LA LEY DE PROTECCIÓN DE DATOS Y SU INCIDENCIA EN LAS BASES DE DATOS PERSONALES Y EL E-COMMERCE

Ariana Palacios Chavez-Taffur

Sumario: I. Las normas que actualmente regulan la protección de datos en el Perú. II. Sujetos obligados a cumplir con la LPD y el RLPD. III. Elaboración de Bases de Datos Legales. IV. El consentimiento del dueño de los Datos personales. V. Principales derechos que asisten a los dueños de los datos personales. VI. Los bancos de datos y el registro ante la Dirección General. VII. Limitaciones a la transferencia de bancos de datos personales. VIII. El flujo transfronterizo de datos personales. IX. Estándar mínimo de seguridad para la protección de datos personales. X. Compra y transferencia de la titularidad de un banco de datos. XI. Comercio Electrónico y protección del consumidor. XII. Comercio electrónico y el principio de territorialidad. XIII. Experiencia Comparada. XIV. Conclusión.

Resumen:

Sobre la base de lo dispuesto en el artículo 2 de la Constitución Política del Perú[1], el 3 de julio de 2011 se publicó la Ley de Protección de Datos Personales. La misma tiene como objetivo el *"adecuado tratamiento"* de los **datos personales**, los cuales comprenden *"toda información sobre una persona natural que la identifica o la hace identificable a través de medios que pueden ser razonablemente utilizados"*[2].

El marco legal asume una noción amplia del concepto de datos personales. Es decir, considera como "personal" cualquier tipo de información que permita relacionarse con alguna persona natural, lo cual involucra información numérica, alfabética, gráfica, acústica, sobre hábitos personales o de cualquier otro tipo concerniente a personas naturales que identifica o hace identificables a las personas naturales[3].

Como puede apreciarse, la regulación establece una definición amplia acerca de qué puede entenderse como "personal", de tal modo que, por ejemplo, las iniciales de una persona o la dirección de un correo electrónico asignado podrán ser considerados como datos personales en tanto puedan vincularse con algún usuario.

[1] "Art.2 Toda persona tiene derecho: (…) 6. A que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar.
[2] Artículo 2 numeral 4 de la Ley de Protección de Datos Personales.
[3] Artículo 2 numeral 4 del Reglamento de la Ley de Protección de Datos Personales.

Cabe señalar que la Ley establece una diferenciación entre los datos personales respecto de los denominados "datos sensibles". De acuerdo con el artículo 2 numeral 5 de la Ley, estos últimos se refieren a los *"datos biométricos que por sí mismos pueden indentificar al titular; datos referidos al origen racial y étnico; ingresos económicos, opiniones o convicciones políticas, religiosas, filosóficas o morales; afiliación sindical; e información relacionada a la salud o a la vida sexual."*

En ese sentido, los datos sensibles son aquellos referidos a características físicas, morales o emocionales, hechos o circunstancias de la vida afectiva o familiar, hábitos que corresponden a la esfera más íntima u otra información análoga que se encuentre estrecha y directamente vinculada con la intimidad[4].

Como se aprecia, prácticamente todo tipo de datos relacionados con personas naturales, desde el nombre hasta la información patrimonial u otro dato de especial sensibilidad, estarán sujetos a la protección de la Ley.

A partir del concepto de datos personales y sensibles, la Ley basa su aplicación en el llamado "Tratamiento de Datos Personales", que incluye cualquier operación (con o sin intervención humana) en donde se realicen actividades destinadas a captar, registrar, almacenar, conservar, verificar, modificar o transmitir los datos personales o sensibles. Cabe precisar que estos datos podrán ser tratados de manera organizada a través de un Banco de Datos Personales[5], o ser tratados bajo un esquema no sistematizado ni organizado.

I. LAS NORMAS QUE ACTUALMENTE REGULAN LA PROTECCIÓN DE DATOS EN EL PERÚ

Nuestra Constitución Política prevé como un derecho constitucional, *"(…) que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar"* (Artículo 2, numeral 6). Es bajo esta disposición constitucional que, con fecha 3 de julio de 2011, se emitió la Ley No. 29733 – Ley de Protección de Datos Personales (en adelante, "LPD"); primera norma que regula la protección de datos personales en nuestro país. Es en este sentido que, conforme a la LPD: *"La presente Ley tiene el objeto de garantizar el derecho fundamental a la protección de los datos personales, previsto en el artículo 2, numeral 6 de la Constitución Política del Perú, a través de su adecuado tratamiento, en un marco de respeto de los demás derechos fundamentales que en ella se reconocen."* (Artículo 1).

[4] Artículo 2 numeral 6 del Reglamento de la Ley de Protección de Datos Personales.

