Universidad de Lima

Escuela de Posgrado

Maestría en Derecho Empresarial


# EL IMPACTO DE LA LEY DE PROTECCIÓN DE DATOS PERSONALES EN EL CONTRATO DE HOSTING

Trabajo de investigación para optar el Grado Académico de Maestro en Derecho Empresarial

**Alessandra Polo Barrenechea**

**Código 20101797**

**Asesor**

Carmen Velarde Koechlin

Lima - Perú

2020

*"La vida no se trata de hacer cosas por uno mismo. Existe una manera de vivir en la que la felicidad de otros también pueda hacerte feliz*"

*Reki Kawahara*

# EL IMPACTO DE LA LEY DE PROTECCIÓN DE DATOS PERSONALES EN EL CONTRATO DE HOSTING

# RESUMEN

El presente trabajo de investigación tiene como finalidad dar a conocer la importancia de contar con una nueva regulación en Ley de Datos Personales y su Reglamento para que se adapte a las nuevas tendencias del comercio electrónico, y en especial al *contrato de hosting*.

En la investigación se determina que la legislación peruana actual es muy genérica y carece de suficientes herramientas que se adapten al nuevo tipo de contrato, lo cual conlleva a posibles irrupciones que vulneran la seguridad de la información, como principio rector de la normativa nacional en materia de protección de datos personales. Para ello, se proponen supuestos nuevos de cambios en la norma, lo cual conllevará a seguir permitiendo la libertad contractual de las partes al momento de celebrar el *contrato de hosting*, y a su vez hará regulaciones específicas que permitan resguardar los datos personales.

**Palabras claves:** Hosting, proveedor, usuario, contrato, seguridad de la información, datos personales, responsabilidad.

# ABSTRACT

The purpose of this research work is to publicize the importance of having a new regulation in our Personal Data Law and its Regulations, so that it adapts to the new trends in Electronic Commerce and especially in the Hosting Contract.

The Investigation determines that our current legislation is very generic and lacks sufficient tools to adapt to this new type of Contract, which leads to possible breaches that violate the principle of information security, as the guiding principle of our legislation in personal data matter. To do this, we propose new assumptions of changes in our rule which will lead to continue allowing the contractual freedom of the patties at the time of concluding de Hosting Contract, but in turn will give specific regulations that will allow safeguarding personal data.

**Key words:** Hosting, supplier, user, contract, information security, personal data, responsibility.

# TABLA DE CONTENIDO

# ÍNDICE DE FIGURAS

# INTRODUCCIÓN

En la actualidad, con los avances tecnológicos y sus infinitas posibilidades que permiten a las personas cruzar barreras para acceder a cualquier tipo de información que antes tomaba días, meses e incluso años, el derecho al acceso a la información ha cobrado más importancia. Con el transcurrir del tiempo, la información de personas se ha convertido en un activo, que cualquiera quisiera poseer con fines comerciales, a través de la web a nivel global, de modo irrestricto e ilimitado.

Es así como las nuevas tecnologías y su evolución, han impuesto –en contraparte– la obligación de resguardar la información y limitar su acceso a los agentes económicos, razón por la cual el Derecho viene adquiriendo cada vez mayor importancia, ya que busca resguardar los datos e información sensible de las personas, a través de mecanismos de seguridad de la información que tutelen sus derechos.

En ese sentido, el comercio electrónico ha creado nuevas figuras contractuales como el *contrato de hosting*, el cual implica un traspaso de información del titular del banco de datos personales a un servidor web, que es proporcionado por un prestador/proveedor para la utilización del primero. Esta figura contractual permite agilizar procesos, debido a que delega en un tercero la seguridad, custodia y creación de una página web, sin –podría suponerse así– responsabilidad del titular del banco de datos personales por cualquier transgresión al deber de seguridad de la información.

El *contrato de hosting* cada vez tiene mayor acogida en el Perú, por lo que merece una revisión de la legislación nacional actual, entre ellas la Ley de protección de datos personales y su Reglamento, para analizar si dicha norma se encuentra acorde con las necesidades del comercio electrónico, sin vulnerar el principio del deber de seguridad de la información; o delega libremente, sin ninguna limitación, a las partes de la relación contractual, la potestad de regular sus derechos, obligaciones y responsabilidades.

En atención a lo expuesto, la hipótesis de este trabajo es la siguiente:

- Si la Ley de Protección de Datos Personales y su Reglamento son herramientas legales que pueden ser aplicadas o no al 'contrato de hosting'; y si protegen la finalidad del contrato, esto es, el traspaso de información que el titular del banco de datos personales le brinda al proveedor para la colocación de dicha información en la web.

- Si en el supuesto de incumplimiento en el deber de seguridad de la información la responsabilidad recaerá únicamente en el proveedor del servicio que guarda el banco de datos; o si este es un riesgo propio del negocio, que deberá ser asumido por el titular del banco de datos personales.

Para indagar sobre las referidas cuestiones, se desarrolla el presente trabajo, que se divide en tres capítulos. En el primero, se analiza de modo exclusivo el *contrato de hosting* y su implicancia a través del servidor web, sus elementos y su regulación vigente; para luego abordar, en el segundo capítulo, los antecedentes legislativos sobre la Ley de Protección de Datos Personales y la importancia del principio de seguridad de la información. Mientras que, en el tercer capítulo, se examinan modelos de cláusulas contractuales sobre la referida figura atípica, con el fin de determinar las obligaciones y responsabilidades que las partes acuerdan ante un eventual supuesto de vulneración al deber de seguridad de la información. Todo ello para verificar si la actual legislación nacional aborda con suficiencia los retos que plantea esta nueva y recurrente figura contractual, para luego compararla con otras normativas más avanzadas sobre dicho tema.

Por último, en recomendaciones, se propone un mecanismo legal más eficiente que garantice, sin limitar el derecho de libertad contractual de las partes, el resguardo de los datos del titular de la información. Asimismo, se presentan supuestos de responsabilidad de las partes que forman parte de la relación jurídica del *contrato de hosting*, brindando además posibilidades de solución frente a una posible falta y/o infracción que ponga en riesgo o vulnere el deber de seguridad de la información, y quién debe responder por aquello ante la autoridad administrativa y/o el titular de los datos personales.

# CAPÍTULO I: SOBRE EL CONTRATO DE HOSTING

El presente capítulo tiene como fin brindar al lector una noción básica y general del *contrato de hosting*, que día a día adquiere mayor protagonismo con el avance de la tecnología, ya que esta ha permitido ofrecer, a través de la web, un nuevo canal de ventas de bienes y servicios que los usuarios requieran. Es así que, por su relevancia y utilidad, esta figura contractual ha generado que las partes deban adaptar a través de la práctica comercial las cláusulas, elementos y sus obligaciones, a la finalidad que buscan obtener del mencionado contrato, sin un respaldo o regulación legislativa que se aplique en el ordenamiento jurídico peruano.

## 1.1. Definición

A pesar de lo que se puede considerar de los usos y costumbres, el *contrato de hosting* no es un contrato de arrendamiento otorgado en un servidor de la red; por el contrario, está más relacionado con la prestación de un servicio, por medio del cual una persona natural o jurídica pone al servicio de otra persona (natural o jurídica) un espacio de un servidor conectado a internet, para que este sirva de almacén de datos y traspaso de información, y a la vez posibilite su acceso continuo en línea por parte del cliente, contándose siempre con el respaldo del proveedor que brinda el espacio en el sistema digital.

Una definición que completa el detalle y características de este tipo de acuerdos es el ofreció Aguilar (2009):

> El hosting es un servicio remunerado o gratuito, mediante el cual una persona o una empresa pone al servicio de otra un espacio dentro de un servidor conectado a internet. De tal manera que los datos e información alojados en este espacio, las páginas web, pueden ser accedidos en línea. (p. 110)

Otra definición encontrada sobre el referido acuerdo es:

> El contrato de hosting regula el alojamiento de información y la conexión con redes de telecomunicaciones. Una de las partes demanda el espacio lógico para el almacenamiento de datos y software en equipos

> informáticos, y el acceso a esta información por medio de redes de telecomunicaciones abiertas o cerradas. A través de este contrato, se pone a disposición de la parte que no posee equipos informáticos para determinados servicios, la contratación de un espacio lógico en un disco duro de un equipo informático de la otra parte, que a su vez hace de servidor (dedicado o compartido), al tener acceso remoto a dicho espacio lógico, para alojar tanto datos como software. (Gómez-Juárez, 2007, p. 22)

De modo general, debe señalarse que este contrato responde a una contratación informática más relacionada con la prestación de un servicio que con un simple espacio cedido en la red para uso del usuario. Asimismo, que su aplicación depende única y exclusivamente del uso de la internet y de otras redes de comunicación electrónica para su suscripción y ejecución de la prestación, en razón de que el mencionado acuerdo tiene una aplicación relaciona solo a través de una plataforma virtual, de la manera cómo se detallará más adelante.

