

**Tema:**  
**Neurociência e Inteligência artificial:  
As novas interfaces do conhecimento**



## **CIBERSEGURANÇA NO E-COMMERCE: POSTURA EMPRESARIAL E A EFICÁCIA DA LGPD**

Kessia BUENO DE SOUZA<sup>1</sup>  
Ketlyn DE SOUZA SALUSTRIANO<sup>2</sup>  
Marcelo ASCENCIO GARCIA FILHO<sup>3</sup>

**RESUMO:** O presente resumo visa apresentar como as empresas de atuação de ambiente virtual podem evitar o vazamento de dados de seus clientes através de mecanismos de cibersegurança. Para isso, busca-se através do método casuístico, utilizando o caso “Netshoes”, e por meios descritivos dizer qual o melhor posicionamento que a empresa deve adquirir, utilizando-se do caso “Netshoes”, focando na preservação da imagem da empresa. Para além, conceituar dados pessoais, introduzindo a LGPD como um meio jurídico de auxílio destas empresas.

**Palavras-chave:** Empresas. Vazamento de dados. LGPD

### **1 INTRODUÇÃO**

No contexto do e-commerce, onde o processo de compra ocorre inteiramente online, os riscos de violações são intensificados. Esse sistema abrange a comercialização de produtos e serviços pela internet, desde a seleção até o pagamento, expondo frequentemente dados pessoais e financeiros dos consumidores. A natureza digital dessas operações torna as plataformas de e-commerce alvos atrativos para cibercriminosos, que buscam explorar vulnerabilidades para obter acesso indevido a informações sensíveis.

<sup>1</sup> Discente do 2º ano do curso de Gestão Comercial do Centro Universitário Antônio Eufrásio de Toledo de Presidente Prudente. [kessia.bueno@hotmail.com](mailto:kessia.bueno@hotmail.com)

<sup>2</sup> Discente do 1º do curso de Direito do Centro Universitário Antonio Eufrásio de Toledo de Presidente Prudente. [ketlynsalustriano7@gmail.com](mailto:ketlynsalustriano7@gmail.com)

<sup>3</sup> Discente do 2º ano do curso de Análise e Desenvolvimento de Sistemas do Centro Universitário Antônio Eufrásio de Toledo de Presidente Prudente. [garciamarcelo.filho@gmail.com](mailto:garciamarcelo.filho@gmail.com)

Dentro deste cenário de aumento dessas atividades digitais presentes em nossas rotinas, trouxe a preocupação com a proteção dos dados pessoais desses clientes, resultando na criação da Lei Geral de Proteção de Dados (LGPD) – Lei N. 13.709/2018 – no Brasil, sancionada pelo então presidente Michel Temer em 2018, entrando em vigor em setembro de 2020. A LGPD estabelece diretrizes para o tratamento de dados pessoais, definindo responsabilidades, sanções e medidas corretivas em caso de violações.

Assim, faz-se importante neste momento uma devida preparação das empresas em relação a proteção dos dados de seus clientes, procurando uma segurança maior nos sistemas online utilizados. Essa preparação envolve não apenas a adoção de tecnologias avançadas de cibersegurança, mas também o estabelecimento de políticas internas de governança de dados, capacitação contínua dos colaboradores e um comprometimento com a transparência na comunicação com os consumidores.

## **2 DESENVOLVIMENTO**

Segundo a LGPD, dados pessoais são “informações relacionadas a pessoa natural identificada ou identificável” (art. 5º, § I), incluindo informações como nome, endereço, documentos e qualquer dado que permita a identificação de uma pessoa. Em casos de incidentes de segurança, como vazamentos de dados, a legislação estabelece a obrigação de reparação dos danos causados às partes afetadas. Embora a LGPD represente um avanço significativo na proteção de dados, ela também impõe desafios às empresas, especialmente aquelas que não adotam medidas de cibersegurança adequadas

O artigo 42 da lei prevê que “o controlador ou o operador que, em razão do tratamento de dados pessoais, causar dano patrimonial, moral, individual ou coletivo, é obrigado a repará-lo.” As penalidades incluem multas que podem atingir 2% do faturamento da empresa, limitadas a R\$ 50 milhões por infração (art. 52, § II). No entanto, a responsabilidade é atribuída somente se houver comprovação de que o dano foi causado pelo tratamento indevido de dados, conforme o artigo 43.