[5] LEY DE PROTECCIÓN DE DATOS PERSONALES, Artículo 2.- Definiciones.- Para todos los efectos de la presente Ley, se entiende por:
1.- Banco de datos personales.- *Conjunto organizado de datos personales, automatizado o no, independientemente del soporte, sea este físico, magnético, digital, óptico u otros que se creen, cualquiera fuere la forma o modalidad de su creación, formación, almacenamiento, organización y acceso.*

Mucha de la regulación contenida en la LPD se encontró suspendida hasta la emisión de su reglamento, publicado con fecha 22 de marzo de 2013 y aprobado mediante Decreto Supremo No. 003-2013-JUS (en adelante, "RLPD").

Sobre la base de la normativa referida anteriormente, la Dirección General de Protección de Datos Personales del Ministerio de Justicia y Derechos Humanos, autoridad administrativa competente en materia de protección de datos personales (en adelante, la "Dirección General"), ha publicado sendas resoluciones directorales que aprueban los formularios para el procedimiento de registro[6], para el procedimiento de denuncia por actos contrarios a la LPD[7] y para el procedimiento de registro de flujo transfronterizo de datos[8] (temas que abordaremos en acápites posteriores).

Actualmente, la LPD, el RLPD y las resoluciones directorales se encuentran plenamente vigentes y su cumplimiento es obligatorio. Sin embargo, es preciso añadir que, conforme al RLPD, se ha otorgado el plazo de dos (2) años para que los bancos de datos ya existentes sean adecuados a lo previsto en la LPD y el RLPD: *"En el plazo de dos (2) años de la entrada en vigencia del presente reglamento, los bancos de datos personales existentes, deben adecuarse a lo establecido por la Ley y el presente reglamento, sin perjuicio de la inscripción a que se refiere la Quinta Disposición Complementaria Final de la Ley N° 29733, Ley de Protección de Datos Personales."* (Primera Disposición Complementaria Transitoria). Es decir, el plazo de dos (2) años de adecuación no aplica para la obligación de inscribir los bancos de datos personales en el registro correspondiente (tema tratado a detalle en puntos posteriores).

II. SUJETOS OBLIGADOS A CUMPLIR CON LA LPD Y EL RLPD.

La regulación en materia de protección de datos es aplicable a todas las personas, naturales o jurídicas, de derecho público o privado, que tengan banco de datos personales cuyo tratamiento sea realizado en el Perú. Así, la LPD señala: *"La presente Ley es de aplicación a los datos personales contenidos o destinados a ser contenidos en bancos de datos personales de administración pública y de administración privada, cuyo tratamiento se realiza en el territorio nacional."* (Artículo 3). La LPD únicamente contempla dos (2) exclusiones respecto de la aplicación de esta normativa:

a. Datos personales contenidos o destinados a ser contenidos en bancos de datos personales creados por personales naturales para fines exclusivamente relacionados a su vida privada o familiar (Artículo 3, numeral 1, LPD).

[6] Resolución Directoral No. 001-2013-JUS/DGPDP del 08 de mayo de 2013.
[7] Resolución Directoral No. 002-2013-JUS/DGPDP del 31 de mayo de 2013.
[8] Resolución Directoral No. 003-2013-JUS/DGPDP del 31 de mayo de 2013.

b. Datos personales contenidos o destinados a ser contenidos en bancos de datos personales de administración pública, solo en tanto su tratamiento resulte necesario para el estricto cumplimiento de las competencias que les fueron asignadas por ley, para la defensa nacional, seguridad pública, y para el desarrollo de actividades en materia penal para la investigación y represión del delito (Artículo 3, numeral 2, LPD).

Cabe precisar que, por "tratamiento" se entiende *"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."* (Artículo 2, numeral 17, LPD).

De manera mucho más detallada, el RLPD dispone que la normativa peruana resulte aplicable al tratamiento de datos personales en cualquiera de los siguientes casos:

a. Sea efectuado en un establecimiento ubicado en el Perú correspondiente al Titular del banco de datos personales o de quien resulte responsable de su tratamiento (Artículo 5, numeral 1). Los Titulares de los bancos de datos son las personas naturales o jurídicas, de derecho público o privado, que determina la finalidad y contenido del banco de datos personales, el tratamiento de estos y las medidas de seguridad (Artículo 2, numeral 15, LPD).

b. Sea efectuado por un Encargado del tratamiento, con independencia de su ubicación, a nombre del Titular del banco de datos personales o del responsable del tratamiento cuando éstos se encuentren establecidos en el Perú (Artículo 5, numeral 2). Los Encargados del banco de datos personales son las personas naturales o jurídicas, de derecho público o privado, que realizan el tratamiento de los datos personales por encargo del Titular del banco de datos personales (Artículo 2, numeral 6, LPD).

c. El Titular del banco de datos personales o el responsable del tratamiento no esté establecido en Perú, pero le resulte aplicable la legislación peruana por disposición contractual o del derecho internacional (Artículo 5, numeral 3).

d. El Titular del banco de datos personales o el responsable del tratamiento no esté establecido en Perú, pero utilice medios situados en dicho territorio, salvo que tales medios se utilicen únicamente con fines de tránsito que no impliquen un tratamiento (Artículo 5, numeral 4).