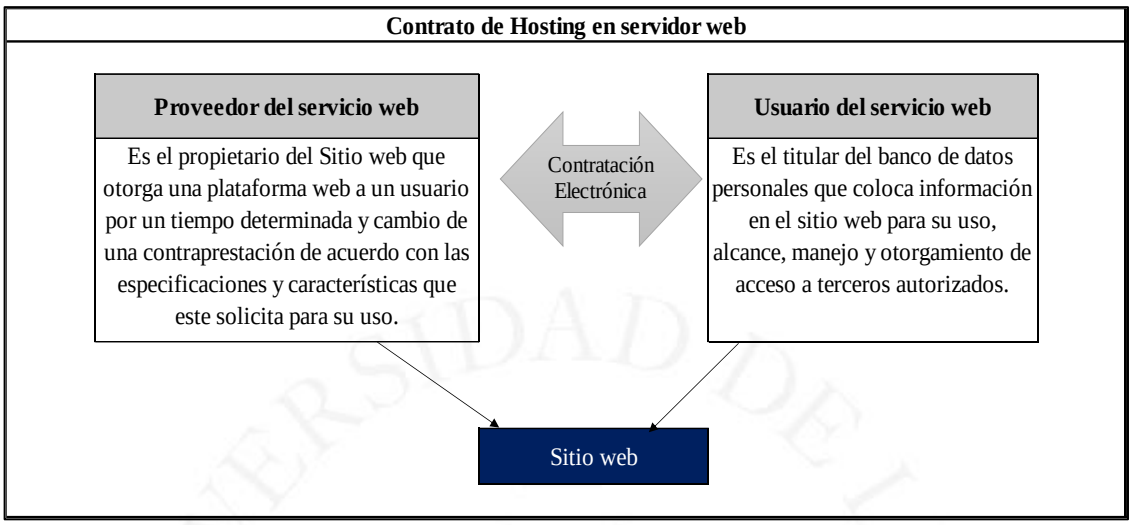
De la misma manera, complementando la definición descrita, es necesario precisar que el *contrato de hosting* puede alcanzar un objeto más amplio que la simple prestación de un servicio de almacenamiento de datos, pues al ser un contrato atípico permite que las partes puedan acordar servicios accesorios o complementarios que generen diferentes obligaciones y responsabilidades entre ellas, conforme expuso Romero (2009):

> El contrato de hosting tiene como objeto básico o característico la prestación de servicio de alojamiento o almacenamiento de datos, pero es usual en el tráfico que la relación contractual que se establece entre el operador de servicios de la sociedad de la información y su cliente tenga un carácter más amplio, alcanzando también una serie de servicios de carácter accesorio o complementario de la prestación de servicios de almacenamiento de datos. Entre otros servicios de este carácter, pueden enunciarse: la conexión a Internet [sic], la creación y desarrollo de un sitio web, el servicio de recuperación de datos, el asesoramiento y la asistencia técnica, o cualesquiera otros servicios de intermediación de la sociedad de la información. (p. 33)

A continuación, se presenta la Figura 1.1., que detalla el objeto y función del *contrato de hosting*.

**Figura 1.1**

*Objeto y función del contrato de hosting*




En ese sentido, se puede comprobar que el *contrato de hosting* sirve como un mecanismo para que las empresas usuarias contraten a un proveedor/operador de servicios de la información a efectos de liberar recursos propios, y de esa manera externalizar el desarrollo de actividades y funciones de comercio electrónico en un operador cuya obligación principal estará relacionada en garantizar la continuidad, calidad y seguridad de la información que se aloje en dicho sitio web.

Por último, en internet se encontró diversos ejemplos de servidores de hosting que cumplen con el objeto anteriormente señalado, entre ellos:

- **GoDaddy:** Es una plataforma digital por medio del cual, a cambio de una contraprestación, los usuarios pueden usar un espacio web, el mismo que pueden configurar para publicitar algún bien o servicio.
- **HostGator:** Es una plataforma digital que provee una variedad de herramientas para que los usuarios puedan desplegar sus negocios en línea.
- **NetworkSolutions:** Es una plataforma digital que ofrece diferentes servicios desde optimizaciones, publicidad *online* y redes sociales para generar publicidad y *marketing* a la empresa contratante.

- **DreamHost:** Es una plataforma digital que crea páginas web para empresas de acuerdo con las necesidades que estos requieran: diseños, publicidad, manejo y más.

### 1.2. Elementos esenciales

Sobre este punto, debe señalarse que el *contrato de hosting* abarca, como todos los contratos, un elemento subjetivo y un elemento objetivo. El primero está vinculado con los sujetos que celebran el acuerdo, los mismos que independientemente de si son los proveedores o clientes, dichos sujetos podrán ser personas naturales o jurídicas, no requiriendo de ningún requisito o cualidad especial para la suscripción del contrato.

Por otro lado, el elemento objetivo está relacionado con el contenido mínimo esencial, que debe regular el contrato de hosting, que abarca, según Aguilar (2009), los siguientes contenidos:

- **Título oneroso o gratuito:** El contrato de hosting no necesariamente se suscribe a cambio de una retribución. Si bien existe un número importante de contratos de hosting suscritos a título oneroso, estos contratos podrían ser suscritos también a título gratuito. Es este último caso, es común que el proveedor del servicio de hosting proporcione una cantidad muy limitada de transferencia y de espacio en el servidor, y que se establezcan cláusulas que le permitan al proveedor contar con la facultad de incorporar avisos publicitarios en las páginas web del usuario [1] […].
- **Obligación de brindar alojamiento:** La obligación principal del proveedor del servicio de hosting es facilitar al usuario un espacio dentro de un servidor conectado a internet. Este servicio de alojamiento implica, por parte del proveedor, obligaciones de otorgar facilidades técnicas necesarias para el sitio web alojado pueda ser accesible a través de Internet […].

[1] Un ejemplo de ello es la página Wix.com.

- **Finalidad:** El acceso a los datos e información (página web) alojados en línea por parte del cliente desde cualquier computador remoto. (p. 110)

De esa manera, a pesar de que el *contrato de hosting* es un contrato atípico, toda vez que carece de regulación expresa en la normativa vigente[2], tiene una figura utilizada de modo recurrente en el Perú, lo cual ha conllevado a descifrar y regular, tácitamente, los elementos esenciales que las partes deben considerar al momento de suscribir un acuerdo.

Y es que la práctica ha conllevado que las partes regulen por los usos y costumbres los elementos y aspectos necesarios que este acuerdo debe tener, lo cual podría descifrar que este contrato, a pesar de ser atípico legalmente, cuente con tipicidad social. O sea, que sus reglas vengan a ser dadas por los usos y costumbres comerciales impuestas por las partes.

Por otro lado, también debe señalarse que sobre la base de los elementos anteriormente descritos podría suponerse que el *contrato de hosting* y el servidor *Cloud Computing* sean lo mismo. No obstante, dicha suposición no es exacta, ya que el *Cloud Computing* funciona como un almacenamiento masivo de datos en varios servidores de internet encargados de responder peticiones en todo momento, siendo que ahí radica la diferencia con el *contrato de hosting*, toda vez que la información almacenada en este no es compartida y se encuentra alojada en una sola unidad; mientras que en el servidor *Cloud Computing* la información sí se encuentra almacenada en varios servidores, por lo que la pérdida de información es casi nula (Latam, 2018).

> Asimismo, otra diferencia característica entre el *Hosting* y el *Cloud Computing* es que en el primero el proveedor ofrece recursos exclusivos en un ambiente que puede hospedar aplicaciones, soluciones de tecnología e información o activos, donde la responsabilidad de administrar tareas de manutención y conservar todo funcionando es papel del proveedor. Por ello, el proveedor que ofrece estos servicios cuenta con la infraestructura tecnología necesaria. En ese sentido, en contraparte, el *Cloud Computing* es un mero almacenamiento de datos y aplicaciones en la nube, que no

[2] De modo específico, el contrato de hosting solo se menciona en la norma tributaria en el Art. 4°A del Reglamento de la Ley de Impuesto a la Renta, aprobado mediante el D.S. 122-94-EF.

