

PROTECCIÓN DE DATOS PERSONALES EN COMERCIOS ELECTRÓNICOS B2C

PERSONAL DATA PROTECTION ON E-COMMERCE B2C

PROTEÇÃO DE DADOS PESSOAIS EM COMÉRCIOS ELETRÔNICOS B2C

*Carolina Sacoto**

Recibido: 13/05/2020

Aprobado: 25/06/2020

Resumen

En Ecuador, el crecimiento acelerado de las transacciones comerciales realizadas por internet ya es una realidad. Desafortunadamente, el auge de esta industria se da en un entorno de incertidumbre total ante la inexistencia de una norma adecuada que regule el tratamiento de datos personales. En ese contexto, este artículo pretende señalar las obligaciones y avisos legales esenciales relacionados con la protección de datos personales que los comercios electrónicos B2C deberían tener presente a la hora de operar en el mercado. El análisis se realiza en atención al actual Proyecto de Ley de Protección de Datos Personales, desde una perspectiva legal y, vinculada a ella, una perspectiva técnica y lingüística. Finalmente, se realizan recomendaciones para facilitar al responsable el cumplimiento de los parámetros revisados en este documento.

Palabras clave: Privacidad en internet; Tratamiento de datos; Seguridad de datos; Procesamiento de datos; Contratación electrónica

Summary

In Ecuador, the accelerated growth of commercial transactions made through internet is already a reality. Unfortunately, its rise is taking place in conditions of total uncertainty caused by the absence of legal regulations regarding data protection and its processing. In this context, this article aims to cover the main obligations and legal notices related to personal data protection that B2C electronic commerce should consider when operating. The analysis is

based on the personal data protection bill of Ecuador from a legal perspective, and linked to it, a technical and linguistic perspective; finally, this work provides recommendations to guide organizations with the compliance of the requirements reviewed in this document.

Key words: Internet privacy; Data treatment; Data security; Data processing; Electronic contracting

Resumo

No Equador, o crescimento acelerado das transações comerciais realizadas por internet já é uma realidade. Infelizmente, o auge desta indústria está acontecendo ao redor de uma incerteza total diante da inexistência de uma norma adequada que regule o tratamento dos dados pessoais. Nesse contexto, este artigo pretende indicar as obrigações e avisos legais essenciais relacionados com a proteção de dados pessoais que os comércio eletrônico B2C deveriam observar na hora de entrar no mercado. A análise se realiza em compatibilidade com o atual Projeto de Lei de Dados Pessoais, desde uma perspectiva legal e, vinculada a ela, uma perspectiva técnica e lingüística. Finalmente, se realizam recomendações para facilitar ao responsável o cumprimento de parâmetros revisados neste documento.

Palavras chave: Privacidade na internet; Tratamento de dados; Segurança de dados; Processamento de dados; Contratação eletrônica

* Abogada por la Universidad Técnica Particular de Loja, Ecuador; Ingeniera comercial por la Universidad del Azuay, Ecuador; Magister (c) en Propiedad intelectual y nuevas tecnologías por la Universidad Internacional de La Rioja, España. Tiene experiencia en comercio electrónico y es abogada en libre ejercicio profesional. Correo electrónico: carolina.sacoto94@gmail.com

INTRODUCCIÓN

El constante desarrollo tecnológico ha permitido la creación y rápida expansión de un nuevo modelo de negocio que gira en torno a la compra y venta de bienes y servicios por internet a través de relaciones contractuales por medios electrónicos. Este es un canal de ventas que, mediante el uso de herramientas tecnológicas, obtiene gran cantidad de información sobre los internautas, la cual, tratada en diverso modo y por diferentes prestadores de servicios, consigue, además de prestar el servicio de compra y venta en línea, mejorar la experiencia del usuario al navegar por una página web.

En este sentido, y si bien las acciones de procesamiento de datos están encaminadas a potenciar las ventajas que un *e-commerce* ofrece, en la misma o mayor medida representan una amenaza latente para la privacidad de las personas, quienes, además, no tienen ningún poder de negociación con los comercios. Esta

situación ha llamado la atención del legislador de cada país, quien ha tenido la difícil tarea de crear la normativa adecuada para tutelar un derecho fundamental de la persona, obviamente sin impedir el desarrollo del comercio electrónico.

Lamentablemente en Ecuador, si bien existe un Proyecto de Ley Orgánica de Protección de Datos Personales, a la fecha, el marco jurídico es insuficiente; pues, con o sin norma que regule este derecho, es de gran importancia que el comercio electrónico cumpla con parámetros adecuados de protección de datos personales. Por tal motivo, este artículo hará una revisión de los requisitos fundamentales que los *e-commerce* B2C deberían tener en Ecuador, al momento de salir al mercado. Para lograr una visión integral del asunto, se abordarán estos puntos desde el ámbito legal y, vinculadas este, las perspectivas técnica y lingüística.

NOCIONES IMPORTANTES SOBRE EL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES EN EL MARCO DEL COMERCIO ELECTRÓNICO

1. Una mirada a la evolución del derecho a la protección de datos personales

La aparición de las primeras normativas que regulaban la protección de datos se remonta a los años 70 (Frosini 1998). Estas formaban parte de la *primera generación de protección de datos* y nacieron como una reacción a la “informatización progresiva de la sociedad y también, a la incertidumbre acerca de sus implicaciones inmediatas, así como de las medidas precisas que debían tomarse” (Lazpita 1994, 404).

A partir de esa base, surgió una variada legislación a nivel internacional. Esta se distinguió, por un lado, por ordenamientos jurídicos que se decantan por el impulso del desarrollo económico, como es el caso de Estados Unidos. Por otro lado -línea que pretende seguir Ecuador- se hallan aquellos otros que han implementado un sistema jurídico con un nivel alto

de protección de datos personales, al que confieren un rango de derecho fundamental independiente, como es el caso de la Unión Europea. Con tal aporte a la doctrina se inició “una nueva etapa, que se basa en la consideración de la protección de datos de carácter personal como un verdadero derecho fundamental autónomo e independiente del derecho a la intimidad” (Piñar 2003, 29).