De esta manera, la regulación peruana en materia de datos personales será aplicable para cualquier banco de datos existente en Perú o cuyo Titular o encargado del tratamiento se encuentre en Perú. Así, la LPD y el RLPD serán aplicables incluso si el Titular o Encargado son de nacionalidad distinta a la peruana o se encuentran domiciliados en el extranjero.

III. ELABORACIÓN DE BASES DE DATOS LEGALES.

El principal requisito es haber obtenido el consentimiento previo, informado, expreso e inequívoco de los dueños de los datos personales que serán incorporados en el banco de datos.

La LPD entiende por "datos personales" a *"Toda información sobre una persona natural que la identifica o la hace identificable a través de medios que pueden ser razonablemente utilizados."* (Artículo 2, numeral 4). El RLPD añade que *"Es aquella información numérica, alfabética, gráfica, fotográfica, acústica, sobre hábitos personales, o de cualquier otro tipo concerniente a las personas naturales que las identifica o las hace identificables a través de medios que pueden ser razonablemente utilizados."* (Artículo 2, numeral 4).

Para estos efectos, el consentimiento del dueño de los datos personales debe cumplir con los siguientes requisitos:

a. Libre. Esto es, que el consentimiento haya sido expresado sin que medie acto alguno que afecte la manifestación de voluntad del dueño de los datos personales (como dolo, violencia, mala fe o intimidación) (Artículo 12, numeral 1, RLPD).

b. Previo. El consentimiento debe ser expresado de manera anticipada a la recopilación de datos o, en su caso, anterior al tratamiento distinto por el cual fueron inicialmente recopilados (Artículo 12, numeral 2, RLPD).

c. Expreso e inequívoco. El consentimiento debe haber sido manifestado de manera tal que no queden dudas sobre su otorgamiento. Esta manifestación puede ser verbal, escrita o, incluso, por medios electrónicos (formularios), siempre que el dueño de los datos personales ejecute una conducta que evidencia que ha consentido inequívocamente (Artículo 12, numeral 3, RLPD).

d. Informado. El Titular del banco de datos personales debe informar de manera clara, expresa e indubitable, con lenguaje sencillo, la siguiente información mínima al dueño de los datos personales antes de que éste exprese su consentimiento: (i) Identidad y domicilio del Titular del banco de datos personales o del responsable de su tratamiento al que pueden dirigirse para revocar su consentimiento; (ii) la finalidad o finalidades del tratamiento a las que los datos a ser proporcionados serán sometidos; (iii) la identidad de los que son o pueden ser los destinatarios de los

datos personales; (iv) la existencia del banco de datos personales en que se almacenarán; (v) el carácter obligatorio o facultativo de las respuestas, cuando sea el caso; (vi) las consecuencias de proporcionar sus datos personales y de su negativa a hacerlo; y, (vii) la transferencia nacional e internacional de datos que se efectúen, de ser el caso.

El tratamiento de los datos personales deberá ser realizado según el consentimiento prestado por el dueño de dichos datos, siguiendo criterios de razonabilidad y proporcionalidad.

Cabe precisar que el RLPD exige que para el caso de "datos sensibles" (estos son, conforme al Artículo 2, numeral 5 de la LPD, aquellos *"Datos personales constituidos por los datos biométricos que por sí mismos pueden identificar al titular; datos referidos al origen racial y étnico; ingresos económicos; opiniones o convicciones políticas, religiosas, filosóficas o morales; afiliación sindical; e información relacionada a la saludo o a la vida sexual"*) se requiere que el consentimiento sea *"(…) otorgado por escrito, o a través de su firma manuscrita, firma digital o cualquier otro mecanismo de autenticación que garantice la voluntad inequívoca del titular."* (Artículo 14).

El RLPD no ha limitado o especificado cuáles son los "otros mecanismos de autenticación" para la consentimiento de recopilación y tratamiento de datos sensibles. Sin embargo, conforme al propio RLPD, *"Para efectos de demostrar la obtención del consentimiento en los términos establecidos en la Ley y en el presente reglamento, la carga de la prueba recaerá en todos los casos en el titular del banco de datos personales o quien resulte responsable del tratamiento."* (Artículo 15). De esta manera, tanto el Titular como el Encargado son los que deberán acreditar, de manera indubitable, el haber obtenido el consentimiento del dueño de los datos sensibles.

