

Los riesgos del e-commerce a la protección de los datos personales de los consumidores: Apuntes sobre cómo afrontarlos

Autora:**Viviana Chavez**, Coordinadora del Comité de Protección de Datos Personales en WCA Perú

Junto con los muchos beneficios derivados del proceso de transformación digital que han venido atravesando la gran mayoría de empresas en los últimos años -algunas impulsadas por la pandemia del COVID-19-, se generan también nuevos riesgos -y/o se incrementa el nivel de exposición a riesgos ya existentes- desde diversos frentes, siendo uno de los más importantes el de protección de datos personales.

A la fecha, no contamos en nuestro país con un marco legal que regule el comercio electrónico y que establezca reglas específicas a ser cumplidas por los proveedores que ofrezcan productos y/o servicios a través de plataformas digitales, incluyendo aquellas relacionadas al tratamiento de los datos personales. Al margen de si un marco legal como tal es necesario o no -discusión que excede el objetivo del presente artículo-, existen algunas iniciativas al respecto, aunque estas estarían enfocadas en la protección de los derechos económicos de los consumidores, más no en la protección de sus datos personales.

En efecto, el pasado 6 de abril de 2021, el Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual - INDECOPI, publicó el Documento de Trabajo Institucional denominado*"Propuestas para la Protección del Consumidor en el Comercio Electrónico y la Seguridad de Productos"* (el Documento de Trabajo). Conforme a lo señalado en el numeral I del Documento de Trabajo, este tendría por objetivo (…)*establecer un estándar mínimo de cumplimiento en las transacciones realizadas a través de canales digitales y su ejecución, así como garantizar la seguridad de los consumidores.*

A través de dicho Documento de Trabajo se propone incluir algunas modificaciones a la Ley N° 29571, Código de Protección y Defensa del Consumidor (Código de Consumo). En lo que respecta a la protección de datos personales, solo hay una breve mención en el propuesto artículo 48-A, sobre opciones preseleccionadas, que advierte que el consumidor puede (…) *seleccionar libremente y de manera inequívoca las prestaciones accesorias opcionales, las prestaciones sucesivas y el tratamiento de sus datos personales que desee incorporar al contrato*. Por lo demás, se establece que el tratamiento de datos personales deberá regirse por su propia normativa, esto es, por la Ley N° 29733, de Protección de Datos Personales (LPDP) y su Reglamento, aprobado mediante Decreto Supremo N° 003-2013-JUS (el Reglamento).

Tratándose de una iniciativa pública del INDECOPI como autoridad de protección al consumidor, es comprensible que en esta no se aborde la problemática desde la legislación sobre protección de datos personales. Puede que la Autoridad Nacional de Protección de Datos Personales también tenga previsto formular alguna propuesta normativa al respecto o no. Lo cierto es que, al día de hoy, las empresas ya vienen enfrentando un nuevo escenario de riesgos en materia de protección de datos personales y existe un marco legal que ha guiar su comportamiento a efectos de evitar incurrir en prácticas ilícitas. Según lo ya indicado, dicho marco legal está conformado por la LPDP y su Reglamento.

El objetivo del presente artículo es, en primer lugar, hacer un breve repaso sobre los nuevos escenarios de riesgos que enfrentan tanto las empresas como los titulares de datos personales a propósito del -vertiginoso- desarrollo del comercio electrónico en el Perú para, posteriormente, ensayar algunas recomendaciones en relación a cómo afrontarlos adecuadamente.

Factores que desencadenan nuevos riesgos (o incrementan los ya existentes)

- Muchos negocios están in**cursionando en el mundo del e-commerce y/o recién se están comunicando con sus clientes a través de plataformas digitales.** Como resultado de ello, algunos podrían no estar del todo familiarizados con la legislación sobre protección de los datos personales o, de estarlo -pues ya habrían adoptado medidas para adecuarse a esta-, podrían no estar preparados para enfrentar los retos que esta les impone en un nuevo contexto como el que enfrentamos.
- **Empresas manejan datos personales de un universo más grande de consumidores.** En efecto, como ya hemos anotado, el e-commerce ha crecido de manera muy importante. Como resultado de ello, los negocios están accediendo a información sobre un mayor número de clientes que antes no proporcionaban su información personal. Un claro ejemplo de lo anterior es el de las empresas de retail (por ejemplo, tiendas por departamento y supermercados), las cuales antes accedían a información muy básica sobre sus consumidores (por ejemplo, número de documento de identidad) y que, al día de hoy, acceden a una mayor

cantidad de información a efectos de procesar la compra y/o coordinar la entrega de los productos (por ejemplo, número de tarjeta de crédito, teléfono, domicilio del consumidor, entre otros).