La explicación a esta evolución conceptual, que sitúa el derecho a la protección de datos personales en la 3.^a generación de derechos fundamentales, viene dada por el crecimiento preponderante que ha tenido el uso de la tecnología en todos los ámbitos de la vida diaria. Y “la protección de datos personales constituye una respuesta jurídica frente al fenómeno de la sociedad de la información para frenar la potencial amenaza que el desarrollo tecnológico representa para los derechos y libertades de las personas” (Herrán 2003, 15).

Finalmente, y en respuesta a las crecientes exigencias que la era digital ha traído, en el año 2012 se inició en Europa la elaboración del más moderno instrumento que se tiene en la materia, el RGPD¹. Esta normativa es un modelo nuevo que, por los principios, derechos y obligaciones que incorpora, pretende lograr un uso ético y responsable de la información. Además, intenta armonizar dos objetivos importantísimos: por un lado, la protección de datos y, por otro, libre circulación en el mercado para no limitar de forma injustificada la innovación. En Ecuador, el nuevo proyecto de ley en la materia sigue casi en su totalidad los preceptos legales contenidos en el mencionado Reglamento.

Nuestro país no es uno de los que ha respondido con rapidez a la era digital. Como consecuencia, la ley para la protección de datos personales en Ecuador aún no es una realidad, y lo único que tenemos son preceptos legales dispersos en diversas normas que no son ni suficientes, ni claros, ni completos para regular eficientemente el tratamiento de los datos personales en instituciones públicas y privadas. Sin embargo, no deja de ser una normativa vigente y plenamente aplicable para el caso concreto; y, por esta razón, la revisamos brevemente a continuación.

La Constitución del Ecuador, en su art. 66 numeral 19 establece que se reconoce y garantiza a las personas el acceso, la decisión y protección sobre información y datos de carácter personal que le concierne, de forma que su tratamiento requerirá la autorización del titular o el mandato de la ley; y el art. 92 de la misma norma posee un sentido similar. Luego, tenemos la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, que principalmente contiene una definición bastante básica sobre lo que se considera dato personal, regula la contratación electrónica; y dedica su art. 9 a la protección de datos, en el que pone énfasis en el consentimiento y el mandato legal como base para el tratamiento de datos. También establece que el procesamiento de los datos debe responder a los derechos de privacidad, intimidad y confidencialidad. En definitiva, esta ley sí recoge algunos preceptos importantes en la materia, pero sin una estructura clara y adecuada que resulte eficiente.

2. ¿Qué se considera dato personal?

El art. 5 del proyecto de Ley Orgánica de Protección Datos Personales, recoge una definición que tiene en cuenta todo dato que concierne a una persona, cuya identidad es evidente (identificada) o puede establecerse y llegar a serlo, directa o indirectamente, a partir de la combinación de unos datos con otra información (identificable). Esta identificación requiere obligatoriamente, elementos que describan de forma clara a una persona de tal modo que no se la confunda con otra.

Además, hace énfasis en la posibilidad de que un dato se haga identificable en el “presente o en el futuro” como un anticipo a las novedades que tecnologías inexistentes hoy en día podrían traer. Este es un concepto más adecuado en comparación con la única e incompleta definición disponible en el ordenamiento jurídico ecuatoriano a la fecha, que está prevista en la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos y que textualmente dice: “son aquellos datos o información de carácter personal o íntimo, que son materia de protección en virtud de esta ley” (Disposición general 9.ª, glosario de términos).

Para entender de mejor manera esta definición es preciso mencionar unos cuantos ejemplos, con datos que permiten identificar directamente a una persona, su nombre o número de identificación; asimismo permitirán identificarla indirectamente, mediante información como su dirección o número de celular. A estos clásicos datos personales, se suman aquellos que provienen del uso de la tecnología y que también hacen posible la identificación, los cuales usualmente son recogidos cuando la persona navega por internet en una web, por ejemplo, la dirección IP.

Finalmente, en ese concepto se evidencia que la persona objeto de protección es una persona física.

3. Características de los comercios electrónicos B2C

Pues bien, para comprender las obligaciones legales en materia de protección de datos personales que se

¹ Reglamento General de Protección de Datos, vigente para su aplicación desde el 25-V-2018.

abordarán más adelante hay que tener claro algunas cuestiones importantes sobre los *e-commerce*.

Desde el surgimiento del comercio electrónico en los años 90 hasta la fecha, las plataformas digitales han atravesar varias etapas para poder llegar a su actual estado: un modelo de negocio que incluye el uso de herramientas tecnológicas de seguridad, funcionalidades que permiten personalización del servicio, elementos de publicidad, campañas de marketing masivas integradas, etc. Es decir, es un modelo de negocio capaz de incorporar todo tipo de tecnologías para el tratamiento de datos personales, y estos rasgos lo han posicionado como el canal de ventas más importante a nivel mundial.

Existen tantas definiciones de comercio electrónico como autores; sin embargo, resultan más acertadas aquellas que ya tienen presente la distribución de información que se genera en las transacciones comerciales por internet.² Así mismo, existen varias formas de clasificar al comercio electrónico. La que nos interesa es aquella que tiene en cuenta a quiénes participan en la transacción electrónica; particularmente, el modelo B2C (*business to consumer*), en el que interviene, por un lado una empresa, y por otro el consumidor final hacia el que la compañía dirige sus esfuerzos de venta.