Finalmente, para la recopilación y tratamiento de datos personales de menores de edad, será necesario el consentimiento de sus padres o tutores legales. Excepcionalmente será posible obtener datos personales de mayores de catorce (14) y menores de dieciocho (18) años, cuando ésta sea realizada en un lenguaje comprensible y bajo los términos previstos en el RLPD (Artículos 27 a 29).

IV. EL CONSENTIMIENTO DEL DUEÑO DE LOS DATOS PERSONALES.

El Artículo 14 de la LPD contempla las siguientes excepciones en los que no se requiere obtener el consentimiento del dueño de los datos personales para su tratamiento. Las excepciones más relevantes para efectos de esta consulta son las siguientes:

a. Cuando se trate de datos personales contenidos o destinados a ser contenidos en fuentes accesibles al público. El RLPD pone, como ejemplos, a las guías telefónicas, los diarios y revistas, y los Registros Públicos, entre otros.

b. Cuando los datos personales sean necesarios para la ejecución de una relación contractual en la que el dueño de los datos personales sea parte, o cuando se trate de datos personales que deriven de una relación científica o profesional del titular y sean necesarios para su desarrollo o cumplimiento. Tal es el caso de los empleadores que requieren de la recopilación y tratamiento de datos personales para poder cumplir con las normas propias del ámbito laboral.

   El tipo de datos y el tratamiento a los que podrán someterse dependerá del caso concreto. Por ejemplo, la recopilación de datos vinculados a la salud del trabajador puede ser necesaria para aquel personal que trabaje en puestos con riesgos para la salud (hospitales), pero no para otro tipo de labores.

c. Cuando se hubiese aplicado un procedimiento de anonimización o disociación. Esto es, los datos personales deben ser sometidos a un procedimiento irreversible que impida la identificación del dueño de los datos.

   Para garantizar la completa anonimidad, no debe existir posibilidad alguna de que el dueño de los datos pueda ser identificado. Si el procedimiento es reversible (por ejemplo, si completando la información con información adicional en posesión del Titular del banco de datos o que puede ser obtenida de cualquier fuente es posible identificar al dueño de los datos personales), entonces se entenderá que la información no es anónima y será exigible el consentimiento del dueño de los datos.

d. Cuando se trate de datos personales relativos a la solvencia patrimonial y de crédito, conforme a ley. Esta es la información obtenida por o de las centrales de riesgo que operan en el país bajo la regulación pertinente (entre ellas, la Ley No. 27489 – Ley que regula las centrales privadas de información de riesgos y de protección al titular de la información).

V. PRINCIPALES DERECHOS QUE ASISTEN A LOS DUEÑOS DE LOS DATOS PERSONALES.

Los principales derechos, reconocidos por la regulación vigente, son:

a. Derecho de información.- consiste en el derecho del dueño de los datos a ser informado en forma sencilla, detallada, expresa, inequívoca y de manera previa a la recopilación, sobre la finalidad para la que los datos serán tratados; quiénes son o pueden ser los destinatarios, la existencia del banco de datos en que se almacenarán, así como la identidad y domicilio de su Titular y del Encargado del tratamiento de los datos personales; el carácter obligatorio o facultativo de las respuestas, en

especial en cuanto a los datos sensibles; la transferencia de los datos personales; las consecuencias de proporcionar los datos personales y de la negativa a hacerlo; el tiempo durante el cual se conservarán; y la posibilidad de ejercer los derechos reconocidos por ley (Artículo 18, LPD).

b. Derecho de acceso.- el dueño de los datos tiene derecho a obtener la información que sobre sí mismo sea objeto de tratamiento en bancos de datos de administración pública o privada, la forma en que sus datos fueron recopilados, las razones que motivaron su recopilación y a solicitud de quién se efectuó la recopilación, así como la transferencias realizadas o que se prevén hacer de ellos (Artículo 19, LPD).

c. Derecho de actualización, inclusión, rectificación y supresión.- el dueño de los datos personales tiene derecho a exigir la actualización, inclusión, rectificación y supresión de sus datos personales objeto de tratamiento, cuando estos sean parcial o totalmente inexactos, incompletos, cuando se hubiere advertido omisión, error o falsedad, cuando hayan dejado de ser necesarios o pertinentes a la finalidad para la cual hayan sido recopilados o cuando hubiera vencido el plazo establecido para su tratamiento (Artículo 20, LPD).

d. Derecho de oposición.- el dueño de los datos personales puede oponerse al tratamiento cuando no hubiese prestado consentimiento previo ni exista ley que autorice dicho tratamiento (Artículo 22, LPD).