> exige servidores locales para lidiar con los datos, siendo que su demanda de espacio crece en base a las necesidades del cliente. (Latam, 2020)

Por último, otra diferencia resaltante es que en el «*Cloud Computing* el usuario paga por la cantidad que usa, siendo que en base a la demanda de almacenamiento existen escalas, mientras que en el *contrato de hosting* la contraprestación es un monto fijo conforme el modelo web creado» (Latam, 2020).

En ese orden de ideas, debe señalarse que el futuro y las nuevas tecnologías están permitiendo la creación de nuevas figuras contractuales que suponen una mezcla de los negocios jurídicos que a la fecha se tienen, como el *Hosting Cloud*, que es una combinación de ambos contratos, razón por la cual es importante que la legislación se adapte a estas necesidades del mercado que cada día van desarrollándose. Y esto por la exigencia de la globalización de una normativa que regule y delimite los aspectos fundamentales del resguardo y protección de la información personal y sensible que se coloca y traspasa a dichos servidores.

### 1.3. Legislación aplicable al Perú

Conforme se expresó en los párrafos anteriores, el *contrato de hosting* es un contrato atípico. Sobre el particular, Aguilar (2009) señaló que:

> Si bien es cierto la norma tributaria, en específico el artículo 4-A del Reglamento de la Ley del Impuesto a la Renta, define el almacenamiento de páginas de Internet o website hosting, esto no convierte al *contrato de hosting* en una figura típica en nuestro país. En efecto, para considerar a una figura como contrato típico, no basta una simple referencia a la figura contractual o una simple definición contenida en un glosario de términos, sino que resulta necesario que el contrato cuenta con una regulación particular propia, dada por la ley. (p. 112)

El *contrato de hosting* no tiene tipicidad legal, pues no está regulado en la legislación peruana, y no se enmarca dentro de las figuras típicas legales existentes en la actualidad. Por tales consideraciones, es a través de la práctica comercial y la voluntad de las partes que el *contrato de hosting* establece sus condiciones, prevaleciendo la voluntad de las partes conforme lo dispone el Art. 1354° del Código Civil Peruano.

Así, la práctica comercial ha establecido ciertos aspectos relevantes que deben considerarse al momento de suscribir un contrato de hosting, como sugirió Aguilar (2009):

1. **Ancho de banda digital:** La garantía de un mínimo de capacidad de tráfico para la transferencia de datos en un determinado periodo (generalmente mensual). El ancho de banda digital es muy relevante, pues determinará, por ejemplo, el número de usuarios que pueden acceder al mismo tiempo a la página web del cliente […].
2. **Sistema operativo y lenguaje de programación por utilizar:** La modificación por parte del proveedor del sistema operativo o del lenguaje de programación puede implicar para el cliente costos técnicos de adaptación muy importantes. Por ello, debería especificarse en el Contrato de Hosting tanto el sistema operativo como el lenguaje de programación que se utilizará.
3. **Soporte técnico:** El Contrato de Hosting debería contener la disponibilidad, los medios y las acciones de soporte técnico que incluye. Las acciones de soporte técnico permitirán al cliente solucionar los inconvenientes que se pudieran presentar durante la vigencia de su contrato de hosting.
4. **Seguridad:** El sistema operativo debe cumplir con el «Libro Naranja» del Departamento Nacional de Seguridad Informática de los Estados Unidos, que es considerado el estándar para la evaluación de la seguridad informática. Asimismo, será muy importante que se detalle el sistema de seguridad del proveedor, tanto a nivel físico (instalaciones, vigilancia) como lógico (contrafuegos, *routers*), el mecanismo para la gestión de incidencias (ataques contra el sistema) y la realización de los chequeos. (p. 115)

# CAPÍTULO II: SOBRE LA LEY DE PROTECCIÓN DE DATOS PERSONALES Y SU REGLAMENTO

El presente capítulo tiene como fin brindar al lector las nociones básicas de la Ley de Protección de Datos Personales, la misma que al ser publicada tardíamente en comparación a otras legislaciones –como la aprobada por el Parlamento del *Land* alemán de Hessen en 1970, y de países como Suecia, Estados Unidos, Nueza Zelanda, Canadá y gran parte de los países europeos–, buscó crear una regulación que estableciera las reglas de recopilación, utilización y transmisión de datos personales solo por medio del consentimiento expreso de su titular, el cual debe ser libre, inequívoco e informado.

En ese sentido, la norma desarrolla un derecho fundamental nuevo que anteriormente la legislación peruana no contemplaba y de modo vago la doctrina local explicaba como el derecho a la «autodeterminación informativa», el mismo que, de acuerdo con Safria (2013):

> […] es un derecho más amplio que el derecho a la privacidad, a partir del cual se origina (y que protege básicamente frente a intromisiones indebidas), pero que ha ganado autonomía, y hoy otorga a los individuos el control sobre el flujo de su información personal, sujeto únicamente a ciertas excepciones de orden público. (p. 13)

De esa manera, se analizará el respaldo normativo que establece la Ley de Datos Personales y sus alcances, haciendo énfasis es un principio fundamental que contempla la mencionada norma, como es el principio de seguridad de la información; derecho y garantía que resulta fundamental cuando se comparte e intercambia información personal entre las partes de una relación contractual.

## 2.1. Antecedentes de la Ley de Datos Personales

El antecedente más remoto de la Ley de Protección de Datos Personales se halla en el inciso 6 del Art. 2° de la Constitución Política, el cual reconoce que toda persona tiene derecho a «que los servicios informáticos, computarizados o no públicos o privados no suministren informaciones que afecten la intimidad personal y familiar». Es así que, desde la Carta Magna, se ha regulado la protección de los datos personales; agregándose

el Art. 200° que crea el Habeas Data, garantía que «procede contra el hecho u omisión, por parte de cualquier autoridad, funcionario o persona, que vulnera o amenaza los derechos a que se refiere el Art. 2°, incisos 5 y 6, de la Constitución.»

Al respecto, puede señalarse que la protección de los datos personales ha existido en el país desde hace más de 20 años. Sin embargo, recién el 3 de abril del 2011 salió publicado en el Diario Oficial «El Peruano» la Ley 297330, Ley de Protección de Datos Personales, la cual estableció los términos y condiciones sobre el tratamiento de los datos personales, asegurando un marco de respeto conforme a los demás derechos fundamentales regulados y garantizados en la Constitución Política del Perú.

Es en aras de garantizar los datos personales de los titulares, la norma contempló los famosos derechos 'ARCO'»:

- **Derecho de acceso:** Por medio del cual el titular puede solicitar y acceder a la información que sobre sí mismo sea objeto de tratamiento en bancos de datos.
- **Derecho de rectificación:** Por medio del cual el titular puede actualizar o completar sus datos personales faltantes o modificados.
- **Derecho de cancelación:** Por medio del cual el titular puede solicitar la eliminación de sus datos personales.
- **Derecho de oposición:** Por medio del cual el titular puede oponerse al tratamiento de sus datos, cuando existan motivos fundados y legítimos de que aquellos están siendo usados para fines distintos a los otorgados.

Asimismo, la mencionada norma dispuso la creación de la Autoridad Nacional de Protección de Datos Personales, adscrita al Ministerio de Justicia, siendo que la función principal de dicha entidad es realizar todas las acciones necesarias con el fin de velar por el cumplimiento de la normativa sobre protección de datos personales.

Luego, el 20 de abril del 2012, se publicó en el Diario Oficial «El Peruano» el D.S. 011-2012-JUS, Reglamento de Organización y Funciones del Ministerio de Justicia y Derechos Humanos, por medio del cual se creó un órgano denominado Dirección General de Protección de Datos Personales, adscrito al Despacho Viceministerial de

Derechos Humanos y Acceso a la Justicia, llamado también Autoridad Nacional de Protección de Datos Personales, que cuenta con cuatro unidades orgánicas[3].

A su vez, el 22 de marzo de 2013 también se publicó el D.S. 003-2013-JUS, que aprobó el *Reglamento* de la Ley 29733, Ley de Protección de Datos Personales, que entró en vigencia el 8 de mayo de 2013. Con esa norma, el mencionado reglamento permitió regular los alcances de la ley estableciendo definiciones, procedimientos, infracciones y sanciones para quienes vulneren los alcances contenidos en la normativa mencionada.

Por último, están los últimos cambios legislativos a la Ley de Protección de Datos Personales y su Reglamento, regulados por el D. Leg. 1353, del 7 de enero del 2017, que busca fortalecer el ejercicio de dos derechos constitucionalmente reconocidos: el derecho al acceso a la información pública y el derecho a la protección de datos personales, que pueden entrar en conflicto en ciertas situaciones, por lo que se dispuso la creación de un Tribunal de Transparencia y Acceso a la Información Pública.

