Gas y la Energía" ante la Universidad Peruana de Ciencias Aplicadas. Socio del Estudio Muñiz, Ramírez, Pérez-Taiman y Olaya Abogados.

[**] Abogada. Estudio Muñiz, Ramírez, Pérez-Taiman y Olaya Abogados.

La actual expansión empresarial es consecuencia, en gran medida, del avance en la tecnología de la información, dado que facilita la interconexión de los titulares de las distintas bases de datos, reduciendo importantes costos en la recopilación, almacenamiento y demás tratamiento, ofreciendo gran potencial para la generación de negocios, y, por tanto, utilidades e importantes beneficios sociales.

En tal sentido, el intercambio continuo de información es la premisa básica para el desarrollo eficiente de una empresa, lo cual, hasta cierta medida, favorece a la sociedad por la agilidad con la que se realizan las transacciones. Sin embargo, por el mismo motivo, pueden ser vulnerados ciertos derechos fundamentales de las personas tales como el derecho a la intimidad o el de protección a los datos personales, debido a que en cuestión de minutos la información personal de un individuo podría ser utilizada de manera indebida por alguien que no tiene autorización para su tratamiento.

En este contexto, es importante contar con un ordenamiento jurídico que conceda las garantías necesarias a la privacidad de la información de las personas, y que a su vez satisfaga las necesidades empresariales e intereses comerciales de operar en un entorno que los dote de seguridad jurídica, traducida esta en reglas claras de lo que se puede hacer y lo que no se puede hacer, y cuáles son las consecuencias en caso de incumplimiento.

A continuación, realizaremos un breve resumen de las normas y documentos de foros internacionales que influenciaron en nuestra actual Ley de Protección de Datos Personales, y en base a lo establecido principalmente por la legislación europea, determinaremos si el Perú cumple con los estándares internacionales de protección de datos que permita su recepción desde el extranjero, y por lo tanto, que ofrezca un marco seguro y amigable para la inversión extranjera.

I. MARCO GENERAL

La evolución de la tecnología permite la transferencia de gran cantidad de información a través de las fronteras nacionales. Tal situación genera incertidumbre respecto del tratamiento que se le podría estar administrando a dicha información, por lo que la vulneración de los derechos fundamentales, en particular el derecho a la intimidad, es un problema latente.

Ya desde la década de los setenta, la Organización para la Cooperación y el Desarrollo Económico (OCDE) fue la primera organización a nivel mundial en tratar este tema de manera organizada en un documento. En 1980, esta organización elaboró las "Directrices Relativas a la Protección de la Intimidad y de la Circulación Transfronteriza de Datos Personales"[1], que a manera de recomendaciones, dirigidas a los países miembros de dicha organización, sugiere reducir la disparidad en las legislaciones nacionales que pudieran obstaculizar la libre circulación transfronteriza de datos personales, a fin de evitar un perjuicio en ciertos sectores económicos, como la banca y los seguros.

El establecimiento de criterios mínimos de protección de la intimidad y de las libertades individuales busca garantizar la protección de los datos personales tomando como punto de partida el interés mutuo a la libre circulación de la información, eliminando de esta manera la restricción en cuanto al flujo transfronterizo de datos personales por causa de los posibles riesgos asociados a esta actividad. Uno de los valores básicos imprescindibles consagrado en la Directriz es "la libre circulación de los datos personales"; por lo cual, el ámbito de aplicación se circunscribe sólo a aquellos datos cuyo tratamiento efectuado en el sector público o privado presente un peligro para la intimidad y las libertades individuales. En consecuencia, esta norma no le es aplicable a todos los datos considerados personales, sino sólo a aquellos que evidencien algún riesgo para los derechos mencionados.

[1] Adoptada el 23 de septiembre de 1980. En: https://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/organismos_internacionales/ocde/common/pdfs/OCDE-Directrices-sobre-protecci-oo-n-de-privacidad-Trad.pdf.

Posteriormente, la OCDE en su conferencia ministerial "Un Mundo sin Fronteras: Determinación del Potencial del Comercio Electrónico"[2], emitió la "Declaración Ministerial Relativa a la Protección de la Intimidad en las Redes Globales", en la cual los países miembros se comprometieron a tomar las medidas necesarias, dentro del marco de sus respectivos ordenamientos, para garantizar que las Directrices de 1980 sean cumplidas de manera eficaz. Asimismo, reafirmaron el compromiso "(…) relativo a la protección de la intimidad en las redes globales, con el fin de garantizar el respeto de derechos importantes, fomentar la confianza en las redes globales y evitar restricciones innecesarias a los flujos transfronterizos de datos personales."

Como consecuencia de las metas planteadas, las autoridades de cada Estado miembro encargadas de fiscalizar el cumplimiento de las Leyes de Privacidad Nacionales debían de encontrar la manera de cooperar en el intercambio de información para la tramitación de investigaciones, para lo cual el Comité de Políticas de Información, Computación y Comunicación de la OCDE emitió la "Recomendación de la OCDE sobre la Cooperación Transfronteriza en la Aplicación de las Leyes de Protección de la Privacidad", mediante la cual recomienda tomar las medidas necesarias para mejorar los ordenamientos jurídicos nacionales que permitan la cooperación entre autoridades extranjeras, y el desarrollo de mecanismos internacionales efectivos que faciliten el cumplimiento de las leyes nacionales en el extremo referente al flujo transfronterizo de datos personales, entre otros aspectos relacionados[3].

En el mismo sentido, la Organización de las Naciones Unidas (ONU) mediante la Resolución 45/95 de la Asamblea General del 14 de diciembre de 1990, adoptó las "Directrices para la Regulación de los Archivos de Datos Personales Informatizados", cuyos lineamientos son de aplicación a los archivos informáticos públicos y privados, así como también, de manera facultativa, a los archivos manuales y archivos relativos a personas jurídicas, especialmente cuando contengan información relativa a los individuos.

Cabe advertir que si bien algunos de los principios establecidos por la ONU son similares a los establecidos por la OCDE, las Directrices de 1990 son de aplicación de manera general a todos los datos personales, no importando si con su tratamiento se vulnera el derecho a la intimidad o las libertades individuales.

Sin perjuicio de lo mencionado en el párrafo anterior, y respecto del flujo transfronterizo de datos, las Directrices de la Organización de Naciones Unidas también incentivan la libre circulación de datos personales estableciendo que, "Cuando la legislación de dos o más países afectados por un flujo transfronterizo de datos ofrezca salvaguardas similares para la protección de la intimidad, la información debe poder circular tan libremente como dentro de cada uno de los territorios afectados. En caso de que no existan salvaguardas recíprocas, no deberán imponerse limitaciones indebidas a tal circulación, sino solamente en la medida en que lo exija la protección de la intimidad".

En tal sentido, la ONU ha tratado de continuar con el criterio establecido por la OCDE incentivando la libre circulación de datos personales. Sin embargo, las Directrices de la ONU van más allá, pues no exigen un nivel de protección adecuado en el país destinatario de los datos, ni siquiera un nivel de protección equiparable al emisor del flujo, la sola permisibilidad radica en la no vulneración al derecho a la intimidad.

Otra singularidad introducida en las Directrices es la inclusión dentro del ámbito de aplicación de la norma, de manera específica, a aquellos archivos de datos personales mantenidos por organizaciones internacionales gubernamentales. Adicionalmente, se estableció la posibilidad de preverse una cláusula por la cual un archivo

[2] Declaración Ministerial relativa a la protección de la intimidad en las redes globales. Ottawa, 7-9 de octubre de 1998. En:https://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/organismos_internacionales/ocde/common/pdfs/C.10-cp--Declaraci-oo-n-ministerial-Ottawa.pdf.