Este modelo de negocio no sería tan atractivo de no contar con innumerables ventajas tanto para consumidores como para empresarios. Entre las más valoradas están: comodidad, variedad de productos, precios competitivos, atención continua al público, acceso a un mercado global y, una de las más importantes, la personalización del servicio.

Ahora bien, para que las transacciones de un *e-commerce* sean posibles, es necesario que se realicen con otros proveedores de soluciones electrónicas. Los servicios que casi siempre son requeridos son: servidores en la nube para el almacenamiento de datos, pasarelas de pago, herramientas para publicidad, etc. Procesos en los que existe un importante intercambio de datos

personales, sin los cuales no sería posible prestar el servicio. Adicionalmente, el éxito de una página de comercio electrónico está ligado claramente a la eficiencia del servicio; pero, sobre todo, a la estrategia de marketing que se utilice para hacerle apreciar al cliente las ventajas de comprar en su tienda. Y tanto el servicio como los esfuerzos comunicacionales para lograr ese objetivo necesitan de información valiosa de los compradores.

4. Contratación electrónica

En vista de que la dinámica del negocio requiere una importante cantidad de datos personales para que se logre el nivel de eficiencia deseado, ¿cómo hacen los comercios para conseguir toda esa información y poder tratarla de una forma lícita? La respuesta es mediante una contratación electrónica que utilice, como base legal, el consentimiento dado por el internauta.

Para la mayoría de propósitos, cuando no ha existido una relación contractual previa, los comercios electrónicos requieren del consentimiento del titular de los datos personales para tratar su información, que se exterioriza con la aceptación de contratos electrónicos. Ellos son básicamente los Términos y Condiciones, las Políticas de Privacidad y los Avisos sobre. Más adelante abordaremos el contenido sugerido para estos contratos.

En este punto se revisará qué se entiende por consentimiento. Nos remitimos nuevamente a la definición que pretende el proyecto de Ley Orgánica de Protección de Datos Personales en Ecuador³, que lo define como “manifestación de la **voluntad libre, previa, específica, expresa informada e inequívoca**⁴ por la que el titular de los datos personales autoriza al responsable del tratamiento de datos personales a tratar los mismos”.

Así, en ella se entiende que existen requisitos para que el consentimiento en materia de protección de datos sea válido: primero, la voluntad libre; y solo se considera que es libre el consentimiento que se ha dado

² Ver, en este sentido: Anteportamlatinam 2014.

³ Proyecto de Ley Orgánica de Protección de Datos Personales, artículo 5.

⁴ Negrita de la autora.

sin que exista violencia, error, coacción, o temor de consecuencias negativas. Luego, el consentimiento debe ser previo, es decir, tiene que conseguirse antes de tratar los datos personales. También debe ser específico: debe describirse claramente y en términos inequívocos el fin para el que se recogen ciertos datos, de modo que los consentimientos genéricos aplicados a un contexto ilimitado no son válidos.

Después, la norma refiere que el consentimiento debe ser expreso, es decir, manifiesto, cierto y explícito (Albaladejo 2002); además debe ser informado, pues el interesado debe contar con la información suficiente que le permita tener conciencia y comprensión clara y amplia de las consecuencias de dar su consentimiento o de no darlo; y, por tanto, el responsable debe proporcionar una descripción específica y completa de toda la información que permita al titular comprender las implicaciones de su actuar. Finalmente, se dice que debe ser inequívoco ya que no debe caber duda alguna de que el titular quería exteriorizar su voluntad de admitir el tratamiento de sus datos.

En consecuencia, el silencio, por regla general, y al menos en el ámbito de contratación electrónica, no puede considerarse expresión de la voluntad, toda vez que “nadie puede imponer a otro que el silencio sea signo de declaración” (Flume 1998, 94). Se trata, más bien, de una falta de expresión, y considerarla como aceptación de una oferta resultaría abusivo; tampoco podrá entenderse que una oferta ha sido aceptada por el solo hecho de visitar un determinado sitio web.

En el caso particular de las páginas web, la manifestación de la voluntad se da cuando se selecciona la casilla en donde se debería poder visualizar el contrato y se pulsa clic en el botón “aceptar”; razón por la cual, las casillas ya marcadas que llevan a una inacción del sujeto no deben constituir consentimiento.

En cuanto a los contratos electrónicos, existe acuerdo en que es posible la formación del consentimiento por cualquier medio electrónico. Puesto que, “si la voluntad puede declararse por gestos, y aun por silencios, cómo no se va a poder declarar por medio de un ordenador” (Rodríguez 2000, 356). No hay discusión al respecto, debido a que la contratación electrónica cumple con los elementos esenciales de la contratación común, regulada en materia civil; y, si bien incluye el uso de medios telemáticos y presenta particularidades que han sido desarrolladas para generar mayor seguridad jurídica, no aporta novedades relevantes que lleven a un debate sobre el asunto. Asimismo, tampoco parece existir problema jurídico alguno en el uso de las nuevas tecnologías o de internet para expresar el consentimiento.

En el mismo sentido, La Ley de Comercio Electrónico, Firmas y Mensajes de Datos de Ecuador, en su artículo 45, establece la validez de los contratos electrónicos e indica que “no se negará validez o fuerza obligatoria a un contrato por la sola razón de haberse utilizado en su formación uno o más mensajes de datos”; además, regula el consentimiento para el uso de medios electrónicos.

OBLIGACIONES LEGALES EN MATERIA DE PROTECCIÓN DE DATOS RELACIONADAS AL COMERCIO ELECTRÓNICO

En este punto es importante entender que la finalidad de la norma no es impedir a los comercios el uso de datos personales, sino evitar conductas indebidas en el tratamiento de estos datos, a fin de precautelar un derecho fundamental de la persona. Ahora, que las empresas estén preparadas para dar cumplimiento a lo dispuesto en una futura ley en la materia, así como para iniciar operaciones comerciales con otros países que exigen el mismo nivel de protección de

datos personales que ellos ofrecen, será indispensable al menos considerar los puntos que se explican a continuación.