Por tales consideraciones, puede observarse que la protección de datos personales y, sobre todo, de la información digital, siempre ha sido resguardada por la normativa nacional. Empero, la falta de definiciones, procedimientos, condiciones, sanciones, entre otros, ha obligado la implementación de una normativa especial en los últimos diez años. En contraste con los países de primer mundo, al Perú le ha tomado más de 30 años crear y aplicar una regulación específica adaptada al avance digital de esta era[4].

### 2.2. Sobre el deber de seguridad de la información

El Art. 9° de la Ley de Protección de Datos Personales y el Art. 10° de su Reglamento han regulado el principio de seguridad, el mismo que se define como una obligación del titular de banco de datos personales, así como del encargado de su tratamiento de adoptar todas las medidas técnicas, organizativas y legales que garanticen la seguridad de los datos personales.

[3] Dirección de Registro Nacional de Protección de Datos Personales, Dirección de Sanciones; Dirección de Supervisión y Control, y Dirección de Normatividad y Asistencia Legal.

[4] Las primeras leyes de protección de datos personales fueron aprobadas en la década de los años 70 en países como Alemanda, Suecia, Estados Unidos, Nueza Zelanda, Canadá y en gran parte de los países europeos.

En efecto, el dictamen del proyecto de la Ley de Protección de Datos Personales describe que los principios contenidos en dicha norma «tienen la estructura de mandatos de optimización [que] no determinan exactamente lo que debe hacerse, sino que ordenan que algo sea realizado en la mayor medida posible, dentro de las posibilidades jurídicas y reales existentes […]. Orientan y determinan el comportamiento de todos los que van a participar en el tratamiento de datos personales, señalando las reglas de conducta que ellos deben observar.»

No obstante, a pesar de que el proyecto de la norma regula que los principios parecieran más guías de acción, en la práctica las cataloga como normas imperativas cuyo incumplimiento acarrea sanciones para sus infractores. En ese sentido, es ahí donde radica la importancia en el desarrollo de este principio rector, el mismo que es de obligatorio cumplimiento y conlleva un desarrollo en el presente capítulo.

Al respecto, debe señalarse que conforme lo dispone la Dirección de Datos Personales respecto a este principio, esta entidad busca que el actor que brinda tratamiento a los datos personales tenga una actividad más activa sobre los mismos; es decir, que el titular del banco de datos realice y tenga medidas técnicas, organizativas y legales necesarias e indispensables para garantizar la confidencialidad, integridad y disponibilidad de los datos, para evitar su adulteración, pérdida, extracción, desviación, entre otras situaciones que pudieran generar un perjuicio y por ende una responsabilidad por el daño causado con el propietario de los datos personales.

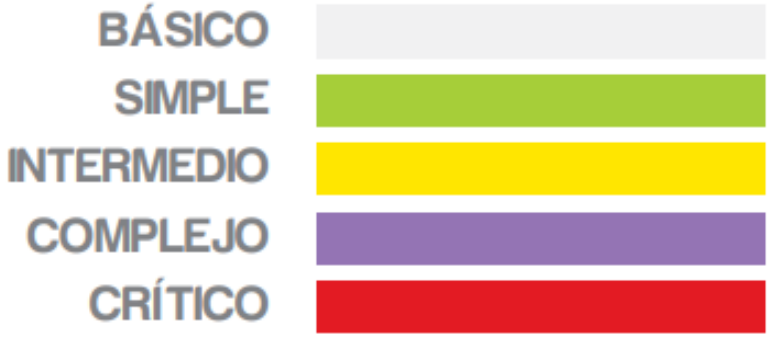
Siguiendo esta línea, en noviembre de 2013, la Autoridad Nacional de Protección de Datos Personales emitió la Primera Edición de la Directiva de Seguridad, la misma que señaló que el Titular del Banco de Datos Personales es responsable de lo siguiente:

a. De otorgar y mantener el nivel suficiente de protección a los datos personales contenidos en el banco de datos personales que tenga bajo su titularidad.
b. De la determinación y cumplimiento de la finalidad y del contenido del banco de datos personales bajo su titularidad.
c. Del tratamiento de los datos personales contenidos en el banco de datos personales bajo su titularidad.
d. Garantizar el cumplimiento de los derechos del titular de los datos personales conferidos en la Ley 29733, Ley de Protección de Datos Personales.

De esa manera, en virtud de la responsabilidad directa que la directiva y la norma le otorgan al titular del banco de datos personales, se han establecidos medidas de seguridad bajo criterios de riesgo que buscan prevalecer y mantener el respeto del principio de seguridad de la información (Minjus, 2013), como la que se muestra en la Figura 1.2.

**Figura 2.1**

*Medidas de seguridad de la información bajo criterios de riesgo*




*Nota*. De «Directiva de seguridad. Autoridad Nacional de Protección de Datos Personales-APDP» (p. 8), por el Ministerio de Justicia y Derechos Humanos del Perú (Minjus), 2013. (https://www.minjus.gob.pe/wp-content/uploads/2014/02/Cartilla-de-Directiva-de-Seguridad.pdf)

Sobre lo anterior, la autora de esta investigación también coincide con Alvarado (2016), acerca de la importancia que recae en el principio de seguridad de la información, el mismo que busca lo siguiente:

- Facilitar la implementación de una gestión en continua evaluación que, mediante la categorización de los bancos de datos personales en razón a los riesgos que conlleva su sensibilidad y el tratamiento dado, complemente las medidas técnicas.
- Informar a los usuarios para que tomen conciencia de la protección requerida.
- Exigir un nivel de seguridad equilibrado entre los riesgos, las técnicas de seguridad y el costo de las medidas.

En ese orden de ideas, debe señalarse que, conforme lo dispone el numeral 19 del Art. 2°[5] de la Ley de Protección de Datos Personales, es responsable del tratamiento quien

[5] 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.

decide sobre el mismo, aun cuando los datos no formen parte de un banco, y es el encargado del tratamiento quien lo realiza, pudiendo ser el propio titular del banco de datos personales u otra persona (tercero) designada por el titular, en virtud de una relación jurídica que los vincule y delimite el ámbito de su actuación; incluyendo a quien lo realice por orden del responsable del tratamiento.

He ahí la importancia en el cumplimiento de la toma de medidas para brindar una adecuado deber de seguridad de la información, toda vez que la falta de toma de medidas preventivas y correctivas constituye no solo una vulneración a la normativa de la Ley de Protección de Datos Personales, sino un riesgo y una vulneración a los derechos constitucionales del titular de la información, el mismo que no necesariamente es quien almacena, trata o controla sus datos, pues esta responsabilidad puede recaer en terceros designados por el titular del banco de datos.

Por tales consideraciones, existe coincidencia y reiteración en que la información es uno de los activos más valiosos del presente siglo, y su respeto debe ser fundamental, por lo que la norma y sus directivas deben estar reinventándose conforme los avances tecnológicos. Así, la única forma de prevalecer y mantener la seguridad de la información es a través de la implementación de un conjunto adecuado de controles, que pueden ser políticas, normas, procedimientos, estructuras organizativas, equipos, prácticas y funciones de *software*, entre otros, cuya responsabilidad no solo debe recaer en el titular del banco de datos personales, sino en la autoridad que los fiscaliza y los proveedores o terceros que tienen acceso, control, estructuración, disposición y supervisión en el manejo y control de los datos.

# CAPÍTULO III: NOCIONES BÁSICAS DE LA LEY DE DATOS PERSONALES Y CÓMO SE COMPLEMENTA CON EL CONTRATO DE HOSTING

El presente capítulo tiene como objeto brindar al lector el detalle de la aplicación práctica de cómo en el Perú la Ley de Protección de Datos Personales y su Reglamento se complementan con el *contrato de hosting*. Asimismo, si los acuerdos que celebran las partes y la legislación son fuentes de derecho de suficiente relevancia para proteger los derechos de las partes de la relación jurídica y terceros, así como para delimitar la responsabilidad entre los mismos.

De la misma manera, se evaluará cómo viene siendo tratada la regulación del *contrato de hosting* en otros países para brindar al lector fuentes de derecho alternativas que permitan afrontar la realidad de un contrato que, sobre la base de los avances tecnológicos, viene adquiriendo más relevancia y por ende requiere de una regulación más adecuada que satisfaga los intereses de la sociedad.