[3] Organización para la Cooperación y el Desarrollo Económico (OCDE). Recomendación relativa transfronteriza de cooperación en la aplicación de las leyes que protegen la intimidad. 12 de junio de 2007. p. 7. En: http://www.oecd.org/dataoecd/43/28/38770483.pdf.

se encuentra exento del cumplimiento de los principios contenidos en la Directriz cuando medien razones sustentadas en la protección de los derechos humanos y las libertades fundamentales de la persona afectada o la ayuda humanitaria (cláusula humanitaria).

Posteriormente, en concordancia con los valores básicos de los Lineamientos de Protección de la Privacidad y Flujos Transfronterizos de Datos Personales de 1980 de la OCDE, el Foro de Cooperación Económica Asia Pacífico (APEC) aprobó en noviembre de 2004 un Marco de Privacidad con la intención de proporcionar una clara orientación a las empresas que se desarrollan dentro de las economías de APEC, sobre los asuntos de privacidad y las repercusiones de este tema sobre su negocio, enfocando tal análisis desde la perspectiva del consumidor y la expectativa que éste tiene sobre las empresas en el manejo de su información con respeto de sus derechos fundamentales.

El Marco de Privacidad diseñado por APEC consta de nueve principios guías, que fueron desarrollados reconociendo la importancia de[4]:

a) Desarrollar protecciones apropiadas para la información personal, particularmente contra las dañinas consecuencias de intrusiones no deseadas y del uso incorrecto de la información personal.

b) Reconocer el libre flujo de información como algo esencial para economías de mercado desarrolladas y en desarrollo, para sustentar el crecimiento económico y social.

c) Propiciar organizaciones globales que recopilen, accedan, usen o procesen información en Economías de APEC para desarrollar e implementar enfoques uniformes dentro de sus organizaciones para tener acceso global y uso de la información personal.

d) Posibilitar agencias de seguridad para cumplir con su mandato de proteger la privacidad de la información.

e) Presentar mecanismos internacionales para promover y hacer cumplir la privacidad de la información, y mantener la continuidad de los flujos de información entre economías de APEC y sus socios comerciales.

Estos principios guías giran en torno a lo siguiente:

a) Evitar daños causados por el mal uso de la información personal.
b) Información.
c) Limitación en la recolección a lo estrictamente necesario.
d) Limitación en el uso de la información.
e) Derecho de decisión del titular de la información sobre el destino de la misma.
f) Integridad y exactitud de la información.
g) Medidas de protección de la información.
h) Derecho de acceso y corrección de los titulares.
i) Responsabilidad en caso de incumplimiento.

Con el fin de lograr los objetivos mencionados, en septiembre de 2007[5] las economías de APEC aprobaron un documento denominado "*APEC Data Privacy Pathfinder"* que busca implementar el Marco de Privacidad aprobado en el 2004 en relación al flujo transfronterizo de información personal. En dicho docu-mento, las economías se comprometen a trabajar conjuntamente para crear marcos de aplicación y cumplimiento de un sistema de reglas de privacidad para el flujo transfronterizo entre las economías de la región, así como promover procesos de consulta que involucren a las partes interesadas tanto en la creación normativa como en su implementación.

[4] Foro de Cooperación Económica Asia Pacífico (APEC). Marco de Privacidad. 16ª Reunión Ministerial APEC. Santiago, Chile. 17-18 de noviembre de 2004. Parte I. Preámbulo. Párrafo 8. 29 de octubre de 2004. p.4. En: http://www.nacpec.org/docs/APEC_Privacy_Framework.pdf

[5] Foro de Cooperación Económica Asia Pacífico (APEC), Directrices de Datos Personales. Concluyendo la reunión de altos funcionarios. Sydney, Australia. 2 y 3 de septiembre de 2007. p. 2. En: http//aimp.apec.org/.../SOM/CSOM/07_csom_019.doc.

En este contexto, el subgrupo APEC de Privacidad de los Datos (DPS por sus siglas en inglés) desarrolló un Sistema de Reglas de Privacidad Transfronteriza (CBPR por sus siglas en inglés)[6] que va dirigido a las organizaciones que deseen desarrollar prácticas y políticas de privacidad que estén en concordancia con los principios guías del Marco de Privacidad APEC. Dichas prácticas y políticas serán evaluadas por una autoridad acreditada (*"Accountability Agent")* que certificará que las organizaciones cumplan con los requerimientos exigidos por el sistema. Una vez obtenida la certificación, las políticas y prácticas serán de obligatorio cumplimiento para dichas organizaciones[7]. No obstante, las Economías miembro de APEC sólo podrán ser consideradas participantes del Sistema CBPR después de cumplir con ciertas condiciones[8].

Finalmente, a nivel sudamericano, la Red Iberoamericana de Datos Personales[9] ha diseñado las "Directrices para la Armonización de la Protección de Datos en la Comunidad Iberoamericana", cuyo ámbito de aplicación abarca todo tratamiento manual o automatizado de datos de carácter personal, que permite la identificación de las personas físicas en el sector público y privado. Están exentos aquellos datos a los que se brinda un tratamiento manual o no automatizado, y que no son incorporados en ficheros cuyos criterios permitan la identificación de las personas mediante los datos personales proporcionados, o que sean tratados por una persona para sus fines personales o familiares[10].

El objetivo de tales Directrices es establecer una serie de principios básicos que todo ordenamiento jurídico de datos personales debe contener para permitir el tratamiento de datos personales, entre ellos el flujo transfronterizo, debiendo destinarse a países que cumplan con dichos principios. Sin embargo, establece la posibilidad de permitir el flujo transfronterizo, de manera excepcional, en el caso de que las leyes nacionales lo establezcan, teniendo en cuenta los derechos e intereses del afectado, y mientras este haya prestado su consentimiento, o cuando una autoridad competente lo disponga.

Como puede apreciarse, la importancia de la protección al derecho a la intimidad y al derecho a la protección de los datos personales ha sido reconocida en diversos foros y documentos internacionales respecto del flujo transfronterizo de datos, enfocando su protección en la necesidad de

6 Si bien el Sistema de Reglas de Privacidad Transfronteriza fue aprobado por el Subgrupo APEC de Privacidad de los Datos (DPS), este actualmente no ha sido implementado. Esta situación fue reportada en el Documento "Reunión APEC del Subgrupo de Privacidad de los Datos. San Francisco, del 16 al 18 de setiembre de 2011. Reporte del Observador" para la 33ª Conferencia Internacional de los Comisionados de Protección de Datos y Privacidad. Presentado en octubre de 2011. p. 3.
En: http://www.privacyconference2011.org/htmls/adoptedResolutions/2011_Mexico/2011_OBS_R_002_APEC_Rpte_Obs_ESP.pdf.

7 Foro de Cooperación Económica Asia Pacífico (APEC), Sistema de Reglas de Privacidad Transfronteriza (CBPR por sus siglas en inglés) – Políticas, normas y directrices. Subgrupo de Privacidad de los Datos. Reunión en San Francisco, Estados Unidos de Norteamérica. 18 de septiembre de 2011. p. 4.
En: http://aimp.apec.org/Documents/2011/ECSG/DPS2/11_ecsg_dps2_009.pdf.

