
PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS
ESCOLA DE DIREITO E RELAÇÕES INTERNACIONAIS
NÚCLEO DE PRÁTICA JURÍDICA
COORDENAÇÃO ADJUNTA DE TRABALHO DE CURSO
ARTIGO CIENTÍFICO

# RESPONSABILIDADE DOS FORNECEDORES NA PROTEÇÃO CONTRA FRAUDES E CRIMES CIBERNÉTICOS EM TRANSAÇÕES ONLINE

ORIENTANDO (A): ARIANE FERREIRA DA SILVA
ORIENTADOR (A): PROF. (A): JOSÉ HUMBERTO ABRÃO MEIRELES

GOIÂNIA-GO
2024

ARIANE FERREIRA DA SILVA

# RESPONSABILIDADE DOS FORNECEDORES NA PROTEÇÃO CONTRA FRAUDES E CRIMES CIBERNÉTICOS EM TRANSAÇÕES ONLINE

Artigo Científico apresentado à disciplina Trabalho de Curso II, da Escola de Direito, Negócios e Comunicação, Curso de Direito, da Pontifícia Universidade Católica de Goiás (PUC GOIÁS).

Prof. Orientador: ME José Humberto Abrão Meireles.

GOIÂNIA-GO

2024

ARIANE FERREIRA DA SILVA

# RESPONSABILIDADE DOS FORNECEDORES NA PROTEÇÃO CONTRA FRAUDES E CRIMES CIBERNÉTICOS EM TRANSAÇÕES ONLINE

Data da Defesa: ____ de _____ de _____

BANCA EXAMINADORA

_____

Orientador: Prof. José Humberto Abrão Meireles Nota

_____

Examinador (a) Convidado (a): Prof. (a): Titulação e Nome Completo Nota

# RESPONSABILIDADE DOS FORNECEDORES NA PROTEÇÃO CONTRA FRAUDES E CRIMES CIBERNÉTICOS EM TRANSAÇÕES ONLINE

Ariane Ferreira da Silva[1]

Com o aumento das transações online, a proteção contra fraudes e crimes cibernéticos tornou-se essencial. Este estudo analisa a responsabilidade dos fornecedores em garantir a segurança dessas transações, destacando a importância de leis como o Código de Defesa do Consumidor (CDC) e a Lei Geral de Proteção de Dados (LGPD). O estudo examina casos reais e propõe soluções para melhorar a proteção dos consumidores. Os resultados mostram que os fornecedores precisam adotar medidas de segurança eficazes e que é fundamental educar os consumidores para reduzir os riscos. Conclui-se que a responsabilidade dos fornecedores é vital para manter a confiança nas plataformas digitais, e que uma colaboração entre leis, empresas e consumidores é necessária para um ambiente digital mais seguro.

**Palavras-chave:** Responsabilidade dos fornecedores. Crimes cibernéticos. Proteção ao consumidor. Fraudes online. Segurança digital.

[1] Qualificação do autor.