El comercio debe cumplir el principio de licitud, lealtad y transparencia, en virtud del cual se exige que el tratamiento de datos personales tenga un fundamento legal. En el caso de los *e-commerce*, como ya se indicó, hay que tener en cuenta principalmente el consentimiento

como base para el procesamiento legal de datos personales, tratamiento que ha de ser ético. Además, la empresa debe proporcionar al usuario suficiente información relativa a sus datos personales. En todo caso, ha de existir un esfuerzo honesto de usar todos los medios disponibles para mantener al interesado informado antes, durante y después de cualquier proceso relacionado al tratamiento de los datos personales.

También hay que tener presente que la finalidad del tratamiento de los datos debe delimitarse correctamente, de modo que resulte específica y clara. De igual manera, el responsable debe identificar cuáles son los datos mínimos que requiere para cumplir con su propósito legal, de modo que no resulten excesivos e inadecuados; así se dará cumplimiento a los principios de limitación de la finalidad y de minimización.

Y, en concordancia con el principio de limitación de almacenamiento, los datos personales deben conservarse únicamente por el tiempo que sea necesario para cumplir el fin para el que se recogieron. Transcurrido ese periodo deben eliminarse, o pueden mantenerse, pero siempre que se vuelvan anónimos, de manera que no se identifique al titular.

El responsable del tratamiento garantizará razonablemente que los datos sean exactos y precisos, que se han actualizado, y que todo dato falso o engañoso se ha rectificado o eliminado sin dilaciones. Asimismo, el responsable debe implementar medidas técnicas y organizativas, de forma que se minimice el riesgo de actos fraudulentos vinculados con los datos del interesado, sin importar que estén vinculados al su uso, acceso, divulgación, pérdida o destrucción no autorizado, accidental o deliberado. Los comercios deben asegurarse de evitar cualquier tipo de consecuencia desfavorable para el interesado que vulnere sus derechos y libertades; porque, en virtud del principio de seguridad, se tiene que garantizar una protección apropiada de la información.

Por otro lado, íntimamente relacionados a estas obligaciones que tienen los responsables del tratamiento, los derechos de las personas usuarias de estas

plataformas digitales. La exigencia de informar al usuario para obtener su consentimiento es un derecho específico del interesado: el de tener a su disposición toda la información respecto del tratamiento sus datos personales. Su contenido depende de si los datos se recogen directamente del individuo o si se los consiguieron de otra fuente; y, por lo general, los datos que se deben compartir incluyen:

- Información completa del responsable del tratamiento de los datos o su encargado: nombre, datos de contacto, de registro, etc.
- Propósitos del procesamiento de los datos personales vinculados a la base legal correspondiente, incluido el interés legítimo que pudiera tener el comercio, sobre todo relacionados a marketing, publicidad, seguridad, etc.
- Los destinatarios de los datos personales. Más en concreto, al usuario se le debe poner al tanto acerca de los prestadores de servicios de la sociedad de la información involucrados en cada caso, así como de las medidas de seguridad que se tomarán para precautelar la integridad y confidencialidad de la información en estas transferencias. También, los destinatarios de los datos se deben corresponder con los propósitos del procesamiento.
- El tiempo que se pretende almacenar los datos del internauta, que está ligado a la finalidad para la cual se recogió la información.
- Los derechos del usuario en relación con sus datos personales.
- Igualmente, los comercios han de tener en cuenta que no basta con colocar la información en la web, sino que, además, **la información ha de ser concisa, transparente, inteligible y de fácil acceso**⁵.
- Entre los derechos que pueden ser ejercidos por el interesado y que, por tanto, se han de tener presentes en la plataforma web están: el derecho de acceso, por el que el interesado puede requerir una confir-

⁵ Negrita de la autora.

mación de si se están tratando o no sus datos, y obtener una copia de estos; el de rectificación, por el que el interesado tiene derecho a corregir o completar sus datos personales cuando estos sean inexactos o estén incompletos; el de supresión⁶ o derecho al olvido, que faculta al interesado a pedir al comercio que elimine sus datos personales tanto del sistema activo como del de respaldo; el de limitación del tratamiento, que otorga a cada persona el derecho de restringir temporalmente el procesamiento de sus datos personales. Para cumplir con esta exigencia se puede considerar mover temporalmente los datos a otro sistema de procesamiento, evitar que estén disponibles para los usuarios o eliminarlos temporalmente del sitio web. En todo caso, el responsable, durante este tiempo, no puede usarlos en ninguna forma.

Similar al anterior es el derecho de oposición al tratamiento del total o de una parte de sus datos personales. La valoración de la aplicabilidad de este derecho depende de las circunstancias particulares, sobre todo, del objetivo del procesamiento y de la base legal que lo justifica. Sin embargo, en el caso del procesamiento de datos personales con fines de marketing directo, este derecho es absoluto e inmediato.

Luego, el derecho a la portabilidad de los datos permite a las personas solicitar al responsable del tratamiento, los datos personales que le corresponden y que le ha proporcionado al comercio; también es posible que se le pida que los datos sean transmitidos directamente a otro responsable, y esta obligación se extiende a la información que la empresa haya podido recabar mediante el análisis de las actividades que realiza la persona en internet. Los datos deben proporcionarse en un formato estructurado, comúnmente utilizado y legible para una máquina.

Además, se debe dar a conocer al internauta si el comercio, ya sea directamente o por medio de terceros, toma decisiones automatizadas con el uso de herramientas netamente tecnológicas o elabora perfiles a partir de estos procedimientos para evaluar aspectos personales de un usuario. Al respecto, está prohibido

usar estas herramientas para tomar decisiones que produzcan efectos jurídicos o tengan consecuencias adversas similares para el interesado, debido a que afectan a aspectos importantes en su vida relacionados con otros derechos o libertades fundamentales. Para los demás asuntos, el responsable debería poner a disposición del interesado información significativa sobre el razonamiento que se usa en estas herramientas automáticas y que, en todo momento, puede ser objeto de alegación por parte del interesado.