## 3.1. Aplicación práctica: análisis de modelo de cláusulas

La práctica en la revisión de cláusulas sobre protección de datos personales permite de manera genérica llegar a las siguientes conclusiones:

a. La prohibición genérica de ambas partes de ir en contra de lo dispuesto en la Ley 29733 y su Reglamento.
b. Permitir la divulgación de datos en los siguientes casos: (i) Cuando la información sea de conocimiento público; (ii) cuando la información haya sido solicitada por un tercero, contando para ello con el consentimiento previo y por escrito de la otra parte; (iii) cuando la información haya sido solicitada por las autoridades judiciales.
c. Indicar que la parte que incumpla lo dispuesto en la cláusula de protección de datos personales, será requerido por la parte afectada, la cual le podrá solicitar una indemnización por daños y perjuicios.

De esa manera, dichos tres preceptos se encuentran siempre en la cláusula genérica de protección de datos personales que las partes consignan en sus contratos

genéricos, y en específico en los contratos de hosting, pero… ¿qué quiere decir esta cláusula? ¿Quién tiene la obligación de resguardar la información y mantener su seguridad frente a cualquier intromisión de terceros? ¿Existe la responsabilidad solidaria, o solo el proveedor del servicio es responsable? ¿Es posible delimitar la responsabilidad? ¿Es posible mitigar la responsabilidad y/o que las partes se eximan de ella?

Estas son todas las interrogantes que, ante la falta de detalle y acuerdo de las partes, la ley debe brindar una solución que permita al titular de los datos personales resguardar sus derechos.

Sobre el particular, conforme se indicó en los párrafos anteriores, el *contrato de hosting* es un contrato con tipicidad social; esto porque su regulación está sujeta a los usos y costumbres de las partes. Sin embargo, como se indicó en el punto anterior, las partes no siempre regulan todas las connotaciones que puede implicar un tema tan novedoso como es el *contrato de hosting*.

Es así que, en aplicación del Art. 1353° del Código Civil, si en el marco de un *contrato de hosting* lo pactado por las partes no otorgara solución a un supuesto determinado y tampoco se encontrara respuesta en los usos y costumbres, entonces recién quedaría habilitada la aplicación de las reglas generales de los contratos y además las normas relativas a las obligaciones según la naturaleza de las prestaciones involucradas (dar, hacer o no hacer).

Al respecto, conforme lo señala el Art. 139° inciso 8 de la Constitución Política del Perú, los jueces no pueden dejar de administrar justicia por defecto o deficiencia de la Ley. En ese sentido, de presentarse un caso como el mencionado, el juez debe apelar a los criterios doctrinarios. En dicho caso, Aguilar (2009) señaló que el juez puede acudir a las ‘normas de los contratos afines’, que son: (i) Teoría de la absorción, (ii) teoría de la combinación y (iii) teoría de la aplicación analógica.

La primera –la teoría de la absorción– implica una división de las prestaciones del contrato atípico para determinar el elemento preponderante en él y, sobre la base de ello, aplicar las normas que correspondan a dicho elemento. Es decir, que al *contrato de hosting* se le pueden aplicar las normas del contrato de cesión en uso; o si es gratuito u oneroso podría ser de arrendamiento o comodato. Sin embargo, esto no quiere decir que el *contrato de hosting* sea un contrato de arrendamiento o comodato, sino que implica utilizar las normas de estos para llenar un vacío normativo o de las partes.

La teoría de la combinación implica segmentar todas las prestaciones del contrato atípico, y a cada una de ellas aplicar supletoriamente las normas del contrato a la cual pertenecen. En efecto, si el *contrato de hosting* es a título oneroso, se le podrían aplicar las reglas del contrato de arrendamiento, siendo que para las prestaciones vinculadas con el almacenamiento dentro del espacio del servidor web se le aplicarán las normas de prestación de servicios (podrían ser las normas del contrato de obra o de locación de servicios según corresponda).

Por último, la teoría de la aplicación analógica analiza todas las prestaciones como un conjunto del contrato, para aplicar el contrato típico que más se le asemeje. En ese sentido, aplicando esta teoría, podría decirse que el *contrato de hosting* se asemeja en su mayoría a un contrato de arrendamiento o de prestación de servicios. Sin embargo, se precisa que esto no significa que sea un contrato igual a dichas figuras típicas.

De esa manera, dependiendo de la situación acontecida, es decir, de la omisión o interpretación que se debe dar a la cláusula o contrato en general para definir la voluntad o la prestación que deba ser cumplida, será responsabilidad del órgano jurisdiccional determinar la teoría que corresponde aplicar al caso para poder dilucidar la omisión o la interpretación correcta que no vulnere la voluntad de las partes ni a la regulación vigente materia de resguardo sobre los datos personales.

### 3.2. Seguridad de la información y obligaciones de las partes

El Art. 9° de la Ley 29733, Principio de Seguridad, establece que el titular del banco de datos personales y el encargado de su tratamiento deben adoptar las medidas técnicas, organizativas y legales necesarias para garantizar la seguridad de los datos personales. Luego, el Art. 16° de la mencionada norma señala que, para los fines del tratamiento de datos personales, el titular del banco de datos personales debe adoptar medidas técnicas, organizativas y legales que garanticen su seguridad y eviten su alteración, pérdida, tratamiento o acceso no autorizado.

En ese sentido, puede concluirse que, para la norma, en principio, el principal responsable de adoptar las medidas de seguridad y las políticas a seguir para su seguridad es el titular del banco de datos personales, siendo que el tercero encargado de su tratamiento sería responsable siempre que no cumpla con las medidas de seguridad encargadas por el titular del banco de datos personales. Pero la cuestión es si esta

interpretación de la norma es suficiente para afirmar que si el titular de banco le informa al tercero las medidas de seguridad que deberá emplear para realizar el tratamiento de sus datos, lo cual implicaría una exención de responsabilidad.

Ahora bien, el Reglamento de la Ley 29733 es un poco más específico en las medidas, políticas y métodos que las partes deben emplear para realizar un correcto tratamiento de los datos personales, pero respondiendo a la cuestión anterior se puede concluir que no existe una exención de responsabilidad por parte del titular del banco de datos personales como del tercero que realiza el tratamiento. Es decir, ante la Autoridad Nacional de Protección de Datos Personales ambos responderán por cualquier infracción a las medidas adoptadas por la ley, siendo que la norma pone mayor énfasis en el titular del banco de datos personales como el principal encargado de cumplir con la legislación sobre la materia. No obstante lo anterior, debe señalarse que la norma peruana es genérica y tuvo como principal objetivo adecuarse a un contexto de constante cambio desde hace más de 20 años, desde la promulgación de la actual Constitución, y no tenía ordenamiento.

Conforme se indicó en párrafos anteriores, el *contrato de hosting* es un contrato con tipicidad social por lo que cabe preguntarse ¿cómo regulan las partes la responsabilidad por incumplimiento al deber de seguridad de la información? ¿Acaso aplican lo dispuesto en la norma; esto es que ambos, tanto el proveedor del servicio del hosting, como el usuario que utiliza el espacio, son responsables frente a la Autoridad Nacional de Protección de Datos Personales por infracciones a la normativa, o solo el usuario que utiliza el espacio, a pesar de estar sujeto a las disposiciones de uso del sitio web del proveedor? Son estas cuestiones sobre las obligaciones y la regulación que establecen las partes, las que deben esclarecerse para entender mejor el panorama.

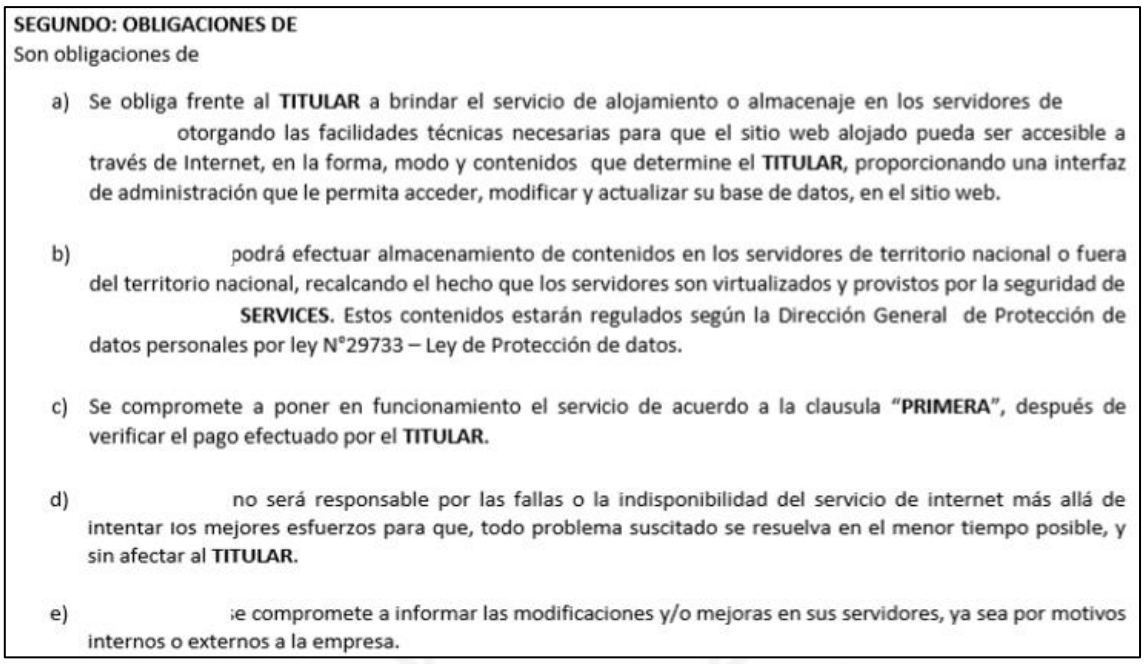
Con ese fin, en las figuras 1.3 y 1.4, se presenta el caso del contrato de una empresa dedicada al servicio de hosting a nivel internacional, cuya figura contractual se ha aplicado en diversos casos para comprobar si resuelve las interrogantes planteadas.