# SUMÁRIO

**INTRODUÇÃO**

**1 CONTEXTO ATUAL DE FRAUDES E CRIMES CIBERNÉTICOS**

1.1 TIPOS DE FRAUDES ONLINE

1.1.1 Phishing

1.1.2 Ransomware

1.2 IMPACTO DAS FRAUDES E CRIMES CIBERNÉTICOS NOS CONSUMIDORES

1.3 CONSCIENTIZAÇÃO E PREVENÇÃO

**2 MARCO LEGAL E TEÓRICO**

2.1 LEGISLAÇÃO APLICÁVEL

2.1.1. Código de Defesa do Consumidor (CDC)

2.1.2 Lei Geral de Proteção de Dados (LGPD)

2.1.3 Normas Internacionais

2.2. RESPONSABILIDADE CIVIL DOS FORNECEDORES

2.3. EDUCAÇÃO DOS CONSUMIDORES SOBRE RISCOS CIBERNÉTICOS

**3 ANÁLISE E DISCUSSÃO**

3.1 DESAFIOS NA IMPLEMENTAÇÃO DE MEDIDAS DE SEGURANÇA

3.1.1. Desafios para Pequenas e Médias Empresas

3.1.2 Desafios na Aplicação da LGPD

3.1.3 Soluções Propostas

3.2 COLABORAÇÃO INTERNACIONAL E EDUCAÇÃO DO CONSUMIDOR

**CONSIDERAÇÕES FINAIS**

**REFERÊNCIAS**

# INTRODUÇÃO

A digitalização das relações de consumo é uma tendência inegável na sociedade moderna. Com a crescente popularidade das transações online, os consumidores têm desfrutado de conveniência e eficiência sem precedentes. No entanto, essa transformação também trouxe consigo um aumento significativo das ameaças cibernéticas, como fraudes, phishing e outros crimes digitais, que comprometem a segurança financeira e pessoal dos usuários. Essas ameaças não discriminam, afetando tanto pessoas físicas quanto jurídicas, e criando um ambiente onde a segurança cibernética se tornou uma preocupação crucial.

Os métodos de fraude online evoluem rapidamente, tornando-se cada vez mais sofisticados e difíceis de detectar. Este cenário desafia continuamente as legislações existentes, que precisam se adaptar para acompanhar o ritmo das novas tecnologias. A confiança dos consumidores nas plataformas digitais e nas empresas de serviços financeiros está em jogo, uma vez que a segurança percebida é um fator determinante na decisão de realizar transações online. Portanto, assegurar um ambiente digital seguro é não apenas uma responsabilidade ética, mas também uma necessidade legal e comercial para os fornecedores.

A responsabilidade dos fornecedores em garantir a segurança das transações online é um tema de extrema relevância jurídica. É essencial compreender e definir claramente o papel dos fornecedores na proteção contra ameaças cibernéticas e na implementação de medidas preventivas e reparadoras adequadas. A definição clara desses direitos e responsabilidades não apenas protege os consumidores afetados, mas também promove práticas empresariais mais éticas e transparentes, fortalecendo a confiança no comércio eletrônico e nos serviços online.

Os impactos das fraudes e crimes cibernéticos são profundos, afetando tanto a segurança econômica quanto a confiança dos consumidores. Diante desse contexto, este estudo visa oferecer uma análise aprofundada das lacunas na legislação atual, elucidando os direitos dos consumidores em situações de fraude online e definindo

claramente a responsabilidade das empresas nesses contextos. Através da investigação de casos concretos e da aplicação de teorias jurídicas e de segurança da informação, espera-se fornecer insights valiosos para legisladores, empresas e consumidores.

# 1 SEGURANÇA CIBERNÉTICA E CONSUMO ONLINE

## 1.1. Contexto Atual de Fraudes e Crimes Cibernéticos: Descrição dos principais tipos e métodos de fraudes online.

Os crimes cibernéticos são uma realidade crescente e preocupante na sociedade moderna, com diversos tipos e métodos de fraudes online que afetam consumidores, empresas e governos em todo o mundo. A proliferação desses crimes está diretamente relacionada à expansão da internet e ao aumento do uso de dispositivos conectados. Entre os principais tipos de fraudes cibernéticas estão o phishing, ransomware, fraudes em e-commerce e roubo de identidade.

O phishing, segundo cita Crespo (2011), envolve o envio de mensagens fraudulentas que se disfarçam como comunicações legítimas de instituições confiáveis, com o objetivo de obter informações sensíveis, como senhas e números de cartões de crédito. Essas mensagens geralmente contêm links para sites falsos que imitam os originais, induzindo as vítimas a inserir seus dados pessoais.

O ransomware é outra forma grave de crime cibernético, onde um malware é instalado no sistema da vítima, criptografando seus dados e exigindo um pagamento para a liberação dos mesmos.