En caso de que no se haya atendido el requerimiento del interesado, se debe justificar razonadamente por qué no se ha dado una respuesta, y poner en conocimiento del solicitante las acciones legales o administrativas que puede ejecutar. Adicionalmente, estos derechos serán gratuitos a menos que sean excesivos o infundados; en cuyo caso, el comercio puede fijar un precio para cumplir con la solicitud. Para el caso de los *e-commerce*, lo ideal es proporcionar al usuario un mecanismo para realizar estas solicitudes por vía electrónica, preferiblemente desde la propia web.

También es relevante el hecho de que el responsable del tratamiento de datos debe ser capaz de demostrar, de forma efectiva y en todo momento, tanto a los interesados como a las autoridades y al público, que viene ejecutando adecuadamente las obligaciones a ellos impuestas en virtud del principio de responsabilidad proactiva.

1. Accesibilidad técnica y lingüística

Ya se ha visto como la norma pretende incidir de forma importante en las transacciones electrónicas que se llevan a cabo mediante una plataforma web, al regular estas con una serie de obligaciones que el comercio deberá cumplir. Sin embargo, los límites anotados tampoco son suficientes para cumplir eficientemente el espíritu de la norma, ya que dejan abierto un abanico de posibilidades sobre cómo estas obligaciones han de ser cumplidas. Por ej., aunque con el pasar del tiempo los comercios cumplan la normativa, en ocasiones lo hacen mediante la publicación de políticas y términos de muy difícil acceso dentro de la plataforma; o

⁶ En este punto es interesante la sentencia del CJEU, C-131/12, Google Spain SL, Google Inc. versus la Agencia Española de Protección de Datos (AEPD).

efectivamente permiten el ejercicio de los derechos del usuario, pero mediante procesos tan complejos, que al final resultan inútiles. Puede pasar también que estos términos y políticas están presentes en extensiones poco razonables, de modo que no habrá manera de que el usuario las lea; menos aún, cuando la comodidad es una ventaja muy valorada en este tipo de modelo de negocio y, dado que leer políticas extremadamente largas, con tecnicismos o incomprensibles, no resultaría nada cómodo para un internauta.

Este es justamente el gran problema al que nos enfrentaremos en un futuro cercano, pues si los avisos legales no fueron de fácil acceso, si el usuario ni siquiera los notó, o si estuvieron presentes, pero en una extensión tal que era casi imposible que el internauta los lea, sería adecuado dudar de si el usuario ha dado su consentimiento informado. Y evidentemente no sería así, porque la información que se dé al usuario ha de ser concisa, transparente, inteligible y de fácil acceso.

Pues bien, para entender a qué se refiere la accesibilidad técnica es necesario comprender que no solo es importante colocar toda la información en el sitio web, sino que, además, esta debe ser de fácil acceso; pues, de otra manera, poco se lograría con tener los datos completos en la web si un usuario medio es incapaz de identificarlos dada la complejidad de diferenciarlos de los otros elementos.

Este aspecto forma parte integrante del cumplimiento de las obligaciones legales en materia de protección de datos. Aquí ya no se aborda el qué se debe cumplir, sino el cómo; y, para hacerlo operativo, es esencial desarrollar procesos intuitivos que permitan llegar hasta los avisos legales, formularios y otros elementos que garanticen el efectivo cumplimiento de las obligaciones antes descritas; esto. Tal procedimiento debe ser posible para un internauta sin que este sea un experto en el uso de plataformas digitales. Así, se entiende que las herramientas puestas a disposición de los individuos deben ser de uso sencillo e idealmente amigables.

En suma, el comercio no usará las herramientas tecnológicas de las que dispone solo para mejorar la experiencia del usuario o para inducirlo a la compra, sino también para conseguir una plataforma web en la

que, por los elementos que incorpora, la persona sienta confianza al usarla, y perciba que efectivamente la empresa ha puesto esfuerzo en dejar a la vista las condiciones bajo las cuales prestará su consentimiento. Este proceder, sin lugar a duda generará un impacto positivo en el potencial comprador, quien no temerá que el comercio pretende ocultar información.

Para lograrlo habrá que tener en cuenta los requerimientos siguientes:

- Los avisos legales deberán estar disponibles en todo momento durante la navegación de la página web.
- Los procesos no han de ser complicados en el sentido de que obliguen al usuario a adelantar y retroceder en las páginas para conseguir información.
- El despliegue de los avisos debe evitar interrumpir la navegabilidad del usuario; y, en este sentido, es recomendable el uso de ventanas tipo *pop-up*.
- Los avisos legales deben ser fáciles de distinguir y, para conseguirlo, hay que cuidar la ubicación, el tipo y el tamaño de la letra.
- Idealmente, el formato de los avisos legales debe permitir archivarlos.
- Los avisos legales deben ser accesibles desde cualquier dispositivo móvil.
- Los procedimientos para retirar el consentimiento o ejercer los derechos también deben estar técnicamente optimizados, de modo que sean igual de sencillos que los que se usan para conseguirlo.
- No se pueden usar, en ningún caso, casillas ya marcadas.

Luego, y en relación con la accesibilidad lingüística, ha de considerarse que los textos que se ponen a disposición del interesado han de proporcionar, en su conjunto, un mensaje inteligible; y, por ende, usar términos que faciliten el entendimiento de los avisos legales para los internautas. También, en este aspecto se debe considerar que la extensión de los avisos legales

debe ser razonable y, de preferencia, debe incorporar diagramas, ejemplos u otros elementos que ayuden al lector a comprender el mensaje; para lograrlo se deberían tener presentes los siguientes puntos:

- La información que se facilita debe ser concisa, y debe transmitirse con un lenguaje claro y sencillo, a fin de evitar el uso de tecnicismos.