Debido al detalle de las obligaciones reguladas por las partes, pareciera que el único que podría encargarse del tratamiento de los datos personales es el titular del banco de datos personales, lo cual recae en la misma persona: el titular, conforme se pudo observar en los párrafos adjuntos de este modelo de contrato. Asimismo, se observa que la única obligación del proveedor del sitio web es la de brindar el servicio de alojamiento

y darle la accesibilidad al titular, pero acaso no tiene ningún tipo de responsabilidad, si existiera una falla en el sistema que ponga en riesgo los datos almacenados en él; sería solo responsabilidad del usuario que adquirió el servicio o el proveedor sí podría encontrarse en un supuesto de responsabilidad que permita equilibrar mejor el balance en beneficio de las partes. En ese sentido, se considera que, en determinadas situaciones –que se explicarán más adelante–, el proveedor del servicio sí debe responder por infracciones al deber de asegurar la información.

**Figura 0.1**

*Obligaciones del proveedor del sitio web*



**SEGUNDO: OBLIGACIONES DE**
Son obligaciones de

a) Se obliga frente al **TITULAR** a brindar el servicio de alojamiento o almacenaje en los servidores de otorgando las facilidades técnicas necesarias para que el sitio web alojado pueda ser accesible a través de Internet, en la forma, modo y contenidos que determine el **TITULAR**, proporcionando una interfaz de administración que le permita acceder, modificar y actualizar su base de datos, en el sitio web.

b) podrá efectuar almacenamiento de contenidos en los servidores de territorio nacional o fuera del territorio nacional, recalcando el hecho que los servidores son virtualizados y provistos por la seguridad de **SERVICES.** Estos contenidos estarán regulados según la Dirección General de Protección de datos personales por ley N°29733 – Ley de Protección de datos.

c) Se compromete a poner en funcionamiento el servicio de acuerdo a la clausula **"PRIMERA"**, después de verificar el pago efectuado por el **TITULAR.**

d) no será responsable por las fallas o la indisponibilidad del servicio de internet más allá de intentar los mejores esfuerzos para que, todo problema suscitado se resuelva en el menor tiempo posible, y sin afectar al **TITULAR.**

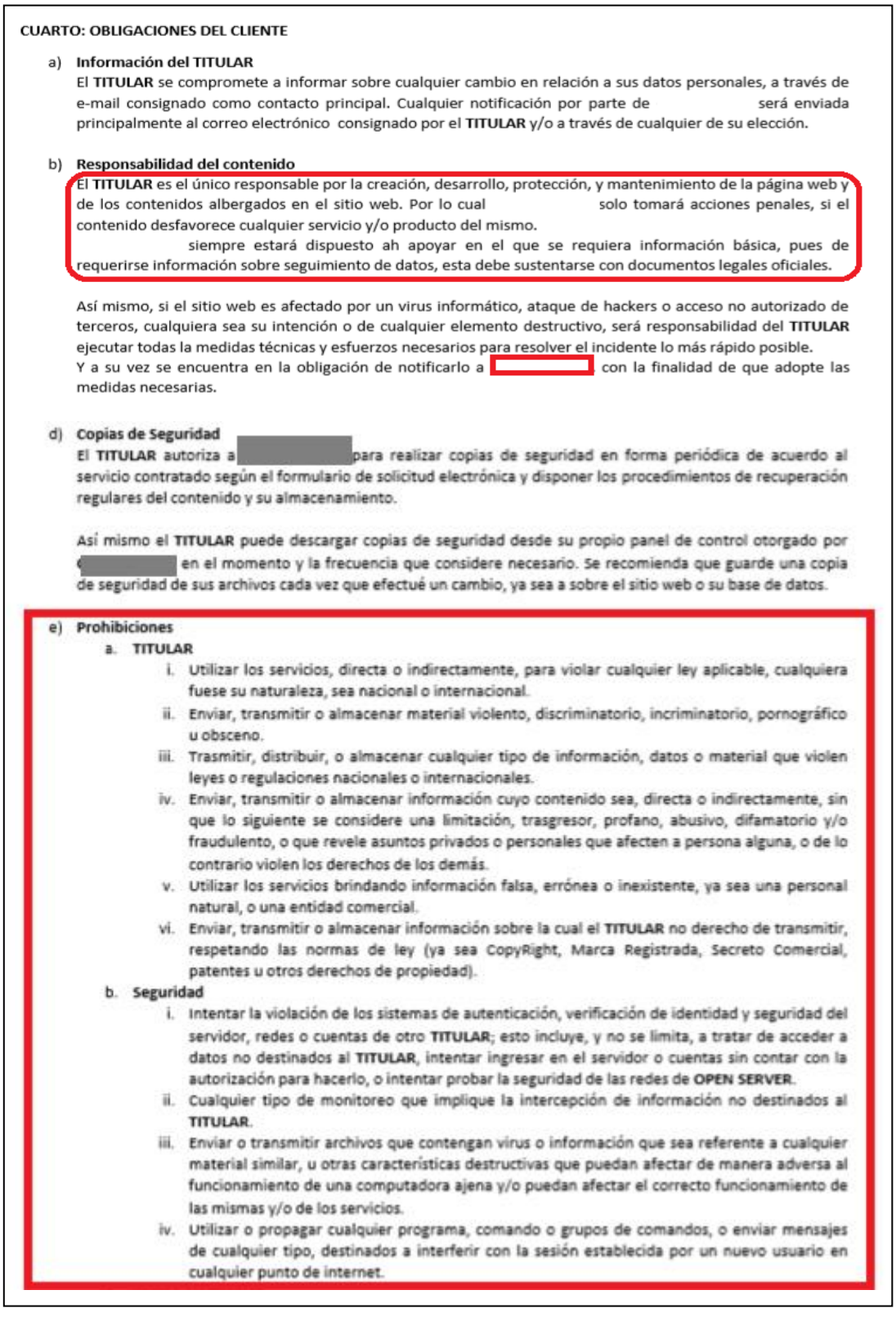
e) se compromete a informar las modificaciones y/o mejoras en sus servidores, ya sea por motivos internos o externos a la empresa.

Lamentablemente, la Ley de Protección de Datos Personales y su Reglamento no ofrecen una solución inmediata en ese escenario, y es muy posible que ante una eventual fiscalización el único responsable sea el titular del banco de datos personales que adquirió el servicio de hosting, por lo que debe recurrirse a la doctrina y a elementos adicionales que permitan dilucidar este inconveniente.

Ahora bien, con aquello no se pretende quitar importancia a la libertad contractual de las partes recogida en el Art. 1354° del Código Civil, la falta y/o limitada regulación en dicho punto no ha analizado todos los posibles escenarios que podrían recaer en el *contrato de hosting*.

**Figura 0.2**

*Obligaciones del usuario solicitante*



**CUARTO: OBLIGACIONES DEL CLIENTE**

a) **Información del TITULAR**

El **TITULAR** se compromete a informar sobre cualquier cambio en relación a sus datos personales, a través de e-mail consignado como contacto principal. Cualquier notificación por parte de será enviada principalmente al correo electrónico consignado por el **TITULAR** y/o a través de cualquier de su elección.

b) **Responsabilidad del contenido**

El **TITULAR** es el único responsable por la creación, desarrollo, protección, y mantenimiento de la página web y de los contenidos albergados en el sitio web. Por lo cual solo tomará acciones penales, si el contenido desfavorece cualquier servicio y/o producto del mismo.

siempre estará dispuesto ah apoyar en el que se requiera información básica, pues de requerirse información sobre seguimiento de datos, esta debe sustentarse con documentos legales oficiales.