El Titular del banco de datos deberá implementar un procedimiento sencillo que permita a los dueños de los datos personales ejercer los derechos que les son reconocidos por ley (Artículo 53, RLPD). Para estos efectos, se deberán respetar los lineamientos mínimos establecidos en el RLPD (tales como los plazos mínimos de respuesta, requisitos de las solicitudes a ser presentadas por los dueños de los datos personales, etc.).

VI. LOS BANCOS DE DATOS Y EL REGISTRO ANTE LA DIRECCIÓN GENERAL.

Todos los bancos de datos que se encuentren sujetos a la LPD y el RLPD según los términos detallados en la respuesta a la pregunta 2 precedente.

De esta manera, tanto una empresa domiciliada en el Perú como una empresa extranjera, deberán registrar ante la autoridad peruana dichos bancos de datos personales, con independencia de la nacionalidad de los dueños de los datos personales cuya información se encuentre contenida en dichos bancos de datos personales, siempre que se encuentren sujetas a la aplicación de la LPD.

La única excepción a la obligación de inscripción versa sobre los bancos de datos de personas naturales destinados exclusivamente a su vida privada o familiar (RLPD, Artículo 77, numeral 1).

VII. LIMITACIONES A LA TRANSFERENCIA DE BANCOS DE DATOS PERSONALES.

El RLPD entiende como "transferencia" a la *"(…) comunicación de datos personales dentro o fuera del territorio nacional realizada a persona distinta al titular de los datos personales, al encargado del banco de datos personales o al encargado del tratamiento de datos personales."* (Artículo 18)

De otro lado, el RLPD entiende por "flujo transfronterizo" a *"(…) la transferencia de datos personales fuera del territorio nacional."* (Artículo 18). El flujo transfronterizo de datos personales no sólo debe haber sido autorizado previamente por el dueño de los datos personales, sino que debe ser objeto de registro ante la Dirección General.

De las normas arriba citadas, podemos concluir que cualquier transferencia que se realice entre el Titular del banco de datos y/o el Encargado del banco de datos y/o el Encargado del tratamiento no será considerado como una "transferencia" de datos y, por lo tanto, tampoco constituirán un flujo transfronterizo de datos personales.

Así, por ejemplo, si una empresa extranjera contrata a un encargado para el tratamiento de datos personales en el Perú, dicha empresa extranjera deberá inscribir el banco de datos personales ante la Dirección General (debido a que el banco de datos se encontrará materialmente en Perú para su respectivo tratamiento). Sin embargo, las transferencias de datos personales entre el titular y el encargado (de ida y vuelta) no serán objeto de registro por flujo transfronterizo (debido a que, bajo el RLPD, este traslado de información no constituye una transferencia ni flujo transfronterizo de datos personales).

Cabe precisar que cualquier transferencia de datos personales debe haber sido previamente autorizada por el dueño de los datos personales. Para estos efectos, nos remitimos a la respuesta dada a la pregunta 3.

VIII. EL FLUJO TRANSFRONTERIZO DE DATOS PERSONALES.

De acuerdo a la LPD, el flujo transfronterizo de datos personales será posible si *"(…) el país destinatario mantiene niveles de protección adecuados conforme a la presente Ley."* (Artículo 15). De esta manera, lo que establece la LPD es que el flujo transfronterizo únicamente se podrá realizar con países que cuenten con leyes y regulaciones que otorguen, como mínimo, los mismos derechos y protecciones a los dueños de los datos personales que los reconocidos por la legislación peruana.

Si el país destinatario no cuenta con el nivel de protección adecuado, entonces el emisor de los datos personales (esto es, el "exportador") deberá garantizar que el tratamiento se efectuará conforme a lo dispuesto en la LPD y el RLPD (Artículo 15, LPD). Para estos efectos, el RLPD añade que el flujo transfronterizo de datos personales podrá realizarse cuando *"(…) el receptor o importador de los datos personales asuma las mismas obligaciones que corresponden al titular del banco de datos personales o responsable del tratamiento que como emisor o exportador transfirió los datos personales."* (Artículo 24)

Estas reglas, sin embargo, tienen diversas excepciones previstas en el Artículo 15 de la LPD, entre ellas, cuando el dueño de los datos personales hubiera dado su consentimiento previo, informado, expreso e inequívoco de que la transferencia se realizará a un país que no cuenta con las mismas protecciones y garantías que el Perú. Es decir, este consentimiento deberá revestir las características descritas al dar respuesta a la Pregunta 3.

El emisor de los datos personales tendrá la obligación de acreditar que el flujo transfronterizo se realizó cumpliendo con las disposiciones legales peruanas (Artículo 20, RLPD).