8 Foro de Cooperación Económica Asia Pacífico (APEC), Sistema de Reglas de Privacidad Transfronteriza (CBPR por sus siglas en inglés) – Políticas, normas y directrices. Anexo A. Párrafo 2.2.- "An APEC Member Economy is considered a Participant in the Cross Border Privacy Rules (CBPR) System (CBPR Participant), after the Chair of the Electronic Commerce Steering Group (ECSG Chair) has notified the Economy that the following conditions have been met: (i) The Economy's ECSG delegation, or appropriate governmental representative, submits to the ECSG Chair a letter indicating its intention to participate and confirming that at least one Privacy Enforcement Authority in that Economy is a participant in the APEC Cross Border Privacy Enforcement Arrangement (CPEA); (ii) The Economy indicates its intention to make use of at least one APEC-recognized Accountability Agent subject to the procedures outlined in paragraph 6.2; (iii) The Economy's ECSG delegation, or appropriate governmental representative, after consulting with the Joint Oversight Panel, submits to the Chair of the ECSG an explanation of how the CBPR system program requirements may be enforced in that Economy; and (iv)The Joint Oversight Panel submits to the Chair of the ECSG a report as to how the conditions in (i)-(iii) above have been satisfied". p. 15.

9 Con motivo de la Cumbre Iberoamerica de Jefes de Estado y de Gobierno, de fecha 30 y 31 de mayo de 2007, se suscribió la Declaración de Santa Cruz de la Sierra, en la cual se reconoce la protección de datos personales como derecho fundamental y destaca las iniciativas regulatorias para tal efecto.

10 Directrices para la armonización de la protección de datos en la Comunidad Iberoamericana". Red Iberoamercana de Protección de Datos. p. 13.
En: http://www.redipd.org/reuniones/encuentros/V/common/9_nov/Directrices_de_armonizacion.pdf.

cooperación entre países para coadyuvar al cumplimiento de las leyes de protección de datos nacionales, o imponiendo marcos generales de armonización legislativa que contribuyan a otorgar mayor seguridad en dicho flujo transfronterizo. De esta manera se reducen los potenciales riesgos que implica el avance de la tecnología de la información, y la relación entre legislaciones que pueden ser disímiles, garantizando el desarrollo comercial y a la vez brindando al consumidor mayor confianza y seguridad en sus transacciones.

II. DIRECTIVA UE 95/46/CE DEL PARLAMENTO EUROPEO Y DEL CONSEJO DEL 24 DE OCTUBRE DE 1995 RELATIVA A LA PROTECCIÓN DE LAS PERSONAS FÍSICAS EN LO QUE RESPECTA AL TRATAMIENTO DE LOS DATOS PERSONALES Y LA LIBRE CIRCULACIÓN DE ESTOS

Creemos necesario realizar un acercamiento general sobre la Directiva UE 95/46/CE (en adelante, Directiva), pues consideramos que ha sido uno de los referentes más influyentes en la regulación del derecho a la protección de los datos personales de nuestra legislación.

La Directiva reconoce que la libre circulación de datos personales entre los países miembros es necesaria para cumplir con los objetivos del Tratado Constitutivo de la Comunidad Europea[11], especialmente para el establecimiento y funcionamiento del mercado interior[12]. Para lograr dicha finalidad, es necesario eliminar los obstáculos a la circulación de datos personales causados por las diferencias entre los niveles de protección de los derechos y las libertades de las personas, particularmente el derecho a la intimidad. Esta diferencia surge como consecuencia de la disparidad existente entre los ordenamientos nacionales, lo cual constituye un impedimento para el ejercicio de actividades económicas a escala comunitaria. En tal sentido, los estados miembros disponen de un "margen de maniobra" establecido por la Directiva, según el cual los ordenamientos nacionales podrán realizar una aproximación entre ellos para lograr una protección equivalente de los derechos fundamentales que no dificulte el desplazamiento de información personal[13].

En esta línea, la Directiva en el artículo 25.1[14] dispone que el flujo transfronterizo de datos personales de aquellos que sean objeto de tratamiento o destinados a ser objeto de tratamiento, sólo puede ser efectuado si el país destinatario garantiza un nivel de protección adecuado. El apartado 2[15] prescribe que el carácter de "nivel adecuado" deberá ser evaluado en cada caso, teniendo en consideración las circunstancias particulares que se presenten en la transferencia y la categoría de datos.

Al respecto, el Grupo de Trabajo sobre la protección de las personas físicas en lo que respecta al tratamiento de datos personales[16] (en

11 Tratado de Funcionamiento de la Unión Europea.
En: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:083:0013:0046:es:PDF.

12 Tratado de Funcionamiento de la Unión Europea:
"Artículo 26.2.-
El mercado interior implicará un espacio sin fronteras interiores, en el que la libre circulación de mercancías, personas, servicios y capitales estará garantizada de acuerdo con las disposiciones de los Tratados".

13 Directiva UE 95/46/CE. Parte expositiva. Numerales 6, 7, 8, 9.

14 Directiva UE 95/46/CE:
"Artículo 25. 1.-
Los Estados miembros dispondrán que la transferencia a un país tercero de datos personales que sean objeto de tratamiento o destinados a ser objeto de tratamiento con posterioridad a su transferencia, únicamente pueda efectuarse cuando, sin perjuicio del cumplimiento de las disposiciones de Derecho nacional adoptadas con arreglo a las demás disposiciones de la presente Directiva, el país tercero de que se trate garantice un nivel de protección adecuado".

15 Directiva UE 95/46/CE:
"Artículo 25.2.-
El carácter de adecuado del nivel de protección que ofrece un país tercero se evaluará atendiendo a todas las circunstancias que concurran en una transferencia o en una categoría de transferencia de datos; en particular, se tomará en consideración la naturaleza de los datos, la finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, las normas de Derecho, generales o sectoriales, vigentes en el país tercero de que se trate, así como las normas profesionales y las medidas de seguridad en vigor en dichos países".

adelante, Grupo de Trabajo), ha establecido dos criterios de evaluación para determinar si el país receptor de los datos personales cuenta con un nivel de protección adecuado: "el contenido de las normas aplicables y los medios para asegurar su aplicación eficaz". Según el documento de trabajo, "debería ser posible lograr un "núcleo" de principios de "contenido" de protección de datos y de requisitos "de procedimiento/ de aplicación", cuyo cumplimiento pudiera considerarse un requisito mínimo para juzgar adecuada la protección"[17].

Es así, que desde el punto de vista normativo, el Grupo de Trabajo ha sugerido incluir en los ordenamientos nacionales una serie de principios básicos que determinen el nivel de seguridad mínimo para asegurar que el tratamiento en el país receptor no vulnere los derechos fundamentales. Dichos principios son los siguientes[18]:

a) Principio de limitación de objetivo: el tratamiento de los datos debe realizarse con un objetivo específico, y la posterior utilización o transferencia no debe ser incompatible con el objetivo inicial de la transferencia. Salvo excepciones[19].

b) Principio de proporcionalidad y de calidad de los datos: los datos deben ser exactos, y cuando sea necesario, deben estar actualizados. Asimismo, deben ser adecuados, pertinentes y no excesivos para el objetivo por el que se transfieren o tratan posteriormente.

c) Principio de transparencia: los interesados deben ser informados acerca del objetivo del tratamiento y la identidad del responsable de dicha acción en el país destinatario del flujo, o de algún otro elemento necesario que garantice un trato leal. Salvo excepciones[20].

d) Principios de seguridad: el responsable del tratamiento debe adoptar las medidas técnicas y organizativas adecuadas respecto a los riesgos inherentes al tratamiento. Toda persona que actúe bajo la autoridad del responsable del tratamiento (entidad capacitada para decidir los fines del tratamiento), incluido el responsable del tratamiento (prestador material del servicio) no debe efectuar el tratamiento salvo por instrucción del primero.

e) Derecho de acceso, rectificación y oposición: el titular de los datos debe tener el derecho a obtener una copia de los datos que de él se traten, así como rectificar aquellos que resulten inexactos. De igual manera, debe poder oponerse a su tratamiento. Salvo excepciones[21].

f) Restricciones respecto a transferencias sucesivas a otros terceros países: las transferencias sucesivas sólo podrán efectuarse en tanto los países receptores de los datos garanticen un nivel de protección adecuado. Salvo excepciones[22].