Así mismo, si el sitio web es afectado por un virus informático, ataque de hackers o acceso no autorizado de terceros, cualquiera sea su intención o de cualquier elemento destructivo, será responsabilidad del **TITULAR** ejecutar todas la medidas técnicas y esfuerzos necesarios para resolver el incidente lo más rápido posible.
Y a su vez se encuentra en la obligación de notificarlo a con la finalidad de que adopte las medidas necesarias.

d) **Copias de Seguridad**

El **TITULAR** autoriza a para realizar copias de seguridad en forma periódica de acuerdo al servicio contratado según el formulario de solicitud electrónica y disponer los procedimientos de recuperación regulares del contenido y su almacenamiento.

Así mismo el **TITULAR** puede descargar copias de seguridad desde su propio panel de control otorgado por en el momento y la frecuencia que considere necesario. Se recomienda que guarde una copia de seguridad de sus archivos cada vez que efectué un cambio, ya sea a sobre el sitio web o su base de datos.

e) **Prohibiciones**

a. **TITULAR**

i. Utilizar los servicios, directa o indirectamente, para violar cualquier ley aplicable, cualquiera fuese su naturaleza, sea nacional o internacional.
ii. Enviar, transmitir o almacenar material violento, discriminatorio, incriminatorio, pornográfico u obsceno.
iii. Trasmitir, distribuir, o almacenar cualquier tipo de información, datos o material que violen leyes o regulaciones nacionales o internacionales.
iv. Enviar, transmitir o almacenar información cuyo contenido sea, directa o indirectamente, sin que lo siguiente se considere una limitación, trasgresor, profano, abusivo, difamatorio y/o fraudulento, o que revele asuntos privados o personales que afecten a persona alguna, o de lo contrario violen los derechos de los demás.
v. Utilizar los servicios brindando información falsa, errónea o inexistente, ya sea una personal natural, o una entidad comercial.
vi. Enviar, transmitir o almacenar información sobre la cual el **TITULAR** no derecho de transmitir, respetando las normas de ley (ya sea CopyRight, Marca Registrada, Secreto Comercial, patentes u otros derechos de propiedad).

b. **Seguridad**

i. Intentar la violación de los sistemas de autenticación, verificación de identidad y seguridad del servidor, redes o cuentas de otro **TITULAR**; esto incluye, y no se limita, a tratar de acceder a datos no destinados al **TITULAR**, intentar ingresar en el servidor o cuentas sin contar con la autorización para hacerlo, o intentar probar la seguridad de las redes de **OPEN SERVER**.
ii. Cualquier tipo de monitoreo que implique la intercepción de información no destinados al **TITULAR**.
iii. Enviar o transmitir archivos que contengan virus o información que sea referente a cualquier material similar, u otras características destructivas que puedan afectar de manera adversa al funcionamiento de una computadora ajena y/o puedan afectar el correcto funcionamiento de las mismas y/o de los servicios.
iv. Utilizar o propagar cualquier programa, comando o grupos de comandos, o enviar mensajes de cualquier tipo, destinados a interferir con la sesión establecida por un nuevo usuario en cualquier punto de internet.

### 3.3. Responsabilidad de las partes por vulneración al deber de seguridad de la información

Al respecto, conforme ya se abordó en puntos anteriores, en la legislación peruana es responsable de la seguridad de la información el titular del banco de datos personales y quien se encarga de su tratamiento; y quien genera una vulneración a las medidas de seguridad de la información adoptadas por la Ley 29733 y su Reglamento podría incurrir en diferentes tipos de responsabilidad, de manera simultánea, tal como se explica a continuación:

a. **Responsabilidad administrativa:** Frente a la Autoridad Nacional de Protección de Datos Personales, conforme se encuentra contemplado en los artículos 38° y 39° de la Ley 29733, en los cuales se han tipificado diversas infracciones que acarrean sanciones leves, graves y muy graves, con hasta el pago de un máximo de 50 UIT.

b. **Responsabilidad civil:** Frente al titular de datos personales, el cual puede solicitar una indemnización por los daños causados. En ese caso, se estaría ante una responsabilidad objetiva, regulada en el Art. 1970° del Código Civil, lo cual significa que no importa si la culpabilidad recae en el titular del banco de datos personales y/o en el encargado de su tratamiento. Esto, ya que solo bastaría con acreditar el daño ocasionado, a efectos de solicitar una indemnización por la vulneración de la seguridad de la información, cuyas únicas eximentes de responsabilidad están recogidos en el Art. 1972° del Código Civil. De esa manera, el sujeto solo se liberará de responsabilidad si acredita que el daño fue ocasionado por un hecho de fuerza mayor, un hecho determinante de tercero, o por la imprudencia de la víctima.

c. **Responsabilidad penal:** Frente al Estado Peruano, sobre todo cuando los datos personales son de seguridad del mismo, en el cual este es el titular de los datos. O cuando se realiza un tráfico ilegal de los datos personales pertenecientes al Estado Peruano, conforme se encuentra recogido en el Código Penal.

En suma, puede concluirse que, independientemente de quién sería el ente responsable por una infracción al deber de seguridad de la información, en determinadas situaciones, la posibilidad de incurrir en tres tipos de responsabilidad se encuentra recogida en la legislación peruana; y que dicha potestad sancionadora obliga a enfatizar la importancia de resguardar y respetar el deber de seguridad de la información.

### 3.4. Legislación comparada y su tratamiento

En la actualidad, en países como Perú, Chile, México y en general en Latinoamérica, no existe una normativa especial que regule el comercio electrónico y menos el Contrato de Hosting, toda vez que parten del principio de libertad contractual. Esto es, que las partes puedan determinar libremente el contenido del contrato, siendo que la legislación genérica (Ley de Protección de Datos Personales, Código o Ley de Protección al Consumidor, entre otras) regularán la parte fundamental de la relación jurídica.

Sin embargo, existen otras legislaciones con más desarrollo del tema, como la española, que tiene una normativa especial denominada Ley 34/2002, Servicios de la Sociedad de la Información y de Comercio Electrónico (en adelante LSSICE), la cual regula el *contrato de hosting* o de alojamiento, como lo llama la norma mencionada. En ese sentido, conforme lo indicó Solana (2005), el Art. 16° de la LSSICE formula y define los límites de la exención de responsabilidad para las actividades de hosting o alojamiento de datos; es decir, del servicio de la sociedad de información, consistente en almacenar datos facilitados por el destinatario de este servicio.

Según la norma citada, el prestador de servicios que aloja a un usuario en un sitio web sí tiene responsabilidad por la información que se almacena en sus servidores, siendo que para quedar exentos de toda responsabilidad deben incurrir en dos supuestos:

a. Que no tenga conocimiento efectivo de que la actividad o la información almacenada es ilícita o de que lesiona bienes o derechos de un tercero susceptibles de indemnización.
b. O, si lo tienen, actúen con diligencia para retirar los datos o hacer imposible el acceso a ellos.

Al respecto, Solana (2005) precisó que el primer requisito es de carácter negativo, y consiste en la falta de conocimiento efectivo de que la actividad o la información hospedada es ilícita o de que lesiona bienes o derechos de un tercero susceptibles de indemnización; en tanto que el segundo requisito es de carácter positivo, consistente en que si el prestador tiene conocimiento efectivo actúe con diligencia para retirar los datos o para imposibilitar el acceso a los mismos.

De la misma manera, el artículo referido, en su segundo párrafo, indica que se entenderá que el prestador de servicios tiene conocimiento efectivo de lo referido en el

primer supuesto, cuando un órgano competente haya declarado la ilicitud de los datos, ordenando su retirada o que se imposibilite el acceso a los mismos, o se hubiera declarado la existencia de la lesión, y el prestador conociera la correspondiente resolución, sin perjuicio de los procedimientos de detección y retirada de contenidos que los prestadores apliquen en virtud de acuerdos voluntarios y de otros medios de conocimiento efectivo que puedan establecerse.

La autora de esta investigación coincide con la opinión de Solana (2005), para quien el primer supuesto no tiene la intención de limitar las vías por las cuales el prestador podría obtener un conocimiento jurídicamente relevante, es decir, un conocimiento que lo obligue a tomar las medidas de pronta retirada o bloqueo para perder la exención de responsabilidad, ya que el artículo no impide reconocer el conocimiento efectivo adquirido por otras vías; por ejemplo, que no solo basta las vías de conocimiento tradicionales como son las resoluciones dictadas por el órgano competente que ordene el bloqueo o retirada de datos o haya declarado la existencia de lesión. También existen las vías no convencionales que implican acuerdos voluntarios-consensuados entre el usuario y el prestador, por medio de los cuales el segundo se obliga a retirar la información o bloquearla cuando se incurran en ciertos supuestos pactados por las partes, lo cual haría suponer que el prestador de servicios sí tenía conocimiento previo, por acuerdo, como debía proceder.