- **Empresas manejan más información e información más sensible**. No solo es el caso que los negocios están accediendo a información sobre un mayor número de consumidores, sino que también están accediendo a información sensible que requiere especial protección, como es el caso de las preferencias de consumidores y hábitos de compra. Asimismo, en el contexto de contratación digital, se usan diversas técnicas de validación de identidad que suponen el procesamiento de datos biométricos (por ejemplo, huellas dactilares) y/o del uso de la imagen, lo que también requiere especial atención.
- **Debido a la digitalización, las empresas están en capacidad de procesar la información personal de los clientes de manera más intensiva**. En efecto, la gran cantidad de información, sumada a la existencia de tecnologías que permiten su fácil y rápido procesamiento, incrementa el valor de la información y permite a las empresas usarla para nuevas finalidades, incluyendo el agregar valor a sus negocios. A manera de ejemplo, dicha información puede servir a efectos de desarrollar nuevas estrategias de marketing, ofrecer productos y/o servicios que se ajusten más a los intereses y/o necesidades de los clientes (incrementando así el volumen de ventas), compartirla con empresas del grupo para que ofrezcan sus propios productos y/o servicios que puedan ser de interés de los clientes, entre otros.
- **Los consumidores no suelen estar en posición en "negociar" los términos en los que su información va a ser procesada.** Partiendo del ejemplo de las compras por internet, debido a la operatividad de las plataformas, no es posible para los consumidores negociar los términos de la transacción, debiendo más bien adherirse a los términos preestablecidos por las empresas. Esta situación supone un reto para las empresas, pues la validez de los consentimientos que estas obtengan para el tratamiento de los datos personales de dichos consumidores podría ser cuestionada por la Autoridad de Protección de Datos Personales. Recordemos que, conforme a lo previsto por la LPDP y su Reglamento, los consentimientos deben ser libres. Esto supone que los consumidores deberán estar en posibilidad de aceptar o rechazar el procesamiento de sus datos personales -salvo en lo que resulte indispensable para ejecutar la transacción-, lo que puede ser problemático en el mundo del comercio electrónico, en el que se busca simplifica en lo posible los procesos a fin de fomentar un mayor flujo de transacciones.
- **El uso de plataformas tecnológicas para el procesamiento de datos personales genera nuevos riesgos en materia de seguridad**. Debido al gran valor de la información, hay más incentivos para que terceros no autorizados accedan indebidamente a las plataformas que la contienen, lo que es comúnmente conocido como data breach. Cada vez es más usual que conozcamos de casos de hackeos a plataformas digitales. Según una investigación realizada por Fortinet, en el primer trimestre de 2020 se registraron 433 millones de intentos de ciberataques en Perú[1]. Siendo que dichas plataformas al día de hoy contienen información de alta sensibilidad -como es el caso de información sobre tarjetas de crédito-, un acceso indebido podría afectar gravemente los intereses de los consumidores, por lo que las empresas están llamadas a tomar las medidas necesarias a fin de prevenir y/o mitigar dichos potenciales riesgos. De lo contrario, será muy difícil generar confianza en un sector de los consumidores que, al día de hoy, temen por el uso indebido de sus datos personales. En efecto, conforme a lo señalado en un artículo difundido por la revista digital Conexión ESAN[2], una de las principales preocupaciones de los consumidores al momento de realizar compras por internet es hacerlo desde una página web que no brinde la seguridad adecuada.
- **Servicios en línea que se ofrecen en forma gratuita, a cambios de datos personales.** Justamente en consideración al gran valor de la información, existen muchas empresas que ofrecen a los consumidores servicios sin costo a cambio de recibir determinada información personal. Si bien son los consumidores quienes libremente toman la decisión de conceder su información personal a cambio de obtener el servicio, esta práctica no ha estado exenta de cuestionamientos. Estos cuestionamientos son mayores -en tanto generan una mayor preocupación por parte de las autoridades- cuando se trata de consumidores vulnerables, como es el caso de los niños[3].

Como se aprecia de lo antes señalado, son diversos los factores de riesgo desde la legislación sobre protección de datos personales que existen como resultado del desarrollo del comercio electrónico. Como resultado de ello, es de esperar que en el futuro veamos un incremento del ya existente enforcement de la protección de datos personales en el comercio electrónico. En efecto, la Autoridad de Protección de Datos Personales ha manifestado estar particularmente vigilante sobre el cumplimiento de la legislación por los proveedores que vienen realizando actividades de comercio electrónico[4].