- La información debe estructurarse razonadamente en párrafos breves y, en su conjunto, el mensaje debe ser fácil de comprender.
- La tecnología permite la implementación de elementos gráficos que facilitan la comprensión del texto y, por consiguiente, es recomendable usarlos.

AVISOS LEGALES EN LA WEB Y COMUNICACIONES COMERCIALES

Una vez que hemos visto las obligaciones, así como los aspectos que validan y apoyan en gran medida su cumplimiento, en este apartado se revisarán los puntos que usualmente se recogen en cada aviso legal.

1. Contrato de términos y condiciones

Usualmente, el contrato de términos y condiciones de la web cumplirá con el objetivo de informar al usuario sobre los datos del comercio, así como sobre la dinámica y proceso de compra dentro de la web. Respecto a este asunto se abordan las políticas de devolución, las garantías del usuario en el correcto manejo de la plataforma y se definen las responsabilidades de las partes. También se hace referencia a la protección de datos personales, a la política de *cookies* y también en el apartado de legislación y fuero; asimismo se suele hacer mención a los códigos de ética a los que el comercio esté adherido. Lamentablemente, en Ecuador no existe ningún tipo de iniciativa para la creación de códigos en esta rama, situación que se espera cambie con la expedición de la Ley Orgánica de Protección de Datos Personales, pues son especialmente necesarios para establecer pautas a seguir y para la resolución de conflictos.

2. Política de privacidad

En concreto, esta es la política en la que quedarán recogidas las obligaciones y derechos que se han explicado. Generalmente, una política adecuada empieza por informar al internauta quien es el responsable del tratamiento de los datos personales, y proporciona su información completa. Luego, explica cuáles son las finalidades por las cuales se recogen los datos

personales y relaciona esta información con la base legal del tratamiento. Después, se suele informar sobre el tipo de datos que se recogen y cómo, habitualmente existen datos que el usuario proporciona al comercio. Hay datos que la empresa los recoge cuando el internauta navega en la web, otros vendrán de redes sociales o incluso de medios, tales como llamadas telefónicas, mensajes de texto o correos electrónicos y, en plataformas más modernas, de llamadas al robot de la página web.

Además, se informa sobre los terceros con quienes se comparten los datos personales: qué información se les proporciona, con qué fin y en qué condiciones. Hay que considerar que las empresas prestadoras de servicios de *hosting*, de publicidad online y de transporte, comúnmente tienen acceso a datos personales de los clientes de la empresa. También se debe hacer referencia al tiempo que se pretende mantener la información y a las medidas de seguridad que se han implementado en la web.

Finalmente, y de modo fundamental, deben explicarse al usuario los derechos que le corresponden y la forma en que puede ejercitarlos; una política responsable no hace solo una mera lista de estos, sino que los explica en términos sencillos y pone a disposición de la persona vías fáciles para elevar las correspondientes solicitudes al comercio.

3. Política de *cookies*

Este aviso legal es el más duro de comprender para los usuarios, dado el tecnicismo de algunos términos

y, así, representa un reto para el comercio en cuanto a la forma en la que se proporciona la información al usuario. Para empezar, hay que explicar en palabras sencillas qué es una *cookie* y cuáles son los tipos de *cookies* que se usan en el sitio web. Esta herramienta es en extremo versátil y útil, pues permite entre otras cosas: el uso de los carritos de compra, personalizar la página web para el usuario en una segunda visita, almacenar información relacionada a la forma de pago del cliente, analizar y segmentar a los visitantes del sitio, así como enviar y presentar publicidad. Esta tecnología es de vital importancia para lograr el cometido de una plataforma web. Por esta razón, ni bien el internauta aterriza en la página de inicio, el comercio ya pide su consentimiento para usar *cookies*.

Al efecto, es especialmente recomendable usar tablas, paneles u otros elementos que permitan mostrar la relación entre la *cookie* que se implementa, su finalidad, su propiedad, su descripción y la vigencia, de modo que el internauta no se sienta abrumado por términos técnicos o exceso de texto y termine por rechazar el uso de *cookies*. Asimismo, es indispensable que se informe al usuario del sitio cómo puede configurar el uso de *cookies* o, en su caso, deshabilitarlas y nuevamente recordar que, en virtud de los principios revisados, solo se debe recoger la información necesaria para los propósitos explicados al internauta.

4. Comunicaciones comerciales

Por último, se debe tener presente que, en toda transacción por internet, la comunicación electrónica

digital ocupa un papel primordial. En la actualidad, una de las herramientas más comunes que usan los comercios en línea para comunicar sus promociones y productos son las campañas de *mailing*.

Para usarlas se ha de tener presente que estas comunicaciones deben, en primer lugar, tener clara identificación de la persona que las envía. En el caso de promociones, ofertas o concursos, la información que se ofrezca debe ser inequívoca y sugerir con claridad las condiciones de acceso. Además, pueden ser enviadas solo si el interesado lo ha consentido de forma expresa (*opt-in*⁷) o si ya existe una relación contractual previa.

En todo caso, se debe ofrecer al destinatario la posibilidad de oponerse al tratamiento de sus datos para fines promocionales mediante un proceso que sea sencillo y gratuito. Este, además de estar presente en el momento de la recogida de los datos, debe constar en cada comunicación comercial, acompañado de una dirección de correo mediante la que el usuario pueda ejercitar su derecho. De no ser así, estas comunicaciones quedan prohibidas.