Adicionalmente, el Grupo de trabajo ha establecido tres principios adicionales a ser aplicados respecto al tipo de tratamiento:

a) Datos sensibles[23]: para esta categoría de datos se debe establecer protecciones adicionales.

b) Mercadotecnia directa: en el caso de que el objetivo de la transferencia de datos sea la mercadotecnia directa, en cualquier momento el titular puede negar que sus datos sean utilizados para ello.

c) Decisión individual automatizada[24]: cuando la finalidad del flujo

16 Documento de Trabajo: "Transferencia de datos personales a terceros países, aplicación de los artículos 25 y 26 de la Directiva sobre protección de datos de la UE". Aprobado por el Grupo de Trabajo sobre la protección de las personas físicas en lo que respecta al tratamiento de datos personales el 24 de julio de 1998.

17 Ibíd. p. 5.

18 Ibíd. p. 6-7.

19 Directiva UE 95/46/CE. Artículo 13.

20 Directiva UE 95/46/CE. Artículos 11.2 y 13.

21 Directiva UE 95/46/CE. Artículo 13.

22 Directiva UE 95/46/CE. Artículo 26.1.

23 Según el artículo 8 de la Directiva, son considerados datos sensibles aquellos "datos personales que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, las permanencia a sindicatos, así como el tratamiento de los datos relativos a la salud o sexualidad".

transfronterizo sea una decisión individual automatizada, el interesado tendrá derecho a conocer el motivo de tal decisión y deberá protegerse el interés legítimo del interesado.

Por otro lado, en cuanto a Mecanismos de procedimiento/de aplicación, el Grupo de Trabajo señala que es de amplio consenso "que un sistema de **supervisión externa** en forma de autoridad independiente es una característica necesaria de un sistema de cumplimiento de la protección de datos" [El énfasis es nuestro]; por lo cual, diferencia tres objetivos básicos sobre los cuales se podría valorar los procedimientos establecidos para el cumplimiento de la legislación de protección de datos personales. Dichos objetivos son[25]:

a) Ofrecer un nivel satisfactorio de cumplimiento de las normas: se caracteriza por el conocimiento de las obligaciones y derechos por parte de los responsables del tratamiento y los interesados, respectivamente. Asimismo, por la aplicación de sanciones efectivas y disuasorias, además de una fiscalización eficiente por parte de la autoridad.

b) Ofrecer apoyo y asistencia a los interesados en el ejercicio de sus derechos: se debe normar un tipo de mecanismo institucional que permita investigar denuncias en forma independiente, permitiendo que los interesados reclamen sus derechos sin generarles costos excesivos.

c) Ofrecer vías adecuadas de recurso a quienes resulten perjudicados en el caso de que no se observen las normas: el sistema debe de ofrecer la posibilidad de obtener resoluciones judiciales o arbitrales, y cuando sea pertinente, indemnizaciones y sanciones.

Ahora bien, la Directiva ha establecido en su artículo 26.2[26] una excepción al principio de nivel de protección adecuado, dicha excepción establece que un Estado miembro puede autorizar la transferencia en tanto el responsable del tratamiento ofrezca las garantías suficientes para el respeto de los derechos fundamentales y para el ejercicio de estos derechos. Asimismo, el artículo 26.4[27] otorga la facultad a la Comisión para que determine cuales son las cláusulas tipo que cumplen con las garantías suficientes para efectuar el flujo transfronterizo.

Sobre este aspecto cabe advertir que las cláusulas contractuales dentro del contexto comunitario persiguen una finalidad diferente a las cláusulas establecidas entre un país miembro y un tercero. En el primer escenario, el objetivo de una cláusula contractual es la repartición de responsabilidad entre la entidad responsable del tratamiento (aquella que decide sobre la

[24] Según el artículo 15 de la Directiva, los Estados Miembros "reconocerán a las personas a no verse sometidas a una decisión con efectos jurídicos sobre ellas o que les afecte de manera significativa, que se base únicamente en un tratamiento automatizado de datos (…)". Sin embargo, los Estados Miembros pueden permitir que dichas decisiones sean permitidas cuando: "a) se haya adoptado en el marco de una celebración o ejecución de un contrato, siempre que la petición de celebración o ejecución del contrato presentada por el interesado se haya satisfecho o que existan medidas apropiadas, como la posibilidad de defender su punto de vista, para salvaguardia de su interés legítimo; o b) esté autorizado por una ley que establezca medidas que garanticen el interés legítimo del interesado".

[25] Documento de Trabajo: "Transferencia de datos personales a terceros países, aplicación de los artículos 25 y 26 de la Directiva sobre protección de datos de la UE". Op. cit. p. 7-8.

[26] Directiva UE 95/46/CE:
"Artículo 26 apartado 2.-
(…) Los Estados miembros podrán autorizar una transferencia o una serie de transferencias de datos personales a un tercer país que no garantice un nivel de protección adecuado (…), cuando el responsable del tratamiento ofrezca garantías suficientes respecto de la protección de la vida privada, de los derechos y libertados fundamentales de las personas, así como el respeto al ejercicio de los respectivos derechos; dichas garantías podrán derivarse, en particular, de cláusulas contractuales apropiadas".

[27] Directiva UE 95/46/CE:
"Artículo 26.4.-
Cuando la Comisión decida (…) qué determinadas cláusulas contractuales tipo ofrecen las garantías suficientes establecidas en el apartado 2, los estados miembros adoptarán las medidas necesarias para ajustarse a la decisión de la Comisión".

finalidad y medios para el tratamiento) y el encargado del tratamiento (aquel que presta materialmente el servicio). En este contexto, el responsable del tratamiento asume responsabilidad por el cumplimiento de los principios, y el encargado sólo es responsable por la seguridad de los datos[28].

Sin embargo, respecto de la transferencia de datos de un país miembro de la comunidad a un país tercero, si bien es importante que el contrato establezca responsabilidades, su función primordial es establecer garantías para la protección de los derechos del titular de los datos, en los casos en los que el país receptor no cuente con un marco normativo que proporcione las garantías apropiadas[29].

Frente a tal situación, se sugiere que las soluciones contractuales deben proponer un marco que establezca, por lo menos, los principios básicos establecidos para evaluar un nivel de protección adecuado. De igual forma, debe preverse los criterios establecidos para evaluar la efectividad en el cumplimiento de las legislaciones de datos personales (nivel satisfactorio de cumplimiento, apoyo y asistencia a los interesados y vías adecuadas de recursos). Si bien establecer dichos objetivos de manera contractual es una tarea complicada, el Documento de Trabajo señala posibles soluciones[30], por ejemplo:

a) Para proporcionar vías de disposición de recurso a los interesados, se sugiere que en el caso de existir un responsable del tratamiento y un encargado, se establezca en el contrato que los recursos aplicables son aquellos que pertenecen a la legislación del responsable[31]. Sin embargo, pueden presentarse supuestos en los que el receptor de los datos actúa como responsable de los mismos, para lo cual puede ser establecida una cláusula arbitral, entre otras soluciones.

b) Para brindar apoyo y asistencia a los interesados, propone que se redacte una cláusula mediante la cual una autoridad supervisora de un Estado miembro fiscalice el tratamiento realizado por el encargado en el tercer país. Sin embargo, el Grupo de Trabajo admite que es difícil determinar si dicha posibilidad resulta práctica o viable.

c) Para medir el nivel satisfactorio de cumplimiento, se sugiere que mediante contrato se pacte la posibilidad de fiscalización externa por parte de un organismo de normalización o una empresa especializada.