Recomendaciones sobre cómo afrontar nuevos escenarios de riesgo

Ante un contexto como el descrito, surge la siguiente interrogante: ¿cómo cumplir con la legislación de datos personales en un contexto como el que enfrentamos? Si bien no es uno de los propósitos del presente artículo hacer un listado exhaustivo de las tareas que deberán llevar a cabo las organizaciones para actuar en cumplimiento de los principios y obligaciones dispuestos por el marco legal, sí lo es dar algunas recomendaciones sobre los principales aspectos a tener en cuenta:

- **Analizar el impacto que todo nuevo tratamiento de información personal podría tener en los derechos de los titulares de la información.** Esta evaluación debe realizarse desde un primer momento, a efectos de incluir los ajustes que correspondan al proceso de modo tal que este satisfaga las exigencias de la LPDP. Para ello es fundamental que las áreas legales participen en la toma de decisiones que involucren nuevos tratamientos de datos personales. A esto se le conoce como privacy by design. De no proceder de esta manera, podría ocurrir que solo hacia el final de determinado proyecto (por ejemplo, cuando el diseño de una nueva plataforma digital está terminado y listo para su lanzamiento) la empresa advierta que este contraviene la LPDP. Incluir los ajustes necesarios en un momento tan avanzado podría resultar muy costoso e, incluso, podría resultar inviable desde un punto de vista técnico.
- **Revisar y/o elaborar los formularios de consentimiento** para verificar que estos cumplan con dar a los consumidores toda la información necesaria sobre las condiciones bajo las cuales se procesarán sus datos personales. Tomar en cuenta que la LPDP establece qué información mínima deberá ser entregada para cumplir con este requisito. De no cumplir con proporcionar dicha información, podría entenderse que el consentimiento obtenido por los consumidores no cumple con ser informado y, en consecuencia, no se tome como válido. Del mismo modo, deberán revisarse las políticas de privacidad, a fin de garantizar que estas contengan toda la información requerida por la LPDP y en el nivel de detalle exigido por esta. Sobre este punto, es importante reconocer las particularidades de la LPDP. Importar políticas de privacidad aplicables en otras jurisdicciones, sin revisar su adecuación a la legislación local, puede generar una falsa sensación de cumplimiento.
- **Evitar los consentimientos en bloque**. A fin de simplificar el proceso de obtención de consentimiento para el tratamiento de datos personales, las empresas tienden a solicitar consentimientos en bloque (esto es, consentimientos para el tratamiento de los

tratamientos de información y rechazar otros. Lo anterior genera que el consentimiento no cumpla con ser libre y, en consecuencia, se tome como no otorgado. Los consumidores deberán estar en posibilidad de aceptar o rechazar el tratamiento de sus datos personales para cada una de las finalidades (por ejemplo, a través del marcado de check-boxes).

- **Verificar que la información se esté utilizando solo para los fines para los que se obtuvo la autorización**. El hecho de que la empresa tenga la información a su disposición y la haya obtenido por medios lícitos no significa que esta pueda ser utilizada para cualquier fin. Esta suele ser una gran tentación para las áreas comerciales. Las empresas deberán sensibilizar a todos sus colaboradores (especialmente a los del área comercial) sobre la importancia de proteger los datos personales, y utilizarlos solo para los fines específicamente autorizados por sus titulares.
- **Eliminar la información cuando ya no sea necesaria**. En muchos casos las empresas mantienen en sus registros información que ya no les es de utilidad. Tomar en cuenta que almacenar información personal más allá de lo necesario para cumplir la finalidad para la que fue recopilada (o por un plazo mayor al que fue autorizado) se encuentra prohibido por el marco legal, al considerarse un incumplimiento al principio de proporcionalidad que, conforme a lo dispuesto por la LPDP, debe guiar el tratamiento de datos personales. Asimismo, no debe perderse de vista que, a mayor cantidad de información personal almacenada, mayor es el riesgo que la empresa asume ante eventos de acceso y uso no autorizado de datos personales.
- **Anonimizar la información para aquello que no requiera la identidad del titular de los datos**. En muchos casos la información se utiliza para procesos en los cuales conocer la identidad de la persona no resulta necesario (por ejemplo, para elaborar información estadística). En esos casos, lo más recomendable es que las empresas anonimicen la información. De esta manera, la información ya no calificará como datos personales y, en consecuencia, ni las empresas ni los consumidores deberán enfrentar los escenarios de riesgo descritos en párrafos precedentes.
- **Gestionar adecuadamente el riesgo relacionado con la seguridad digital**. A través del documento titulado Protección al Consumidor en el Comercio Electrónico. Recomendación de la OCDE[5], la Organización para la Cooperación y el Desarrollo Económicos (OCDE) ha reconocido la relevancia de la implementación de medidas de seguridad para reducir o mitigar los efectos adversos relacionados con la participación del consumidor en el comercio electrónico. En adición a la implementación de adecuadas medidas de seguridad -para lo cual las empresas pueden tomar como referencia lo dispuesto en la Directiva de Seguridad publicada por la Autoridad de Protección de Datos Personales[6]-, la OCDE recomienda a las empresas implementar protocolos sobre cómo actuar ante brechas de información, de modo tal que se mitiguen los daños derivados de estas, así como capacitar a los miembros de la organización que están a cargo del tratamiento de datos personales.
- En caso una empresa vaya a contratar a terceros para que le brinden determinados servicios de tecnología de la información (por ejemplo, cloud computing), esta deberá**verificar que está contratando a empresas que cuentan con estándares de seguridad adecuados**. Las empresas no deberán perder de vista que no están contratando un servicio más, sino un servicio de gran relevancia y particular sensibilidad. En ese sentido, deberán aplicar un proceso de selección muy riguroso, que parta por verificar las credenciales en materia de seguridad que el proveedor en cuestión ofrece. Asimismo, es recomendable suscribir contratos con dichas empresas (evitando en lo posible que la relación solo se sustente en órdenes de servicio) que incluyan cláusulas de protección de datos que brinden una adecuada protección a los titulares de datos personales.