En definitiva, no existen vías cerradas de conocimiento efectivo, razón por la cual, dependiendo de cada caso, el juez tendría que evaluar si resultaba inminentemente evidente el conocimiento efectivo del prestador de servicios de hosting.

# CONCLUSIONES

a. Luego de analizar las normas, se llegó a la conclusión que no existe una regulación específica sobre el *contrato de hosting* en la legislación peruana, y que la normativa de datos personales tampoco tiene una disposición que regule los escenarios del comercio electrónico según la esencia del *contrato de hosting*.

b. Así, independientemente de la voluntad de las partes para limitar la responsabilidad de estas en cuanto a sus obligaciones, la legislación nacional de datos personales supone que los responsables de una eventual vulneración a los deberes de seguridad de la información serían el titular del banco de datos personales y el encargado de su tratamiento, que, según se pudo dilucidar de la definición del *contrato de hosting*, recaería en la misma persona –el 'usuario'–, razón por la cual no existirá ningún tipo de responsabilidad del proveedor del servicio del sitio web, el cual solo tiene la obligación de proveer al usuario del espacio digital para su uso.

c. La Ley de Protección de Datos Personales asume que el único responsable de velar y resguardar el cumplimiento de los métodos de seguridad de la información es el titular del banco de datos personales y del que trate los mismos, siendo que dicha figura en el *contrato de hosting* recaería en la misma persona, sin analizar si en todos los escenarios es el titular del banco de datos personales quien se encuentra en mejor posición para velar por dicho cumplimiento, sobre todo cuando el proveedor del servidor web sí podría conocer a primera mano si se está ante una información que vulnere los datos personales o cuando un tercero ingrese al servidor a realizar una acción que vulnere las medidas de seguridad de la información.

d. La falta de regulación sobre la materia en la normativa peruana ha buscado que sean las partes que conforman el *contrato de hosting* las encargadas de delimitar su responsabilidad, las mismas que buscan deslindar en todos los escenarios la responsabilidad y obligaciones del prestador del servicio web, quien solo tiene la obligación de brindar el servicio de alojamiento o almacenaje al titular del banco de datos personales, a pesar de que él mismo es titular de un servidor web de acceso libre a nivel nacional e internacional.

# RECOMENDACIONES

a. Se considera que la libertad contractual, conforme lo dispone el Art. 1354° del Código Civil, establece que las partes tienen la libertad de definir el contenido del *contrato de hosting*. No obstante, conforme lo dispone la segunda parte de dicho artículo, esta libertad está condicionada a que no sea contraria a una norma legal con carácter imperativo. En ese sentido, es pertinente que la Ley de Protección de Datos Personales y su Reglamento tengan una modificación normativa que regule los extremos del comercio electrónico, conforme lo realizó la legislación española; y no permita que las obligaciones y responsabilidades de las partes queden sujetas al libre albedrio de estas, sobre todo cuando el principio rector de esta legislación recae en velar por la seguridad de la información.

b. Al respecto, se considera que existen ciertos escenarios en los cuales el proveedor del servicio web no puede evitar eludir algún tipo de responsabilidad civil, administrativa y penal. Estos escenarios son abordados en el Art. 16° de la LSSICE y se dan:

   - Cuando el proveedor del servicio web tenga conocimiento efectivo de que la actividad o la información almacenada es ilícita o de que lesiona bienes o derechos de un tercero susceptibles de indemnización.
   - O cuando el proveedor del servicio actúa con diligencia para retirar los datos o hace imposible el acceso a ellos.

c. En los dos escenarios descritos, queda evidente que la responsabilidad es compartida por el titular del banco de datos personales, quien a su vez se encarga de su tratamiento; y por el proveedor del servicio web, quien sí tendría responsabilidad conjunta por no tener la falta de diligencia ordinaria en verificar y validar el tipo de información que se está colocando en el sitio web del cual este es titular.

d. De la misma manera, se considera que debería incluirse un tercer escenario en el cual el proveedor del servicio web también sería responsable frente a la Autoridad Nacional de Protección de Datos Personales y el titular de los datos personales, así como otras autoridades nacionales, siempre y cuando no tome las medidas de corrección y/o resguardo de la seguridad de la información, ante el ingreso e/o intromisión de un

tercero que busque obtener, sustraer y/o apoderarse de los datos personales subidos en el sistema web.

e. En efecto, a pesar de que el encargado del tratamiento y preparación de las políticas y medidas de seguridad de la información es, en el *contrato de hosting*, el titular del banco de datos personales 'el usuario', de acuerdo a lo dispuesto en los artículos 4° y 13° del Código de Protección y Defensa del Consumidor, que regula la figura de la asimetría de la información, es el proveedor que otorga el servicio de hosting al usuario, quien se encuentra en mejor posición de corregir y mejorar el sistema de seguridad de la información ante las intromisiones de terceros y no necesariamente el titular del banco de datos personales.

f. Sobre la asimetría de la información, Morales Acosta (s.f.) definió este principio de la siguiente manera:

> […] es una característica intrínseca a cualquier transacción económica (e incluso a otros aspectos sociales), en tanto que siempre en un intercambio de bienes y servicios habrá un actor mejor informado que otro. En efecto, dicho actor suele tener mayor y mejor información sobre los productos y servicios que ofrece en el mercado, lo que genera que ciertas prácticas puedan distorsionar excepcionalmente el buen funcionamiento del mismo. En términos económicos, la asimetría informativa genera costos de transacción en el mercado, los cuales deben entenderse como aquéllos en los que las partes deben incurrir para llegar a celebrar un contrato que satisfaga de la mejor manera posible sus intereses, tendiendo así a maximizar la utilidad social. (p. 5)

g. Por consiguiente, es el proveedor del servicio de hosting quien se encuentra en mejor posición y cuenta con mayor información sobre las medidas de seguridad que deben adoptarse a efectos de resguardar la seguridad de la información que el usuario coloca en la plataforma web, por lo que su responsabilidad es intrínseca a la idoneidad del servicio que ofrece, el cual no solo es el otorgamiento de un servidor web, sino de recomendar y modificar aquella plataforma en aras de que realice todas las diligencias posibles de resguardo y custodia de los datos que se encuentran contenidos en el servidor y que manipula el usuario.

# REFERENCIAS


Aguilar, A. F. (2009). El contrato de hosting. Apuntes acerca del contrato de alojamiento de un sitio. En *El impacto de las innovaciones tecnológicas en el Derecho Privado* (pp. 96-115). Lima: Universidad Peruana de Ciencias Aplicadas (UPC).

Alvarado, F. J. (2016). La gestión de la seguridad de la información en el régimen. *Foro Jurídico*, 26.

Gómez-Juárez, I. (2007, enero). Los contratos informáticos de hosting y housing en relación con la normativa española de protección de datos de carácter personal. *Revista de Contratación Electrónica*, 78, pp. 3-39. Recuperado de https://libros-revistas-derecho.vlex.es/vid/informaticos-hosting-housing-caracter-351827

Hidalgo, R. (2009, junio). Contrato de hosting o almacenamiento electrónico de datos: Consideraciones contractuales prácticas. *Revista de Contratación Electrónica*, 105. Recuperado de https://libros-revistas-derecho.vlex.es/vid/hosting-almacenamiento-contractuales-65190961?_ga=2.151805177.1312556390.1574781742-523475224.1547242270

Latam, T. (2020, 27 de febrero). *Entienda la diferencia entre cloud y hosting*. Recuperado de https://blog.tivit.com/latam/entienda-la-diferencia-entre-cloud-y-hosting

Ministerio de Justicia y Derechos Humanos del Perú [Minjus]. (2013). *Directiva de seguridad. Autoridad Nacional de Protección de Datos Personales-APDP*. Recuperado de https://www.minjus.gob.pe/wp-content/uploads/2014/02/Cartilla-de-Directiva-de-Seguridad.pdf

Morales Acosta, A. (s.f.). *Asimetría informativa*. Recuperado de http://www.teleley.com/articulos/art_290507.pdf

Safria, E. C. (2013). ¿Datos protegidos? Implicancias inmediatas y retos que plantea la entrada en vigor de la ley de protección de los datos personales. *Semana Económica*, 1.

Solana, M. V. (2005). Derecho de intimidad y protección de datos personales. En M. P. Poch, *Derecho y Nuevas Tecnologías*, pp. 165-169. Madrid: UOC.