As fraudes em e-commerce são um problema crescente, especialmente com o aumento das compras online. Cavalieri Filho (2010) destaca que essas fraudes incluem a venda de produtos inexistentes, a criação de sites falsos de comércio eletrônico e o uso de informações de pagamento roubadas para realizar compras fraudulentas. Esse tipo de fraude não só causa perdas financeiras para os consumidores, mas também prejudica a confiança no comércio eletrônico.

O roubo de identidade é outro crime cibernético significativo, onde informações pessoais são obtidas e usadas de forma não autorizada para realizar transações fraudulentas.

Além desses métodos, os cibercriminosos estão constantemente desenvolvendo novas técnicas para enganar e explorar suas vítimas. Soares (2022) menciona a utilização da engenharia social, que manipula indivíduos para revelarem informações confidenciais.

Vieira (2024) destaca que a dark web facilita a realização de transações ilícitas, a venda de dados roubados e a disseminação de ferramentas de hacking. Essas plataformas anônimas tornam difícil rastrear e identificar os cibercriminosos, complicando ainda mais os esforços para combater esses crimes.

A responsabilidade de combater os crimes cibernéticos não recai apenas sobre os indivíduos, mas também sobre as empresas e o Estado. A implementação de normas rígidas de segurança cibernética, a aplicação de penalidades severas para os infratores e a educação contínua dos consumidores sobre os riscos e as melhores práticas de segurança são essenciais para reduzir a incidência e o impacto dos crimes cibernéticos.

Fica claro então que além das medidas tecnológicas, é de grande importância investir na conscientização do usuário. Campanhas educativas que instruam os consumidores sobre como identificar e evitar fraudes online podem ser tão eficazes quanto as ferramentas de segurança mais avançadas.

## 1.2. Impacto das Fraudes e Crimes Cibernéticos nos Consumidores: Análise dos impactos econômicos e psicológicos sobre os consumidores.

Os crimes virtuais têm um impacto profundo na sociedade moderna. Segundo Galvão e Silva Advocacia (2022), de acordo com o relatório mais recente da Symantec, conhecida pelo antivírus Norton, aproximadamente 65% dos adultos globalmente já foram vítimas de crimes virtuais, com uma taxa alarmante de 76% no Brasil. A predominância desses crimes está associada ao uso de vírus de computador, que representa 53% dos casos reportados. No entanto, há outros tipos de crimes notáveis, como fraudes online (10%), assédio sexual (7%) e golpes com cartão de crédito (7%).

Esses crimes afetam o patrimônio das vítimas, causando perdas financeiras substanciais e também violam sua privacidade, comprometendo sua reputação,

imagem e até mesmo sua liberdade sexual. As consequências vão além do dano imediato, afetando o bem-estar emocional e psicológico das vítimas. Segundo Cassanti (2014), os crimes virtuais expõem as vítimas a um estado de vulnerabilidade, criando um impacto duradouro em sua saúde mental.

Além do aspecto criminal, as infrações virtuais podem resultar em ações cíveis, onde as vítimas buscam indenização pelos danos sofridos. Cavalieri Filho (2010) destaca que a responsabilidade civil nesses casos envolve não apenas a reparação dos danos materiais, mas também dos danos morais. Os tribunais têm reconhecido o sofrimento psicológico e a ansiedade resultante dessas infrações, concedendo compensações para aliviar o sofrimento das vítimas.

De acordo com Farias, Rosenvald e Braga Netto (2022), a responsabilidade civil no contexto dos crimes cibernéticos deve ser abordada de maneira total, levando em consideração o impacto total sobre a vida das vítimas. O dano moral, frequentemente associado a violações de privacidade e difamação online, é um componente essencial das reivindicações civis.