Las soluciones contractuales no siempre pueden resultar apropiadas para la categoría o volumen de datos que se pretende transferir; sin embargo, consideramos que para transacciones frecuentes entre grandes transnacionales, dicha solución puede ser eficiente y brindar las garantías adecuadas, debido a que dichos organismos se encuentran frente a mayor exposición para que se realice un control eficiente sobre ellos.

Como veremos, muchas de las figuras de la Directiva han sido incorporadas en la legislación peruana. Si bien nuestra legislación no determina lo que podría entenderse como un nivel de protección adecuado, el modelo Europeo nos brinda buenos referentes.

En nuestra legislación, es considerada también como una excepción al principio de nivel de protección adecuado la transferencia

[28] Directiva UE 95/46/CE:
"Artículo 17.3.-
La realización de tratamientos por encargo deberá estar regulada por un contrato u otro acto jurídico que vincule al encargado del tratamiento con el responsable del tratamiento, y que disponga, en particular: - que el encargado del tratamiento solo actúa siguiendo instrucciones del responsable del tratamiento; - que las obligaciones del apartado 1 [adopción medidas técnicas y de organización adecuadas por parte del responsable], tal como las define la legislación del estado miembro en el que está establecido el encargado, incumben también a este" (Corchetes agregados).

[29] Documento de Trabajo: Transferencia de datos personales a terceros países: aplicación de los artículos 25 y 26 de la Directiva sobre protección de datos de la Unión Europea. Op. cit. p. 17.

[30] Ibíd. pp. 19-22.

[31] Este objetivo ha encontrado solución en el Proyecto de Reglamento de la Ley de Datos Personales peruana –Ley 29733–, que prescribe entre sus disposiciones generales, artículo 17, para la transferencia de Datos Personales que "(…) Aquél a quien se transfieran los datos personales se obliga, por el solo hecho de la transferencia, a la observancia de las disposiciones de la Ley y del presente reglamento".

de datos hacia aquellos países que no cuenten con este, en tanto el emisor del flujo otorgue las garantías suficientes para que el tratamiento se efectúe conforme a la Ley. En este caso, las soluciones contractuales resultan oportunas, como bien lo dispone el Proyecto de Reglamento de la Ley de Protección de Datos Personales peruana[32].

III. LA PROTECCIÓN DE LOS DATOS PERSONALES EN LA LEGISLACIÓN PERUANA

El 3 de julio del año 2011 se publicó la Ley 29733 –Ley de Protección de los Datos Personales–, que tiene como objetivo regular el tratamiento de estos dentro del territorio nacional. Si bien dicha Ley es una novedad en nuestra legislación, la protección al derecho fundamental a la protección de los datos personales o autodeterminación informativa[33] no ha sido ajena a nuestro ordenamiento.

En efecto, el artículo 2 inciso 6 de la Constitución Política del Perú de 1993 establece como derecho fundamental "(…) que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar". Para garantizar la vigencia efectiva de tal derecho, se reguló el denominado proceso de *Hábeas Data*, que otorga legitimidad a cualquier persona para acudir a la autoridad con el fin de "Conocer, actualizar, incluir y suprimir o rectificar la información o datos referidos a su persona que se encuentren almacenados o registrados en forma manual, mecánica o informática, en archivos, bancos de datos o registros de entidades públicas o de instituciones privadas que brinden servicio o acceso a terceros. Asimismo, a hacer suprimir o impedir que se suministren datos o informaciones de carácter sensible o privado que afecten derechos constitucionales".

Si bien el derecho a la protección de los datos personales se encuentra fuertemente vinculado con el derecho a la intimidad, el Tribunal Constitucional ha señalado una clara diferencia entre ambos, lo cual denota la importancia de contar con un ordenamiento especial que lo resguarde de manera más eficiente.

Al respecto, el Tribunal Constitucional[34] ha reconocido que: "3. El derecho reconocido en el inciso 6) del artículo 2 de la Constitución es denominado por la doctrina derecho a la autodeterminación informativa y tiene por objeto proteger la intimidad, personal o familiar, la imagen y la identidad frente al peligro que representa el uso y la eventual manipulación de los datos a través de los ordenadores electrónicos. Por otro lado, aunque su objeto sea la protección de la intimidad, el derecho a la autodeterminación informativa no puede identificarse con el derecho a la intimidad, personal o familiar, reconocido, a su vez, por el inciso 7 del mismo artículo 2 de la Constitución. Ello se debe a que mientras que éste protege el derecho a la vida privada, esto es, el poder jurídico de rechazar intromisiones ilegítimas en la vida íntima o familiar de las personas, aquel garantiza la facultad de todo individuo de poder preservarla controlando el registro, uso y revelación de los datos que les conciernen (…)".

Teniendo en cuenta lo establecido en los diferentes rangos de normas y de manera jurisprudencial, es preciso que se adopten las medidas necesarias para salvaguardar los derechos reconocidos. Por tal motivo, y con el objetivo de obtener mayor competitividad a nivel internacional, es que se promulga la Ley de Protección de los Datos Personales, que podría proveernos de mecanismos adecuados para garantizar el respeto al derecho fundamental a la autodeterminación informativa, y a su vez responder a la necesidad de permitir el uso y transferencia de la información para el desarrollo de las actividades comerciales.

[32] Proyecto de Reglamento de la Ley 29733 –Ley de Protección de Datos Personales:
"Artículo 25.- Formalización del Flujo transfronterizo.
(…) el emisor o exportador podrá valerse de cláusulas contractuales u otros instrumentos jurídicos en los que se establezcan cuando menos las mismas obligaciones a las que se encuentra sujeto, así como las condiciones en las que el titular consintió el tratamiento de sus datos personales".

[33] Término utilizado por primera vez en la Sentencia del Tribunal Constitucional Alemán el 15 de diciembre de 1983, que declara la inconstitucionalidad parcial de la Ley Alemana de Censo de la Población de 1982

[34] Sentencia del Tribunal Constitucional recaída en el expediente 1797-2002-HD/TC del 29 de enero de 2003.

A. Disposiciones acerca del consentimiento

La Ley de Protección de Datos Personales es de aplicación a todos los datos personales contenidos o destinados a ser contenidos en bancos de datos personales de administración pública o privada, cuyo tratamiento es efectuado en territorio nacional[35]. Para efectuar su tratamiento[36], es necesario que el titular del banco de datos personales[37] cuente con el consentimiento del titular de estos, el cual debe ser previo, informado, expreso e inequívoco. En el caso de datos sensibles[38], dicho consentimiento se efectuará además por escrito. Nuestro código civil dispone en el artículo 141 que la manifestación de voluntad "(…) Es expresa cuando se realiza en forma oral o escrita, a través de cualquier medio directo, manual, mecánico, electrónico u otro análogo."