IX. ESTÁNDAR MÍNIMO DE SEGURIDAD PARA LA PROTECCIÓN DE DATOS PERSONALES.

No. Tanto la LPD como el RLPD establecen una responsabilidad del Titular (y, por tanto, también de las personas que éste contrate para efectos del tratamiento de los datos personales) de *"(…) adoptar medidas técnicas, organizativas y legales que garanticen su seguridad y eviten su alteración, pérdida, tratamiento o acceso no autorizado."* (Artículo 16). Sin embargo, no impone mecanismos o estándares específicos de protección que deban ser implementados de manera obligatoria.

Sin perjuicio de ello, el RLPD dispone que la norma técnica NTP ISO IEC 17799 EDI – Tecnología de la Información – Código de Buenas Prácticas para la Gestión de Seguridad de la Información, debe ser tomada como referencia (Artículo 40).

X. COMPRA Y TRANSFERENCIA DE LA TITULARIDAD DE UN BANCO DE DATOS.

El "comprador" del banco de datos adquiere la condición de titular del banco de datos y, por lo tanto, se encontrará obligado a cumplir con todas las disposiciones de la LPD y del RLPD: *"El receptor de los datos personales asume la condición de titular del banco de datos personales o responsable del tratamiento en lo que se refiere la Ley y el presente reglamento, y deberá realizar el tratamiento de los datos personales cumpliendo lo establecido en la información que el emisor dio de manera previa al consentimiento recabado del titular de los datos personales"* (Artículo 22, RLPD).

Dichas obligaciones incluyen la de haber obtenido el consentimiento previo del dueño de los datos personales para la adquisición/transferencia del banco de datos a su favor (ver respuesta a la Pregunta 3) y efectuar el registro correspondiente.

En primer lugar debemos señalar que no existe una definición legal recogida dentro de la normativa peruana que nos indique qué debemos entender por e-commerce. No obstante, la Organización Mundial del Comercio ("OMC") define al comercio electrónico como la producción, mercadeo, ventas y distribución de productos y servicios vía redes de telecomunicaciones y siete principales instrumentos: el teléfono, el fax, la televisión, los medios de pago electrónicos y la transferencia electrónica de fondos, el intercambio electrónico de datos y el internet.

Por otro lado, la OCDE define el comercio electrónico como toda forma de transacción ligada a las actividades comerciales, que se basa en el tratamiento y transmisión de datos digitales, sobre todo en lo que concierne al texto, sonido o imagen.

En este sentido, el e-commerce es un mercado en el cual se utilizan las redes informáticas -como el internet o las vías de comunicación telefónica- para poder realizar transacciones comerciales sin la necesidad de ir presencialmente hasta la tienda, de manera que se crea un mercado electrónico a distancia de todo tipo de productos, servicios –incluyendo al financiero-, tecnologías y bienes; asimismo, incluye todo tipo de operaciones necesarias para concretar dichas transacciones, por ejemplo, negociación, información de referencia comercial, intercambio de documentos, en condiciones de seguridad y confidencialidad razonables.

XI. COMERCIO ELECTRÓNICO Y PROTECCIÓN DEL CONSUMIDOR

La legislación peruana protege al consumidor, toda vez que se trate de un proveedor domiciliado en el Perú (Principio de Territorialidad), no solo a través del Código de Consumo, sino por los siguientes medios:

a. Registro "Gracias… no insista" y Ley No. 28493, Ley que regula el uso del correo electrónico comercial no solicitado

   El registro "gracias… no insista" (en adelante, el "Registro") fue creado mediante la Directiva No. 005-2009/COD-INDFECOPI, Directiva de Operación y Funcionamiento del registro de Números Telefónicos y Direcciones de Correo Electrónico excluidos de ser destinatarios de publicidad masiva, vigente desde el 16 de setiembre de 2009 y modificado por la Directiva 159-2012-INDECOPI/COD.

Se trata de una lista que contiene todos aquellos números telefónicos y direcciones de correo electrónico que no podrán ser utilizados por los proveedores de bienes y servicios para realizar llamadas telefónicas, envío de mensajes de

texto a celular o de mensajes electrónicos masivos referidos a la promoción de productos y servicios.

El Registro se encuentra administrado por el Instituto Nacional de Defensa de la Competencia y la Protección de la Propiedad Intelectual-INDECOPI, a través de un sistema diseñado para preservar los datos enviados por los consumidores, adoptando las medidas de seguridad necesarias para velar por la confidencialidad de los mismos.

Los consumidores podrán registrar los números fijos o de celular y correos electrónicos a través de los cuales no deseen recibir llamadas, mensajes de texto y/o correos electrónicos promocionales que promocionen productos y servicios. De esta manera, los proveedores podrán contar con la lista de números telefónicos y correos electrónicos restringidos, a los cuales no podrán enviar ese tipo de información.

Asimismo, cabe resaltar que el Registro es de carácter permanente, de manera que si el consumidor desea salirse del registro deberá solicitar la baja de su inscripción.