Um exemplo emblemático de falha na proteção de dados foi o caso da Netshoes, que, em 2017, teve informações de mais de dezoito mil clientes expostas

devido a um ataque cibernético. Dados como nome, e-mail, data de nascimento e histórico de compras foram acessados por hackers. Inicialmente, a Netshoes negou a ocorrência de invasões, admitindo o incidente apenas dois meses depois. A demora em reconhecer o problema e a falta de transparência demonstraram uma postura inadequada da empresa, que não estava preparada para responder efetivamente a uma crise de cibersegurança, afetando negativamente a confiança dos consumidores e a reputação da marca.

Para além de saber como fornecer um parecer aos seus consumidores, a empresa também deverá realizar reparos em seu sistema. A implementação de estratégias de cibersegurança é essencial nesse contexto, pois envolve a identificação e correção de vulnerabilidades. A cibersegurança, definida como a proteção de sistemas e dados contra acessos não autorizados e ataques cibernéticos, é fundamental para empresas que lidam com grandes volumes de informações pessoais. Para mitigar riscos, é essencial implementar medidas de segurança robustas, tais como:

1. **Firewall:** Sistemas de segurança que monitoram e controlam o tráfego de rede, bloqueando acessos não autorizados e prevenindo ataques cibernéticos.
2. **Testes de Intrusão (Pentests):** Simulações de ataques que permitem identificar e corrigir vulnerabilidades antes que sejam exploradas por atacantes.
3. **Treinamento de Colaboradores:** Capacitar funcionários para identificar ameaças cibernéticas e adotar boas práticas de segurança é essencial para reduzir riscos internos.
4. **Backup e Recuperação de Desastres:** Manter backups atualizados e planos de recuperação de dados para minimizar impactos em caso de incidentes.
5. **Transparência com o Consumidor:** Notificar rapidamente os clientes afetados por qualquer incidente, preservando a confiança na marca.

A cibersegurança no e-commerce exige uma abordagem proativa e bem estruturada. A LGPD oferece um marco regulatório essencial para a proteção de dados, mas a eficácia da lei depende diretamente da capacidade das empresas de implementar práticas eficazes de segurança e de responder com rapidez e clareza em casos de incidentes.

## CONCLUSÃO

Concluimos, então, que o desenvolvimento do comércio no ambiente digital evidencia que a *cibersegurança* é um pilar indispensável para a proteção de dados, especialmente diante do rigor imposto pela LGPD. O caso da *Netshoes*

exemplifica como a ausência de medidas preventivas e uma resposta inadequada a incidentes podem comprometer não apenas a segurança dos dados dos consumidores, mas também a credibilidade da empresa.

A conformidade com a LGPD vai além de um mero cumprimento legal; ela exige das empresas uma postura ativa na gestão de riscos cibernéticos, com a adoção de tecnologias avançadas, treinamentos contínuos e políticas claras de comunicação e transparência com os clientes.

Portanto, é essencial que as empresas de atuação digital invistam em uma infraestrutura de segurança robusta, realizando testes constantes de vulnerabilidade e atualizando suas estratégias conforme novas ameaças surgem. A proteção dos dados pessoais, além de evitar penalidades financeiras, fortalece a confiança do consumidor e consolida a imagem da empresa no mercado. Somente com um compromisso verdadeiro com a cibersegurança e a adaptação contínua às exigências da LGPD, as empresas poderão garantir um ambiente digital seguro e confiável, mitigando os riscos e promovendo um relacionamento ético e seguro com seus clientes.

## **REFERÊNCIAS**

Brasil. Presidência da República. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: [https://www.planalto.gov.br/ccivil\\_03/ Ato2015-2018/2018/Lei/L13709.htm](https://www.planalto.gov.br/ccivil_03/ Ato2015-2018/2018/Lei/L13709.htm)

G1 Tecnologia. Hackers expõem dados de clientes da Netshoes. G1, 2017. Disponível em: <https://g1.globo.com/tecnologia/noticia/hackers-expoem-dados-de-clientes-da-netshoes.ghtml>

CARNEIRO, Leandro; MOREIRA, Elton; TEIXEIRA, Adriano. Cibersegurança: Fundamentos, Gestão e Otimização. São Paulo: Brasport, 2020.

CUNHA, Brenno. O Vazamento de Dados do E-Commerce Netshoes: Implicações da Lei Geral de Proteção de Dados (LGPD). Mossoró, 2022.