No obstante, el Proyecto de Reglamento de la Ley 29733 (en adelante, Proyecto de Reglamento) pretendiendo sobre regular las condiciones para el tratamiento de los datos, describe de manera anecdótica como cada uno de los requisitos del consentimiento debe ser otorgado[39]. Sin embargo, coincidimos en que el consentimiento será libre en tanto "no medie error mala fe, violencia o dolo que puedan afectar la manifestación de la voluntad del titular de los datos (…)", será previo cuando fue otorgado anteriormente "(…) a la recopilación, o en su caso, anterior al tratamiento distinto a aquel por el cual ya se recopilaron".

Acerca de las características "expreso e inequívoco", el Proyecto de Reglamento dispone que se cumplirá con esta condición en tanto "el consentimiento haya sido manifestado en condiciones que no admitan dudas de su otorgamiento", asimismo expresa que puede ser otorgado de forma verbal o escrita. De igual manera, menciona que "La condición de expreso no se limita a la manifestación verbal o escrita. Evaluando con criterio restrictivo y siempre de acuerdo con lo dispuesto por el artículo 7[40] de dicho reglamento, se considerará consentimiento expreso a aquel que se manifieste mediante la conducta del titular que evidencie directamente que ha consentido, dado que de lo contrario su conducta necesariamente hubiera sido otra".

Sobre este último aspecto, consideramos que es acertada la posición del legislador respecto

35 Sin embargo, la Ley excluye del ámbito de aplicación a los siguientes datos personales: "1) A los contenidos o destinados a ser contenidos en banco de datos personales creados por personas naturales para fines exclusivamente relacionados con su vida privada o familiar. 2) A los contenidos o destinados a ser contenidos en bancos de datos de administración pública, solo en tanto su tratamiento resulte necesario para el estricto cumplimiento de las competencias asignadas por ley a las respectivas entidades públicas, para la defensa nacional, seguridad pública, y para el desarrollo de actividades en materia penal para la investigación y represión del delito" (artículo 3).

36 Ley 29733 –Ley de Protección de Datos Personales:
"Artículo 2. 17.- Tratamiento de datos personales.
Cualquier operación o procedimiento técnico, automatizado o no, que permite la recopilación, registro, organización, almacenamiento, conservación, elaboración , modificación, extracción, consulta, utilización, bloqueo, supresión, comunicación por transferencia o por difusión o cualquier otra forma de procesamiento que facilite el acceso, correlación o interconexión de los datos personales".

37 Ley 29733 –Ley de Protección de Datos Personales:
"Artículo 2.15.- Titular del banco de datos personales.
Persona natural, persona jurídica de derecho privado o entidad pública que determina la finalidad y contenido del banco de datos personales, el tratamiento de estos y las medidas de seguridad".

38 Ley 29733 –Ley de Protección de Datos Personales:
"Artículo 2.5.- Datos sensibles.
Datos personales constituidos por los datos biométricos que por sí mismos pueden identificar a su titular; datos referidos al origen racial o étnico; ingresos económicos, opiniones o convicciones políticas, religiosas, filosóficas o morales; afiliación sindical; e información relacionada a la salud y vida sexual".

39 Artículo 12 del Proyecto de Reglamento de la Ley 29733 –Ley de Protección de Datos Personales.

40 Proyecto de Reglamento de la Ley 29733 –Ley de Protección de Datos Personales:
"Artículo 7.- Consentimiento.
En atención al principio de consentimiento el tratamiento de los datos personales es lícito cuando el titular hubiere prestado su consentimiento libre, previo, expreso, informado e inequívoco. No se admiten fórmulas de consentimiento en las que este no sea expresado de forma directa, como aquellas en las que se requiere presumir, o asumir la existencia de una voluntad que no ha sido expresa. Incluso el consentimiento prestado con otras declaraciones, deberá figurar de forma expresa y clara".

a tratar el concepto de "expreso" como "inequívoco". En otras palabras, la rigidez con la que fue redactada la Ley no permitía que el titular del banco de datos personales efectúe un tratamiento acorde con las necesidades del mercado actual, debido a que para cada transferencia de información para llevar a cabo una finalidad determinada se necesitaba del consentimiento "expreso" del titular, lo cual provocaba mayores costos en las transacciones que son traspasados a los consumidores en su perjuicio, y que a su vez contravienen el principio de libre circulación de los datos personales, que si bien no se encuentra explícitamente señalado en nuestro ordenamiento, es un valor fundamental para el desarrollo económico y social a través de la tecnología de la información.

En la misma línea, consideramos que es otro acierto haber considerado como expresa la manifestación realizada a través de "hacer *click*", "clickear", "pinchar", "dar un toque", "*touch*" o "*pad*", ya que con este precepto queda absuelta la duda en cuanto al otorgamiento de consentimiento en el entorno digital, en el cual es más relevante. Adicionalmente, la norma dispone que dicha manifestación constituye una manifestación escrita; sin embargo, para el caso de los datos sensibles dicho mecanismo debe de contar con un mecanismo de autentificación que garantice la voluntad inequívoca del titular[41].

Finalmente, se considerará que el consentimiento es "informado" cuando al titular se le comunique de manera clara, expresa e indubitable y con lenguaje sencillo, lo siguiente: (i) la finalidad del tratamiento, (ii) la identidad de los que son o pueden ser sus destinatarios, de ser el caso, (iii) la existencia del banco de datos en el que se almacenarán, (iv) el carácter obligatorio o facultativo de sus respuestas al cuestionario que se le proponga, de ser el caso, (v) la transferencia nacional o internacional que se efectúe. Al respecto, consideramos que la introducción de este inciso en el Proyecto de Reglamento es totalmente innecesaria, debido a que este aspecto ya ha sido regulado en la Ley[42].

Ahora bien, en referencia al flujo transfronterizo de datos personales, el Proyecto de Reglamento dispone que "cuando se solicite el consentimiento para una forma de tratamiento que incluya o pueda incluir la transferencia nacional o internacional de los datos, el titular de los mismos deberá ser informado de forma que conozca inequívocamente tal circunstancia, además de la finalidad a la que se destinarán sus datos y el tipo de actividad desarrollada por quien recibirá los mismos"[43]. De igual forma, consideramos que esta acotación es innecesaria, debido a que una de las características fundamentales establecida por la norma es que el consentimiento sea informado, para lo cual debe prestarse una manifestación inequívoca.

B. Flujo transfronterizo de datos personales

La Ley dispone que "El titular y el encargado del banco de datos personales[44] deben realizar el flujo transfronterizo de datos personales solo si el país destinatario mantiene niveles de protección adecuados conforme a la presente Ley. En caso de que el país destinatario no cuente con un nivel de protección adecuado, el emisor del flujo transfronterizo de datos personales debe garantizar que el tratamiento de los datos personales se efectúe conforme a lo dispuesto en la presente Ley (…)".

Nuestra legislación vigente no ha establecido un concepto de nivel de protección

41 Proyecto de Reglamento de la Ley 29733 –Ley de Protección de Datos Personales:
"Artículo 13.- Consentimiento y Datos Sensibles.
Tratándose de datos sensibles, el consentimiento debe ser por escrito, a través de su firma manuscrita, firma digital o cualquier otro mecanismo de autentificación que garantice la voluntad inequívoca del titular (…)".

42 Ley 29733 –Ley de Protección de Datos Personales. Artículo 18– Derecho de Información del titular de datos personales.