Esta Directiva se crea como complemento a la Ley No. 28493, Ley que regula el uso del correo electrónico comercial no solicitado (SPAM) ya que ésta establece en su artículo 4, la obligación de los proveedores de servicio de correo electrónico domiciliados en el país a contar con sistemas o programas de bloqueo y/o filtro para la recepción o la transmisión que se efectúe a través de su servidor, de los correo electrónicos no solicitados por el usuario.

Asimismo, el artículo 5 señala las características de todo correo electrónico comercial, promocional o publicitario no solicitado originado en territorio peruano. De manera que aquellos proveedores que no cumplan con las aquellas características deberán compensar al receptor de manera pecuniaria.

b. Protección de datos del *ciberconsumidor*

   La primera pregunta que surge al momento de inscribirse en el Registro mencionado en líneas anteriores es ¿Cómo protejo mis datos? Respecto a este tema cabe indicar que no es posible conocer los datos personales de las personas que inscriben los números telefónicos y correos electrónicos en el Registro, ya que el proveedor sólo tendrá acceso a los números de teléfono (fijos y celulares) y direcciones de correo electrónico registradas y no a otro tipo de información.

Asimismo, respecto a este tema encontramos la Ley No. 29733, Ley de Protección de Datos Personales, la misma que de conformidad con su artículo 1, tiene como objetivo garantizar el derecho fundamental a la protección de los datos personales, entendida como toda información sobre una persona natural que la identifica o la hace identificable a través de medios que pueden ser razonablemente utilizados.

En este sentido, la referida Ley desarrolla el contenido del derecho fundamental reconocido en el artículo 2 inciso 6 de la Constitución de 1993. En términos generales, la Ley No. 29733 de Protección de Datos Personales dispone obligaciones para los sujetos pasivos, es decir los titulares y encargados de bancos de datos personales de administración pública y de administración privada, exceptuándose los bancos de datos privados creados para uso privado y los bancos de datos de la administración pública destinados al cumplimiento de las competencias de las entidades públicas o para la defensa nacional, la seguridad pública y la investigación penal, de conformidad con el artículo 3 de la referida normativa.

Las obligaciones específicas para los titulares y responsables de los bancos de datos se precisan en el artículo 28 de la Ley.

La normativa busca lograr su objetivo a través del consentimiento, es decir, busca que los sujetos pasivos cuenten con el consentimiento fehaciente del titular para proceder con la recopilación de datos. En este sentido, el artículo 13 de la Ley de la referencia, señala que los datos personales sólo pueden recogerse en una base de datos con consentimiento previo, informado, expreso e inequívoco de su titular, salvo ley autoritativa o enumeradas excepciones contempladas en el artículo 18.

De conformidad con el artículo 17, la norma también ha previsto el deber de confidencialidad respecto a los datos personales por parte de los titulares de los bancos de datos, los responsables del mismo y del personal que interviene en cualquier etapa de su tratamiento.

Por otro lado, debemos hacer referencia a la Ley 27309, que reprime punitivamente los delitos informáticos toda vez que se utilice indebidamente una base de datos, sistema o red de computadores o cualquier parte de la misma para diseñar, ejecutar, alterar un esquema u otro similar, o para interferir, interceptar, acceder o copiar información en tránsito o contenida en una base de datos. Así como cuando se daña información o se destruye o se pone en peligro la seguridad nacional.

XII. COMERCIO ELECTRÓNICO Y EL PRINCIPIO DE TERRITORIALIDAD

Hemos indicado que la normativa aplicable a las transacciones que se llevan a cabo de manera electrónica se aplica siempre y cuando se trate de una operación que se lleve a cabo dentro de territorio peruano, diferente es el caso de un consumidor que compra perfumes o ropa de una tienda cuya dirección electrónica pertenece a los Estados Unidos.

Para estos casos, no existe una normativa especial aplicable, y de conformidad con el Derecho Internacional Privado es la voluntad de las partes la clave en estos

casos, y en especial de las empresas, recurriendo estas a la legislación y juez aplicable del país de origen de los productos o servicios. Aunque nada está escrito aún, y existen diferentes teorías y opiniones respecto a este campo que pocos países se han atrevido a regular.

XIII. EXPERIENCIA COMPARADA

Dentro de las investigaciones realizadas para el presente análisis, encontramos cifras abrumadoras respecto al comercio electrónico en la República de Brasil.

Por ejemplo, de acuerdo a la información que proporciona la Cámara Brasileña de Comercio Electrónico, más del 75% de todos los negocios efectuados electrónicamente entre empresas en América Latina corresponden a Brasil. Asimismo, desde el 2001, el comercio minorista electrónico ha aumentado en un abismal 355%, convirtiendo a Brasil en el país donde el comercio electrónico es más utilizado por sus pobladores.