Nuestra legislación⁸ hace referencia a la publicidad y promoción por redes electrónicas, y hace énfasis en que el consumidor debe tener acceso a toda la información disponible relacionada al bien o al servicio del que se trate; igualmente exige que se facilite un medio sencillo para que el destinatario de las comunicaciones comerciales pueda solicitar la exclusión de listados con objetivos de marketing y publicidad.

CONCLUSIONES Y RECOMENDACIONES

La situación que vivimos hoy en día ha hecho que comprar por internet no sea solo una opción sino una necesidad. Si antes de esta emergencia el papel protagonista que tenía el *e-commerce* era innegable, de aquí en adelante advertiremos un crecimiento exponencial de transacciones electrónicas. La gran mayoría de las

empresas ecuatorianas, sean estas pequeñas, medianas o grandes, se encuentran en proceso de trasladar su negocio físico a internet, y lo están haciendo sin que exista normativa adecuada que alcance a regular eficientemente la cantidad de negocios que tenemos por delante con los nuevos hábitos de compra.

⁷ Acción mediante la cual, el internauta acepta recibir información sobre la empresa, usualmente vía correo electrónico.

⁸ Ley de Comercio Electrónico, Firmas y Mensajes de Datos, artículo 50.

Además, toda persona tiene derecho a conocer el propósito con el que se tratan sus datos y a controlar la forma en la que estos se emplearán, de forma que el uso indiscriminado de datos personales con fines económicos u otros que resulten poco éticos y causen daño al titular de la información están prohibidos.

A fin de evitar que los avisos legales por medio de los cuales se recaba el consentimiento del internauta para tratar datos personales resulten abusivos, los comercios deberían limitar sus acciones de tal manera que respeten las obligaciones en la materia. Hacerlo, a más de preparar al comercio para el cumplimiento de una ley a corto o mediano plazo que le faculte para operar lícitamente en el tráfico mercantil, le permitirá cumplir las expectativas de sus potenciales clientes y ganar credibilidad frente a estos. Hoy en día es fácil para el usuario comparar y verificar el nivel de responsabilidad, transparencia y esfuerzo puesto por otros comercios respecto del tratamiento de datos personales.

Con lo expuesto, es urgente que Ecuador cuente con una ley de protección de datos personales que salvaguarde derechos fundamentales de los ecuatorianos por diversas razones. Por un lado, debe existir una norma completa y suficiente capaz de garantizar a la persona un derecho sobre el uso y empleo de sus datos personales y de equiparar el desequilibrio entre comercios y usuarios, de modo que se reduzca la posición preferente en la que se encuentra una empresa con sus avisos legales frente al usuario del servicio que no tiene ninguna capacidad de negociación. Por otro lado, también se necesita una normativa que promueva el desarrollo del *e-commerce* en nuestro país, y que haga factible el intercambio comercial con otros territorios que exigen niveles mínimos de protección de datos para realizar negociaciones. Ahora bien, esta normativa debe estar a la altura de las exigencias de otros países y tendría que ocuparse no solo sobre qué se debe informar o qué derechos le asisten al internauta, sino que también debería dar pautas sobre cómo deben cumplirse las obligaciones que le sean aplicables al comercio. En relación con este punto, es esencial tener en cuenta aspectos técnicos y lingüísticos, de suerte que se asegure que el consentimiento sea

efectivamente una manifestación de voluntad libre, inequívoca, específica e informada. De la mano de una nueva ley debería promoverse la creación de entidades de certificación con códigos de conducta propios que sin duda impulsarán buenas prácticas entre los comercios más relevantes que se posicionen en Ecuador. Es claro que la norma, por su propia naturaleza, que ha de ser flexible para poder adaptarse a los nuevos retos del ámbito tecnológico, no puede ahondar en cuestiones tan específicas sobre el cómo cumplir las obligaciones en la materia, pero sí que lo puede hacer una entidad de certificación.

Finalmente, es importante decir que estas medidas no deben ser una razón para creer que el internauta va a restringir demasiado las posibles acciones de los comercios en relación con el tratamiento de sus datos personales; de facto, los usuarios aceptan compartir su información para recibir ciertos servicios y lo harán más aún si sienten esa confianza que genera el hecho de que puedan identificar prácticas responsables por parte de la empresa⁹. Además de que, como ya se explicó, hacerlo les permitirá participar lícitamente de la dimensión internacional de este tipo de comercio.

Recomendaciones

Antes de implementar cualquier herramienta para recolección de datos en la web, es recomendable, en primer lugar, definir con precisión los propósitos del tratamiento de datos personales, que deben estar relacionados con la actividad de la empresa. Asimismo, se debe identificar la base legal que respalde el tratamiento de los datos personales para ese fin y, luego, analizar cuidadosamente cuáles son los datos estrictamente necesarios para el cumplimiento de dichos fines. Con este análisis podremos ya escoger las herramientas tecnológicas más apropiadas para recolectar y tratar la información sin que se recojan datos irrelevantes y excesivos. En el proceso de recabar el consentimiento del usuario es recomendable que el *e-commerce* incorpore una página de visualización obligatoria del aviso legal antes de que el internauta pueda marcar la casilla de aceptación; así se presume que la persona ha dado su consentimiento informado.

⁹ Estudio realizado por la compañía *Accenture Interactive* denominado *Pulse Check 2018 Making it Personal*.

También es recomendable que, una vez implementada la web, junto con las pruebas en las que se verifique la experiencia del usuario, se compruebe la accesibilidad técnica. El usuario debería ser capaz de ubicar los avisos legales sin dificultad y de ejecutar órdenes sencillas que validen la facilidad de los procesos relacionados a la protección de datos personales.

Finalmente, se debe comprobar que se han tenido en cuenta todos los puntos mencionados en este

documento, y, para conseguirlo, nada mejor que una lista de verificación en la que se anote si se cumple o no con cada parámetro, de modo que sea posible cuantificar el nivel de cumplimiento. No estará por demás hacer este control con cada actualización del sitio web.