43 Artículo 11 del Proyecto de Reglamento de la Ley 29733 –Ley de Protección de Datos Personales.

44 Ley 29733 –Ley de Protección de Datos Personales:
"Artículo 2.6. Encargado del banco de datos personales.
Toda persona natural, persona jurídica de derecho privado o entidad pública que sola o actuando conjuntamente con otra realiza el tratamiento de los datos por encargo del titular del banco de datos personales".

adecuado para el flujo transfronterizo de datos personales, por lo cual, a efectos de determinar si nuestra norma cumple con dicho estándar, tomaremos como referencia la Directiva UE 95/46/CE y el Documento de Trabajo: Transferencia de datos personales a terceros países: aplicación de los artículos 25 y 26 de la Directiva sobre protección de datos de la Unión Europea, anteriormente desarrollados.

Como mencionamos, son dos los criterios para determinar el nivel de protección adecuado que debe tener el país receptor del flujo:

1. Principios básicos mínimos que deben ser establecidos, y sus equivalentes en nuestra legislación:

- Principio de limitación de objetivos. Este principio es equiparable al "Principio de Finalidad"[45].

- Principio de proporcionalidad y de calidad de los datos, equiparable al "Principio de proporcionalidad"[46] y "Principio de Calidad"[47].

- Principio de seguridad, equiparable al "Principio de Seguridad"[48].

- Derechos de acceso, rectificación y oposición. Estos derechos también se encuentran establecidos como tales en nuestra legislación.

- Restricciones respecto a transferencias sucesivas a otros países, sobre este aspecto contamos con el "Principio de nivel de protección adecuado"[49], que sin hacer diferencia del lugar de ubicación del emisor del flujo, dispone que siempre debe ser garantizado un nivel de protección adecuado para esta acción. Entenderíamos que dicha situación puede presentarse en el supuesto de que el Titular de los datos disponga de un encargado en un país diferente al de su residencia, y que este (el encargado) a su vez transfiera (por encargo del titular) los datos personales a otro encargado que se encuentra en un territorio diferente.

Ahora bien, acerca de los tres principios adicionales que deben ser cumplidos dependiendo de la categoría de datos:

- Datos sensibles. La protección adicional que se ha establecido en nuestro ordenamiento es la exigencia de contar con el consentimiento del titular por escrito para efectuar el tratamiento de datos sensibles.

- Mercadotecnia directa. En nuestra legislación el consentimiento para el tratamiento de los datos puede ser revocado en cualquier momento, sin importar la finalidad por la que estos

45 Ley 29733 –Ley de Protección de Datos Personales:
"Artículo 6.- Principio de Finalidad.
Los datos personales deben ser recopilados para una finalidad determinada, explícita y lícita. El tratamiento de los datos no debe extenderse a otra finalidad que no haya sido establecida de manera inequívoca como tal al momento de su recopilación (…)".

46 Ley 29733 –Ley de Protección de Datos Personales:
"Artículo 7.- Principio de Proporcionalidad.
Todo tratamiento de datos personales debe ser adecuado y no excesivo para la finalidad para la que estos hubiesen sido recopilados".

47 Ley 29733 –Ley de Protección de Datos Personales:
"Artículo 8.- Principio de calidad.
Los datos personales que vayan a ser tratados deben ser veraces, exactos y, en la medida de lo posible, actualizados, necesarios, pertinentes y adecuados respecto de la finalidad para la que fueron recopilados. Debe conservarse de forma tal que garantice su seguridad y sólo por el tiempo necesario para cumplir con la finalidad del tratamiento."

48 Ley 29733 –Ley de Protección de Datos Personales:
"Artículo 9.- Principio de seguridad.
El titular del banco de datos personales y el encargado de su tratamiento deben de adoptar las medidas técnicas, organizativas y legales necesarias para garantizar la seguridad de los datos personales. Las medidas de seguridad deben ser apropiadas y acordes con el tratamiento que se vaya a efectuar y con la categoría de datos personales que se trate".

49 Ley 29733 –Ley de Protección de Datos Personales:
"Artículo 11.- Principio de nivel de protección adecuado.
Para el flujo transfronterizo de datos personales, se debe garantizar un nivel suficiente de protección para los datos personales que se vayan a tratar o, por lo menos, equiparable a lo previsto por esta Ley o por los estándares internacionales en la materia".

fueron recabados[50]. Por ende, si los datos tienen como objetivo ser tratados con el propósito de mercadotecnia directa, el consentimiento por parte del titular puede ser revocado en cualquier momento.

- Decisión individual automatizada. Nuestra legislación contiene una disposición muy similar a la establecida en el artículo 15 de la Directiva[51], según la cual el "titular de los datos personales tiene derecho a no verse sometido a una decisión con efectos jurídicos sobre él o que le afecte de manera significativa, sustentada únicamente en determinados aspectos de su personalidad o conducta, salvo que ello ocurra en el marco de una negociación, celebración o ejecución de un contrato o en los casos de evaluación con fines de incorporación a una entidad pública, de acuerdo a ley, sin perjuicio de la posibilidad de defender su punto de vista, para salvaguardar su legítimo interés"[52] [53].

2. Mecanismos del procedimiento / de aplicación

Si bien se ha mencionado que es fundamental para un sistema de cumplimiento de protección de datos contar con una autoridad de supervisión externa, lamentablemente en el caso de la experiencia peruana dicha característica no se ha cumplido. En efecto, la Exposición de Motivos del Proyecto de Ley de Datos Personales manifiesta que si bien hubiera sido conveniente crear una entidad con autonomía técnica, económica, presupuestal y administrativa, en concordancia con el modelo europeo, la realidad de austeridad por la que atraviesa el país lo impide. Sin embargo, se optó por la creación de la Autoridad Nacional de Datos Personales, ente circunscrito al Ministerio de Justicia y Derechos Humanos, para que cumpla adecuadamente sus funciones y con ello sensibilice y ayude a que la sociedad tome conciencia acerca de la importancia de brindar una adecuada protección de los datos personales[54], opción que podría resultar más adecuada a nuestro contexto.

Adicionalmente, cabe referirnos a los objetivos básicos del sistema de protección de datos personales:

(i) Nivel satisfactorio de cumplimiento de normas. Debido a que nuestra Ley de Protección de Datos Personales aún no ha sido implementada en su totalidad, es difícil determinar si nuestra legislación cumplirá con un nivel satisfactorio de cumplimiento. Sin embargo, contamos con elementos que ayudarán en la ejecución eficiente de la Ley:

- Infracciones y Sanciones: Nuestro ordenamiento cuenta con un listado de infracciones que son clasificadas como leves, graves y muy graves. Las sanciones administrativas a aplicarse son pecuniarias y son establecidas en unidades impositivas tributarias (UIT), asimismo es factible imponer multas coercitivas.

  Sin embargo, la amplitud con la que algunas infracciones fueron redactadas puede llevar a la interpretación que toda vulneración al principio de consentimiento es considerada como grave. En efecto, como infracción leve se ha establecido "dar tratamiento a datos personales sin recabar el consentimiento de sus titulares, cuando el mismo sea necesario conforme a lo dispuesto en

50 Artículo 13.7 de la Ley 29733 –Ley de Protección de Datos Personales.

51 Ver nota al pie número 20.

52 Artículo 23 (Derecho al tratamiento objetivo) de la Ley 29733 –Ley de Protección de Datos Personales.

53 Según la nota al pie de página número 57 de la Exposición de Motivos del Proyecto de Ley 4079-2009-PE Ley de Protección de Datos Personales, "Con el derecho al tratamiento objetivo, se pretende evitar que el tratamiento de datos personales permita o propicie actividades discriminatorias, lo que constituye una de las mayores preocupaciones frente al avance de la informática. Entre los datos que al efecto interesa proteger de este tratamiento tendencioso se encuentran los relativos al rendimiento laboral y a la situación crediticia, entre otros". p. 38. En: http://www2.congreso.gob.pe/Sicr/TraDocEstProc/CLProLey2006.nsf.