En este sentido, cabe preguntarnos ¿A qué se debe la crecida de este tipo de comercio en este país en especial? La respuesta es sencilla: instituciones legales.

En octubre del 2000 se creó el Comité Ejecutivo del Gobierno Electrónico, con el objetivo de formular políticas, establecer directrices, coordinar y articular acciones de implantación del Gobierno Electrónico orientado a la prestación de servicios e información a los ciudadanos (por ejemplo, las subastas electrónicas federales, las licitaciones públicas, etc). Asimismo, en mayo del 2001 se creó la Cámara Brasileña de Comercio Electrónico, entidad que busca promover, representar y defender los intereses colectivos de empresas, entidades y usuarios asociados involucrados en actividades de comercio y negocios electrónicos.

La regulación del comercio en América Latina, especialmente en Brasil, recibió y sigue recibiendo la influencia inevitable de la CNUDMI, especialmente los textos de 1996, 2001, 2005 y 2007, así como de la Política 1999/93 de la Comunidad Europea.

En este sentido, el Proyecto de Ley No. 1.589/99, elaborado por la Comisión Especial de Informática Jurídica de la OAB/SP, trata los siguientes aspectos: (i) ausencia de necesidad de autorización previa para oferta de bienes y servicios en razón del medio electrónico; (ii) obligatoriedad de identificación del oferente, de quien almacena, del proveedor de acceso y de los sistemas de seguridad para el archivamiento del contrato electrónico; (iii) reglas de utilización de informaciones de carácter privado; (iv) seguridad y certificación electrónica de las transacciones; (v) aplicabilidad de las normas de protección y defensa del consumidor al comercio electrónico; (vi) eficacia jurídica de las firmas electrónicas y de los documentos electrónicos; (vii) certificaciones electrónicas públicas y privadas; (viii) sanciones administrativas y penales aplicables, entre otros.

El Proyecto de Ley No. 3.303/00 regula la operación y el uso de la internet en el ámbito nacional, trayendo como innovaciones, entre otras: (i) la institución de mecanismos de seguridad, el registro de usuarios ante los proveedores de acceso y los medios adecuados para la identificación de prácticas ilícitas en la internet; (ii) la creación de Consejo de Ética de la Internet.

El Proyecto de Ley No. 672/99, incorpora casi integralmente los preceptos de la Ley Modelo de la UNCITRAL y aborda los siguientes puntos: (i) validez de las declaraciones de voluntad y formación de contratos a través de mensajes electrónicos; (ii) principios aplicables a la determinación del remitente, del destinatario, del tiempo y del lugar relativos al envío y a la recepción de los mensajes electrónicos, entre otros.

El Proyecto de Ley No. 4.906/01 regula el comercio electrónico en todo el territorio nacional, destacando la necesidad de uniformización de las normas de comercio electrónico en el ámbito internacional, creando dispositivos que reglamentan la aplicación de requisitos legales a los mensajes electrónicos y la comunicación de mensajes electrónicos, inclusive en lo que se refiere a la celebración y validez de los contratos celebrados virtualmente.

Actualmente, existen varios proyectos de ley que tienden a regular con mayor precisión el comercio electrónico, entre ellos se destacan el Proyecto de Ley 1.232/2011 y el Proyecto de Ley 439/2011.

El Proyecto de Ley No. 439/2011 complementa el Código de Consumo y varias normas específicas aplicables al comercio electrónico, entre los cuales los principales son: (i) deber de aparecer en el sitio web, que se ofrece en el producto o servicio, los datos (nombre, dirección, etc) del vendedor responsable; (ii) como medida cautelar el bloqueo de determinar la página electrónica.

XIV. Conclusión.

Así, observamos que la tendencia legislativa para lograr una mayor protección a los consumidores de productos de comercio electrónico, es obligar a las empresas a establecer políticas de uso y contratos para suministrar un adecuado servicio.

Es importante destacar que, a pesar de tratarse de proyectos de ley, el Poder Judicial Brasilero ya se ha manifestado, en base a los principios de la buena fe objetiva, la función social del contrato, la vulnerabilidad en favor de los consumidores.

De manera que en la actualidad, Brasil ha logrado incentivar el comercio electrónico y ha brindado la seguridad que muchos de sus consumidores buscaban.

Como hemos podido analizar a lo largo del presente documentos, no existe una normativa especial para el comercio electrónico en el Perú; es decir, sabemos que

debido a los cambios que surgieron con la globalización y los avances tecnológicos la normativa peruana ha ido evolucionando para acomodarse a las necesidades actuales de los consumidores; no obstante si buscamos que este tipo de comercio se desarrolle de una manera óptima en nuestro país, faltaría promover la seguridad de las transacciones a distancia.