No Brasil, o impacto dos crimes cibernéticos é intenso diante da alta taxa de ocorrência desses delitos. O crescente número de fraudes online e o uso indevido de dados pessoais exigem uma resposta robusta tanto do sistema de justiça quanto das empresas que operam no ambiente digital. As empresas têm a obrigação de implementar medidas de segurança eficazes para proteger os dados dos consumidores e evitar incidentes de segurança.

A proteção do consumidor no ambiente digital é uma responsabilidade compartilhada entre as empresas e o Estado. A legislação deve ser aprimorada para acompanhar a evolução tecnológica e garantir que os direitos dos consumidores sejam efetivamente protegidos. A implementação de normas rígidas de segurança cibernética e a aplicação de penalidades severas para os infratores são passos essenciais nesse processo.

Campanhas de conscientização podem ajudar a reduzir a vulnerabilidade dos consumidores e prevenir muitos dos crimes cibernéticos mais comuns.

Soares (2022) cita o dever de cuidado das instituições financeiras, que devem adotar medidas preventivas para evitar fraudes e proteger os dados dos clientes. A responsabilidade das instituições financeiras em casos de crimes cibernéticos vai

além do simples ressarcimento financeiro, abrangendo a adoção de práticas de segurança que previnam futuros incidentes.

É notado acerca das novas alternativas de proteção do consumidor no comércio eletrônico, enfatizando a necessidade de regulamentações mais rigorosas e de um sistema de monitoramento eficiente para detectar e prevenir fraudes. A proteção do consumidor no ambiente digital deve ser dinâmica e adaptável às novas ameaças que surgem constantemente.

Crespo (2011) argumenta que a colaboração internacional é essencial para combater os crimes cibernéticos de forma eficaz. As fronteiras físicas não limitam os criminosos virtuais, e uma abordagem global, envolvendo a cooperação entre diferentes países, é necessária para enfrentar a crescente ameaça dos crimes cibernéticos.

Após a conclusão do capítulo fica claro que os crimes cibernéticos têm um impacto profundo e abrangente sobre os consumidores, afetando tanto seu bem-estar econômico quanto psicológico. A responsabilidade civil, a educação dos consumidores e a colaboração internacional são componentes-chave para mitigar esses impactos e proteger os direitos dos consumidores no ambiente digital.

# 2 MARCO LEGAL E TEÓRICO

## 2.1. Legislação Aplicável: Análise do CDC, LGPD, e normas internacionais.

No que se refere a legislação fica notado que essa é fundamental para a proteção dos consumidores e também para a criação de um ambiente digital seguro e confiável. Os exemplos dessas leis no Brasil são o Código de Defesa do Consumidor (CDC), a Lei Geral de Proteção de Dados (LGPD). Também existem várias normas internacionais que desempenham papéis importantes na regulação das práticas de segurança da informação e na responsabilidade civil dos fornecedores.

O Código de Defesa do Consumidor (CDC) (Lei nº 8.078) é um marco na proteção dos direitos dos consumidores no Brasil. O CDC veio para reger os direitos básicos dos consumidores, incluindo a proteção contra produtos e serviços perigosos ou nocivos e a proteção contra publicidade enganosa e abusiva. Cavalieri Filho (2010) destaca que o CDC também impõe aos fornecedores a obrigação de fornecer informações claras e precisas sobre produtos e serviços, e também a responsabilidade por danos causados por defeitos de fabricação, design ou informações inadequadas.

Já a Lei Geral de Proteção de Dados (LGPD) estabelece diretrizes para a coleta, armazenamento, tratamento e compartilhamento de dados pessoais no Brasil. A LGPD visa proteger os direitos fundamentais de liberdade e privacidade dos indivíduos, garantindo a transparência e a segurança no tratamento de dados pessoais.

Também é válido citar as normas internacionais. A General Data Protection Regulation (GDPR) da União Europeia é uma das regulamentações mais rigorosas e abrangentes sobre proteção de dados no mundo. O autor Crespo (2011) mostra em seu trabalho que a GDPR estabelece padrões elevados para a coleta e tratamento de dados pessoais, impondo severas penalidades para violações, o que serve como referência para outras jurisdições, incluindo o Brasil.