Estas recomendaciones no son más que una parte de un proceso de planificación para una mejora continua que, de cumplirse, dará a la empresa una ventaja competitiva sobre aquellas que no lo hagan.

BIBLIOGRAFÍA

- Accenture Interactive. 2018. "Making it Personal. Why brands must move from communication to conversation for greater personalization. Pulse Check 2018." Acceso el 15-IV-2020. https://www.accenture.com/_acnmedia/PDF-83/Accenture-Making-Personal.pdf#zoom=50
- Adelola, Tiwalade. Dawson, Ray y Batmaz, Firat. 2015. "Privacy and data Protection in e-commerce in developing nations: evaluation of different data protection approaches". *Journal for Digital Society* 6: 950-959. Acceso el 10-IV-2020. <https://pdfs.semanticscholar.org/ae95/5ceae73996d0d-59ba1a55afaad101405744b.pdf%20> <https://www.omicsonline.org/open-access/data-privacy-issues-and-possible-solutions-in-ecommerce-2168-9601-1000294-104325.html>
- Albaladejo, Manuel. 2002. *Derecho Civil. Introducción y Parte General*. Barcelona: Librería Bosch S.L.
- Alonso Conde, Ana. 2004. Comercio electrónico: antecedentes, fundamentos y estado actual. Madrid: Dykinson. <https://bv.unir.net:3555/es/ereader/unir/60875>
- Anteportamlatinam Valero, José. 2014. Relevancia del e-commerce para la empresa actual. Tesis de Licenciatura en Administración y Dirección de Empresas. Universidad de Valladolid.
- Brkan, Maja y Psychogiopoulou, Evangelia. 2017. *Courts, Privacy and Data Protection in the Digital Environment*. Cheltenham: Edward Elgar Publishing Limited.
- European Union Agency for Fundamental Rights and Council of Europe. 2018. *Handbook on European data protection law*. Luxembourg: Publications Office of the European Union.
- Frosini, Vittorio. 1988. *Informática y Derecho*. Bogotá: Editorial Temis.
- Flume, Werner. 1998. *El Negocio Jurídico*. Madrid: Editorial Fundación Cultural del Notariado.
- Herrán, Ana. 2003. *El derecho a la protección de datos personales en la sociedad de la información: Cuadernos Deusto de derechos humanos*. Bilbao: Universidad de Deusto.
- Illescas Ortiz, Rafael. 2019. *Derecho de la contratación electrónica*. Pamplona: Editorial Civitas.
- Information Commissioner's Office. 2018. "Guide to the General Data Protection". Acceso el 25-IV-2020. <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/>
- Lazpita, María. 1994. "Análisis comparado de las legislaciones sobre protección de datos de los Estados miembros de la Comunidad Europea". *Informática y Derecho* 6-7: 397-420. Acceso el 3-IV-2020. <https://dialnet.unirioja.es/servlet/articulo?codigo=248383>
- Lodder, Arno y Murray, Andrew. 2017. *EU Regulation of e-commerce*. Cheltenham: Edward Elgar Publishing Limited.
- Martín Bernal, José. 2001. "Internet y Virtualización del Derecho en General y del Derecho Civil en Particular". *Revista Actualidad Civil* 2: 443-459. Acceso el 20-IV-2020. <http://actualidadcivil.laley.es>
- Pinochet, Ruperto. 2004. "La Formación del Consentimiento a Través de las Nuevas Tecnologías de la Información". *Ius et Praxis* 10: 267-320. Acceso el 2-IV-2020. https://scielo.conicyt.cl/scielo.php?script=sci_arttext&pid=S0718-00122004000200009#nota46

Rodríguez Adrados, Antonio. 2000. "El Documento Negocial Informático". *Notariado y Contratación Electrónica*, editado por Consejo General del Notariado, 353-74. Madrid: Colegios Notariales España.

Seoane, Eloy. 2005. *La nueva era del comercio electrónico*. Madrid: Ed. Ideas propias.

Singh, Avinash. 2018. "E-Commerce interfering with Privacy: Perceived Risks and Security issues with Techno-policy outcomes". En *Digital Transformation Strategies and trends in E-learning* 1: 802-23. Acceso el 10-IV-2020. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3298224

Piñar Mañas, José. 2003. "El derecho a la protección de datos de carácter personal en la jurisprudencia del Tribunal de Justicia de las Comunidades Europeas". *Cuadernos de Derecho Público* 19-20: 45-90. Acceso el 15-IV-2020. <https://core.ac.uk/download/pdf/61482627.pdf>

Vega Clemente, Virginia. 2013. "COMERCIO ELECTRÓNICO Y PROTECCIÓN DE DATOS". *Revista de Estudios Económicos y Empresariales* 25: 205-244. Acceso el 11-IV-2020. <https://core.ac.uk/download/pdf/72044528.pdf>

Legislación

Carta de los Derechos Fundamentales de la Unión Europea (Parlamento, Consejo y Comisión Europea, 7-XII-2000).

Constitución de la República (Ecuador, Registro Oficial No. 449, 20-X-2008).

Convenio No. 108 del Consejo de Europa para la Protección de las Personas con Respecto al Tratamiento Automatizado de datos de Carácter Personal (Consejo de Europa, 28-I-1981).

Directiva 95/46/CE. Relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Parlamento Europeo y del Consejo, 24-X-1995).

Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos (Ecuador, Registro Oficial No. 557, 17-IV-2002).

Proyecto de Ley Orgánica de Datos Personales (Ecuador, Memorando No. PAN-CLC-2019-0184, 19-IX-2019).

Reglamento General de Protección de Datos de la Unión Europea (Parlamento y Consejo de la Unión Europea, Reglamento (UE) 2016/679, 27-IV-2016).