A medida que las empresas tomen conciencia de los retos que el desarrollo del comercio electrónico plantea y decidan afrontarlos partiendo de las exigencias contenidas en la LPDP y su Reglamento, será posible construir un mercado respetuoso de los derechos de los consumidores a la protección de sus datos personales que, como tal, genere confianza en ellos y se vea dinamizado, reportando beneficios a todos.

[1] Conforme a un artículo publicado por la revista digital Conexión ESAN, de la Universidad ESAN, con fecha 8 de setiembre de 2020, disponible en el siguiente enlace: https://www.esan.edu.pe/apuntes-empresariales/2020/09/comercio-electronico-como-evitar-quejas-y-reclamos-de-tus-clientes/ (visitado el 12 de mayo de 2021).

[2] Ver nota al pie anterior.

[3] Sobre el particular, la Organización para la Cooperación y el Desarrollo Económicos (OCDE) ha señalado que: La protección al consumidor se ha vuelto más compleja en la era digital, incluso con respecto a los consumidores vulnerables (por ejemplo, los niños). Al mismo tiempo, han surgido nuevos problemas, por ejemplo, en relación con las aplicaciones y servicios en línea que se ofrecen de forma "gratuita" a cambio de obtener acceso a los datos personales del usuario. En: Panorama del comercio electrónico: políticas, tendencias y modelos de negocio. OCDE, 2019. Traducido por Asociación Mexicana de Internet. Disponible en: https://www.oecd.org/sti/Panorama-del-comercio-electro%CC%81nico.pdf (visitado el 12 de mayo de 2021).

[4] Conforme a una Nota de Prensa emitida por la APDP con fecha 15 de junio de 2020, esta informó que: (…) en el ámbito privado, ha intensificado su labor de fiscalización a empresas que realizan comercio electrónico para ofrecer sus productos y servicios a los consumidores. Así, en este periodo marcado por la pandemia, se han realizado 37 supervisiones de diferentes sitios web y plataformas, verificando la licitud de las políticas de privacidad y el cumplimiento del deber de información al ciudadano-consumidor respecto al uso que se le dará a sus datos personales. Las principales infracciones que se han verificado están relacionadas al incumplimiento del deber de confidencialidad, usos distintos y no autorizados de los datos personales de los usuarios de estas plataformas (uso publicitario, por ejemplo) y el incumplimiento del deber de informar. Disponible en: https://www.gob.pe/institucion/anpd/noticias/208703-durante-periodo-de-emergencia-sanitaria-se-continua-fiscalizando-el-tratamiento-de-los-datos-personales (visitado el 12 de mayo de 2021).

[5] Recomendación de la OCDE. Protección al Consumidor en el Comercio Electrónico, disponible en: https://www.oecd.org/digital/consumer/proteccion-al-consumidor-en-el-comercio-electronico.pdf

[6] Disponible en: https://www.minjus.gob.pe/wp-content/uploads/2014/02/Cartilla-de-Directiva-de-Seguridad.pdf