#FreshStartMonday

Políticas de privacidad para transacciones comerciales digitales

El comercio electrónico ha crecido de una manera exponencial en 2020. Gran parte de la economía se trasladó a Internet como consecuencia de la pandemia creando un impacto significativo. Tal como lo revela el segundo Estudio de Comercio Electrónico Nacional elaborado por la Cámara de Comercio de Guatemala, 5 de cada 10 guatemaltecos compran en línea al menos una vez al mes[1]. Se cree que el COVID-19 aceleró la adopción del comercio electrónico en cinco años y es poco probable que este crecimiento se estanque en 2021. Incluso si el país comienza a superar la pandemia, el comercio electrónico vino para quedarse.

Las transacciones electrónicas han pasado a formar parte de nuestras vidas. Esta forma de comercio tiene muchas ventajas, de las cuales las más importantes son la comodidad y la oferta global de bienes y servicios. Sin embargo, se debe de tomar en cuenta que estas transacciones electrónicas generan datos e información personal que debe protegerse y su uso debe regularse.

Muchas empresas en línea utilizan los datos personales de los clientes para ofrecer publicidad personalizada, servicios personalizados y relaciones estratégicas con los clientes. Algunas incluso llegan a comercializar esos datos, pero el manejo de estos datos debe hacerse cuidadosamente para no generar contingencias para la empresa, por lo que es necesario que existan políticas de privacidad que garanticen la protección de estos.

Una política de privacidad es un acuerdo que detalla todas las medidas que aplica una empresa u organización para garantizar la seguridad y el uso lícito de los datos de los usuarios o clientes que recoge en el contexto de la relación comercial. La política de privacidad también detalla la forma en que se recolectan, se almacenan y se utilizan estos datos, así como si se envían a terceros y, en caso afirmativo, de qué manera.

Es por esto que una política de privacidad es uno de los acuerdos legales más importantes para una empresa que opere en línea. Pues otorga a los usuarios la seguridad necesaria para hacer una transacción en línea, la cual redundará en mayores ventas[2] y a la vez minimiza los riesgos para la empresa.

Adicionalmente, la normativa en materia de privacidad y protección de datos en muchos países es cada día más estructura y obligatoria para poder comercializar de forma digital. Por ejemplo, en Estados Unidos se encuentra vigente la Ley Estatal de Protección de la Privacidad de California (*The California Online Privacy Protection Act -CalOPPA*), la cual regula que al solicitar cualquier tipo de información personal de cualquier usuario con sede en California, como: direcciones de correo electrónico, localización GPS, números de teléfono o direcciones postales, se debe de tener una política de privacidad disponible para la consulta de los usuarios que describa las prácticas de privacidad del negocio[3].

En la Unión Europea (UE) a partir del año 2018, entró en vigor el Reglamento General de Protección de Datos (*General Data Protection Regulation -GDPR-*) que exige a todas las empresas que operan en la UE, así como las empresas extranjeras que manejan datos personales de personas ubicadas en la UE, contar con una Política de Privacidad. Esto forma parte de su objetivo de asegurarse que la información personal se obtiene y se procesa de forma justa.

Estas normativas internacionales recogen principios y estándares de cumplimiento para la privacidad de datos, como los siguientes:

- Informar qué tipos de datos personales se recogen a través del sitio web o la app
- Almacenar los datos sólo durante el tiempo necesario
- Utilizar los datos para el propósito informado y autorizado por el usuario
- Procedimiento para que los usuarios puedan modificar o corregir inexactitudes acerca de los datos personales que se recogen
- El proceso para informar a los usuarios de cualquier cambio en la política de privacidad
- Cláusulas de "*Do Not Track - DNT*" (no rastrear) que permita activar el seguimiento del comportamiento por parte de servicios de terceros como Google Adwords.
- Nombramiento de un responsable de la protección de datos en la empresa

- Informar a los usuarios del derecho a acceder, actualizar o solicitar la eliminación de sus datos personales.
- Informar de cualquier organización afiliada con la que se planee compartir estos datos
- Cualquier otra información que el usuario necesite conocer para garantizar un tratamiento justo de sus datos personales[4].

En Guatemala, a pesar de que no existe regulación específica sobre políticas de privacidad de datos, la Constitución Política de la República de Guatemala, garantiza que toda persona tiene el derecho de conocer lo que de ella conste en registros estatales y la finalidad a que se dedica esta información, así como a corrección, rectificación y actualización[5]. También la Ley de Acceso a la Información Pública regula que toda persona cuyo trabajo sea proporcionar información pública, no podrá difundir, distribuir o comercializar los datos personales contenidos en los sistemas de información desarrollados en el ejercicio de sus funciones, salvo que tuviere el consentimiento expreso de las personas[6].

Asimismo, la Corte de Constitucionalidad de Guatemala se ha pronunciado respecto a datos o archivos en poder de terceros para su uso comercial, estableciendo que existen cuatro derechos que deben ser observados en cuanto a la recolección de datos personales:

- derecho a la actualización de los datos;
- derecho a la rectificación de los datos erróneos;
- derecho a la confidencialidad de la información personal;
- derecho a la exclusión de la información sensible del usuario[7].

Consecuentemente, aunque no existe una ley que expresamente obligue a contar con una política de privacidad, es recomendable contar con ella, ya que protegerá a la empresa de potenciales reclamos y le permitirá prepararse para el cumplimiento de estándares mundiales que irán exigiendo cada vez más los proveedores y clientes internacionales y locales. Es también necesario contar con un plan de emergencia para el manejo de violaciones de ciberseguridad que puedan poner en riesgo los datos personales que maneja la empresa. Muchas empresas contratan seguros contra ataques cibernéticos y cuentan con un equipo especializado en materia de protección de datos y ciberseguridad.

¿Está su empresa preparada para manejar y proteger los datos en la era digital?

---

[1] https://www.ccg.com.gt/web-ccg/2do-estudio-nacional-de-comercio-electronico/

[2] https://legenova.com/7-reasons-privacy-policy-importance/ Ver también: https://www.termsfeed.com/blog/top-4-reasons-you-need-privacy-policy/#:~:text=A%20Privacy%20Policy%20is%20not,their%20personal%20information%20with%20care.

[3] https://www.privacypolicies.com/blog/caloppa/

[4] https://www.privacypolicies.com/blog/gdpr/

[5] Artículo 31 Constitución Política de la República de Guatemala.

[6] Artículo 31 de la Ley de Acceso a la Información Pública

[7] Sentencia de la Corte de Constitucionalidad dictada dentro del expediente número 1356-2006 el 11 de octubre de 2006.