1. Introdução

O termo compliance tem origem no verbo em inglês "**to comply**", que significa agir de acordo com uma regra, uma instrução interna, um comando ou um pedido, ou seja, estar em "**compliance**" é estar em conformidade com leis e regulamentos externos e internos. Neste sentido a finalidade do **compliance digital** é assegurar que os processos adotados pela **empresa** no meio **digital** sejam compatíveis com as leis e regulamentações específicas desse ambiente.

O Comércio eletrônico ou E-commerce é o comércio virtual um tipo de transação comercial feita especialmente através de um equipamento eletrônico, como, por exemplo, computadores e smartphones. Os tipos de *e-commerce* são: Business to Business (B2B), Consumer to Consumer (C2C), Business to Consumer (B2C), Business to Administration (B2A), o Business to Business (B2B), é a venda atacado, ou seja, somente para empresas.

2. A importância do compliance digital e adequação a Lei Geral de Proteção de Dados Pessoais (LGPD)

Para aumentar a confiança do consumidor nas lojas virtuais e tornar o segmento cada vez mais forte, é indispensável que o e-commerce esteja de acordo com as boas práticas de mercado.

Atualmente, só no Brasil, a internet é a responsável por movimentar bilhões de reais. Segundo dados da empresa de segurança digital Compre&Confie, em 2019, as compras pela internet cresceram 23% e somaram R$ 17 bilhões, o que garantiu ao país ser o líder de vendas on-line na América Latina e o 10ª no ranking mundial.

É essencial destacar que as vendas virtuais estão cada vez mais em evidência, sobretudo, em tempos de pandemia, onde o isolamento e o distanciamento social se fazem necessários. Dessa forma, é preciso ainda mais segurança quando se trata de fornecer dados pessoais, por isso que surge a necessidade de uma política de proteção de dados eficiente.

Para tal, as empresas devem pensar em mecanismos e *Compliances*, justamente para tranquilizá-los e permitir que desfrutem de toda comodidade e praticidade que a internet oferece.

Segundo estudos da ABComm - Associação Brasileira de Comércio Eletrônico, o Brasil registrou um aumento de 400% no número de lojas que aderiram às vendas pelo comércio eletrônico, a fim de manter as atividades no mercado e impulsionar as vendas.

Enquanto antes da pandemia, a média mensal era de 10 mil *e-commerces*, sendo que durante a quarentena, esse número saltou para 50 mil. Entretanto, esse novo mercado, apesar de promissor, ainda enfrenta resistências por parte da população no âmbito da segurança.

3. Confiabilidade do sistema de Comércio Eletrônico

As compras realizadas pela internet demandam que o consumidor disponibilize uma grande quantidade de dados pessoais (RG, CPF, endereço, data de nascimento, telefone, e-mail, número do cartão de crédito, dentre outras), sendo que na prática cotidiana, ou seja, nas compras feitas em lojas físicas, esses documentos não são exigidos na mesma quantidade e frequência, principalmente se a compra é realizada com pagamento em espécie.

Embora as compras através do *e-commerce* tenham aumentado, os brasileiros ainda se sentem inseguros em relação à compra on-line, sendo a falta de confiança para informar dados pessoais, uma insegurança que supera, por exemplo, o medo de comprar um produto e não o receber.

Assim, uma vez que o comercio eletrônico gira em torno dos dados pessoais, é preciso olhar para a segurança e proteção do consumidor, inclusive no tocante à proteção e à privacidade desses dados

particulares, visando dar segurança jurídica para as partes no negócio, com o objetivo de coibir excessos e garantir maior transparência e legitimidade no *e-commerce*.

No Brasil, quando se fala em ferramentas de segurança ao consumidor, podemos citar, além do Código de Defesa ao Consumidor (CDC), outros instrumentos normativos, como por exemplo, o Decreto do *e-commerce*, que em seu art. 4°, inciso VII, determina a utilização de mecanismos de segurança eficazes para o tratamento de dados pessoais.

Há também o Marco Civil da Internet (art. 3°, II e III) que tem como um dos princípios centrais, a questão da proteção da privacidade e dos dados pessoais, e por fim, a Lei Geral de Proteção de Dados (LGPD), que garantirá a responsabilização por incidentes advindos da ineficiência no processo de segurança, incluindo o vazamento dos dados pessoais por parte da empresa.

As multas previstas para o descumprimento variam de 2% do faturamento até R$ 50 milhões (por infração). E para além das penalidades pecuniárias que podem ser impostas às empresas, a ausência de segurança nos dados pessoais obtidos e de adoção de boa prática de governança de dados, acarretará certamente sérios danos à imagem negocial e reputação, tais como: advertências, bloqueio dos dados pessoais até regularização da infração, proibição parcial ou total do exercício das atividades relacionadas a tratamento de dados; eliminação dos dados pessoais; publicização infração.