54 Ibíd. pp. 40-41.

esta Ley", como infracción grave "dar tratamiento a los datos personales contraviniendo los principios establecidos en la presente Ley o incumpliendo sus demás disposiciones o las de su Reglamento". Cabe advertir que el consentimiento es un principio establecido en la Ley, por lo cual la vulneración a este podría caber en los dos niveles de infracciones.

A mayor abundamiento, es considerada como infracción muy grave "dar tratamiento a los datos personales contraviniendo los principios establecidos en la presente Ley o incumpliendo sus demás disposiciones o las de su Reglamento, cuando con ello se impida o se atente contra el ejercicio de los derechos fundamentales", por lo que una vulneración al principio de consentimiento podría ser considerada muy grave por atentar contra el derecho a la autodeterminación informativa, que a su vez repercute sobre el derecho a la intimidad por servir como vínculo para la afectación de este último.

Lamentablemente la delimitación de estas infracciones no se ha efectuado en el Proyecto de Reglamento, lo cual afecta el carácter disuasorio de las sanciones por no contar con un parámetro de predictibilidad que determine que conductas son punibles con mayor severidad, incurriendo en una afectación a la seguridad jurídica y al principio de tipicidad.

(ii) Sistemas de verificación directa. La Ley ha establecido como función de la Autoridad de Datos Personales "iniciar fiscalizaciones de oficio o por denuncia de parte por presuntos actos contrarios a lo establecido en la presente Ley y en su reglamento y aplicar las sanciones administrativas correspondientes, sin perjuicio de las medidas cautelares o correctivas que establezca el reglamento"[55].

Para tal efecto, el Proyecto de Reglamento ha establecido un procedimiento fiscalizador mediante el cual la Dirección de Supervisión y Control de la Dirección General de Protección de Datos Personales podrá requerir al titular, al encargado o quien resulte responsable del banco de datos personales, información relativa al tratamiento de estos o la documentación necesaria e incluso el acceso a los bancos[56]. De esta manera se ha constituido un sistema de verificación directa por parte de la autoridad que fiscalice el cumplimiento eficiente de la Ley y su Reglamento.

A. Ofrecer apoyo y asistencia a los interesados en el ejercicio de sus derechos

En concordancia con el Derecho de Tutela[57] establecido en la Ley, el Proyecto de Reglamento ha establecido el llamado "Procedimiento de Tutela Directa", por el cual el titular de los datos hace valer sus derechos enviando una solicitud al titular del banco de datos o responsable de su tratamiento. La solicitud debe dar respuesta a cada uno de los extremos solicitado en el plazo establecido en el Reglamento, en caso contrario, al no haber recibido respuesta, el solicitante considerará denegada la solicitud. Esta situación habilita al titular de los datos a iniciar un procedimiento administrativo[58].

Sin embargo, para permitir que el interesado haga valer sus derechos con rapidez y sin costos excesivos, puede acudir al procedimiento fiscalizador mencionado en el acápite anterior que puede ser iniciado por denuncia de parte dirigida a la Autoridad Nacional de Protección de Datos Personales.

B. Ofrecer vías adecuadas de recurso a quienes vean afectados sus derechos

Otro principio establecido en nuestra legislación es el Principio de Disposición de Recurso[59] que guarda concordancia con el Derecho a la Tutela. Mediante este último, quienes vean afectados sus derechos pueden

55 Artículo 33 inciso 20 de la Ley 29733 –Ley de Protección de Datos Personales.

56 Artículo 99 del Proyecto de Reglamento de la Ley 29733 –Ley de Protección de Datos Personales.

57 Artículo 24 de la Ley 29733 –Ley de Protección de Datos Personales.

58 Articulo 73 del Proyecto de Reglamento de la Ley 29733 –Ley de Protección de Datos Personales.

recurrir a la Autoridad Nacional de Datos Personales para iniciar un procedimiento administrativo o ante el Poder Judicial para efectos de interponer el recurso de habeas data[60].

Al respecto, debemos mencionar que una vez agotada la vía administrativa frente a la Autoridad Nacional de Datos Personales, el interesado puede recurrir a la acción contencioso administrativa ante el Poder Judicial. Sin embargo, el recurso de habeas data puede ser interpuesto de manera directa ante el Poder Judicial, debido a que no es un requisito para los procesos constitucionales el haber agotado la vía administrativa previa.

IV. ¿EL PERÚ CUENTA CON UN NIVEL DE PROTECCIÓN ADECUADO PARA CONVERTIRSE EN RECEPTOR DEL FLUJO TRANSFRONTERIZO DE DATOS PERSONALES Y, POR LO TANTO, SER UN PAÍS ATRACTIVO PARA LA INVERSIÓN EXTRAJERA? – CONCLUSIONES

a) En líneas generales, cumplimos con la mayoría de requisitos para ser considerados como país receptor de datos personales con un nivel adecuado de protección; sin embargo, existen un aspecto fundamental que debe ser reformado: delimitación de las infracciones.

b) Según la exposición de motivos del Proyecto de Ley 4079-2009-PE –Ley de Protección de Datos Personales–, el fundamento para adscribir a la Autoridad Nacional de Protección de Datos Personales al Ministerio de Justicia y Derechos Humanos, encontraría sustento en la situación de austeridad que atravesaba el país en el momento de la redacción de tal documento. Sin embargo, la realidad económica ha cambiado, por lo cual se debería evaluar la posibilidad de crear un ente independiente.

c) Sobre el punto anterior, consideramos también que una vez puesto en marcha el sistema de protección será más sencillo que la Autoridad de Protección de Datos Personales cuente con recursos presupuestarios que incentiven su independencia[61].

d) Delimitación de normas: principio de tipicidad de la potestad sancionadora. Debe verificarse la redacción de la Ley y el Proyecto de Reglamento a fin de establecerse supuestos más específicos de infracción, para evitar así cuestionamientos en su aplicación, y lo que es más importante, dotar de seguridad jurídica a los inversionistas.

e) Finalmente, es muy importante revisar, y por tanto simplificar el Proyecto de Reglamento, ya que tal como se ha mencionado, existen casos de duplicidad de regulación, e inclusive algunas contradicciones entre Ley y Reglamento.

Creemos que el Perú está dando pasos muy importantes en la línea de lograr la implementación de una legislación de protección de datos personales moderna y acorde con los estándares internacionales. Sin embargo, esta legislación requiere aún ser "pulida". Dependerá luego de la manera como se aplique por la autoridad competente, lo que haga que la misma quede legitimada como una herramienta de promoción de la inversión privada.

59 Ley 29733 –Ley de Protección de Datos Personales:
"Artículo 10.- Principio de disposición de recurso.
Todo titular de datos personales debe contar con las vías administrativas o judiciales necesarias para reclamar y hacer valer sus derechos, cuando estos sean vulnerados por el tratamiento de sus datos personales".

60 Artículo 24 de la Ley 29733 –Ley de Protección de Datos Personales:

61 El artículo 36 de la Ley de Protección de Datos establece que son recursos de la Autoridad Nacional de Protección de Datos Personales: (i) Las tasas de derecho de trámite de los procedimientos administrativos y servicios de su competencia; (ii) Los montos que recaude por concepto de multas; (iii) Los recursos provenientes de la cooperación técnica internacional no reembolsable; (iv) los legados y donaciones que reciba; (v) los recursos que se le transfieren conforme a la Ley.