3.1 Outras formas de aumentar a confiabilidade

Para aumentar a confiança do consumidor nas lojas virtuais e tornar o segmento cada vez mais forte, é indispensável que o *e-commerce* esteja de acordo com as boas práticas de mercado, tais como:

Plataformas de pagamento seguras: Muitas das plataformas que dão suporte as lojas virtuais, oferecem integração com várias ferramentas ao mesmo tempo. Essas ferramentas proporcionam segurança e credibilidade nas suas funcionalidades. As conhecidas no mercado por sua seriedade e confiança são: PagSeguro, PicPay, Mercado Pago, PayPal, Cielo, entre outras.

Termos de uso: Trata-se das regras para utilização do serviço on-line, sendo de interesse do proprietário do site/app possuir este tipo de contrato eletrônico para se resguardar de quaisquer riscos jurídicos.

Indicação do Encarregado dos dados (DPO): Com a vigência da LGPD, as empresas que coletam e armazenam dados pessoais dos clientes precisarão se adaptar diante das novas diretrizes quanto ao armazenamento desse tipo de dados. Surge então a figura do "Encarregado dos Dados" ou "Data Protection Officer".

A função deste profissional será a de ajudar as empresas a cumprirem suas obrigações legais, buscando um tratamento adequado para com os dados dos no caso em análise em relação aos consumidores. Esse especialista funcionará como uma ponte entre as empresas, os consumidores e a Autoridade Nacional de Proteção de Dados (ANPD).

Isto significa que todos os *e-commerces* ou qualquer empresa que possua um website ao qual coleta dados pessoais dos consumidores, deverão indicar explicitamente no website quem será o encarregado (DPO) da empresa. Esse mecanismo é uma verdadeira inovação no cenário nacional, porque traz uma maior confiabilidade ao sistema de vendas virtuais, uma vez que o profissional apresentará sua credencial para garantir a segurança dos clientes.

Os consumidores como titulares dos dados pessoais, podem requisitar informações sobre o tratamento de suas informações; possuem direito à qualidade das informações que são tratadas a seu respeito, podendo, inclusive, solicitar correções; podem revogar o consentimento para tratamento de dados a qualquer tempo; e passaram a ter direito a solicitar a portabilidade de seus dados para migração para outras plataformas. Devem ser informados sobre a finalidade do

tratamento, inclusive quando for pretendida a disponibilização de tais informações com empresas parceiras do e-commerce. Podem requisitar, inclusive a eliminação de seus dados.

Política de cookies: Um cookie é um arquivo de texto que é baixado em seu computador ao acessar determinadas páginas da web. Os cookies permitem que essa página, entre outras coisas, possa armazenar e recuperar informações sobre os hábitos de navegação dos clientes/titulares dos dados. Imprescindível obedecer a lei quanto ao tratamento de dados pessoais, com base nas questões da **finalidade, adequação, necessidade e transparência**.

Análise e revisão dos contratos com fornecedores: Prestar atenção se o fornecedor não atrasa os pedidos, entrega o produto e serviço com qualidade, sem oscilação brusca de preço, com boa reputação no mercado e principalmente, se ele respeita o Código de Defesa do Consumidor e mantém as políticas de adequação à LGPD e governança de dados.

Políticas de Privacidade: Elaborar política de privacidade com objetivo de transparência ao tratamento de dados pessoais em um determinado serviço, atendendo os princípios da Lei Geral de Proteção de Dados Pessoais (LGPD).

4. Conclusão

Diante do exposto é primordial alertar os empresários da urgência à implementação da Lei Geral de Proteção de Dados (LGPD), sua inércia é assumir os riscos ao negócio, pois os processos de conformidade e adequação são longos e contínuos e devem ser imediatamente aplicados.

Todos os esforços devem representar uma verdadeira mudança de paradigma, adaptando a "Cultura" da empresa à nova realidade ditada pela sociedade dos dados, havendo real mudança de hábitos e costumes de todos os envolvidos no processo.

Em suma, estar em *compliance* é assegurar a credibilidade, reputação e o alto grau da maturidade da governança e por consequência a boa imagem da empresa, aliada à redução de custos com eventuais penalidades por descumprimento da lei. É acima de tudo, garantir o sucesso do *e-commerce* no mercado e agregar ainda mais valor ao segmento on-line.

Fontes

https://www.istoedinheiro.com.br/pandemia-do-coronavirus-faz-e-commerce-explodir-no-brasil/

https://www.tecmundo.com.br/mercado/138700-pesquisa-revela-brasileiro-sente-inseguro-comprar-internet.htm

BRASIL. Lei 13.7098/2018. Brasília. DF: 2018. Disponível em: www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Lei/L13709.htm

Brasil. Regulamenta a **Lei nº 8.078, de 11 de setembro de 1990**, para dispor sobre a contratação no **comércio eletrônico**. Disponível em http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2013/Decreto/D7962.htm