A Convenção de Budapeste sobre o Cibercrime também estabelece diretrizes importantes para o combate aos crimes cibernéticos. Esta convenção internacional

visa harmonizar as leis nacionais, melhorar a cooperação internacional e desenvolver políticas comuns para combater o cibercrime. Farias, Rosenvald e Braga Netto (2022) destacam que a cooperação internacional é essencial para enfrentar a natureza transnacional dos crimes cibernéticos.

No Brasil, o CDC, a LGPD e as normas internacionais criam um ambiente que possibilita  a proteção dos consumidores. Mas é notado que Gonçalves (2014) cita sobre a efetividade dessas leis visto que dependem da implementação de medidas práticas e da conscientização dos consumidores e fornecedores sobre seus direitos e obrigações.

A adoção de normas rígidas de segurança cibernética e a aplicação de penalidades severas para os infratores são passos essenciais para garantir a proteção dos consumidores no ambiente digital. Neves e Tartuce (2014) argumentam que, além das medidas tecnológicas, é importante investir na educação dos consumidores sobre os riscos cibernéticos.

Soares (2022) destaca o dever de cuidado das instituições financeiras e outras empresas que lidam com dados sensíveis, reforçando a importância de adotar medidas preventivas para evitar fraudes e proteger os dados dos clientes.

## 2.2. Responsabilidade Civil dos Fornecedores: Discussão sobre a responsabilidade dos fornecedores na segurança das transações online.

A responsabilidade civil dos fornecedores no contexto das transações online é um tema muito importante, que se torna cada vez mais atual visto o aumento dos crimes cibernéticos e das fraudes online. O Código de Defesa do Consumidor (CDC) estabelece que os fornecedores são responsáveis por garantir a segurança e a qualidade dos produtos e serviços oferecidos aos consumidores.

A responsabilidade civil dos fornecedores se baseia no princípio da vulnerabilidade do consumidor, que reconhece a posição de desvantagem dos consumidores em relação aos fornecedores.

A responsabilidade civil no contexto das transações online inclui a obrigação de implementar medidas de segurança eficazes para proteger os dados pessoais dos consumidores. Cassanti (2014) destaca que, em casos de violação de dados ou

fraudes, os fornecedores podem ser responsabilizados pelos danos causados, incluindo danos materiais e morais.

A responsabilidade civil dos fornecedores também abrange a obrigação de informar os consumidores sobre os riscos associados às transações online e as medidas de segurança que devem ser adotadas. A falta de informação clara e precisa pode ser considerada uma falha do fornecedor, resultando em responsabilidade por danos causados.

No contexto da Lei Geral de Proteção de Dados (LGPD), a responsabilidade dos fornecedores é ainda mais acentuada. Farias, Rosenvald e Braga Netto (2022) destacam que a LGPD impõe obrigações específicas aos controladores e operadores de dados, incluindo a necessidade de adotar medidas de segurança técnicas e administrativas para proteger os dados pessoais contra acessos não autorizados ou qualquer forma de tratamento inadequado ou ilícito.

A responsabilidade civil dos fornecedores também envolve a obrigação de notificar os consumidores e as autoridades competentes em caso de incidentes de segurança. Gonçalves (2014) argumenta que a transparência e a comunicação rápida são essenciais para minimizar os danos e garantir que os consumidores possam tomar medidas adequadas para se proteger.

A responsabilidade dos fornecedores em transações online, especialmente quando envolve a segurança de dados, é chamada de **responsabilidade objetiva**. Isso quer dizer que o fornecedor é responsável por qualquer problema que cause prejuízo ao consumidor, mesmo sem culpa direta. O Código de Defesa do Consumidor (CDC) garante que, se o fornecedor falhar e isso prejudicar o consumidor, ele deve reparar o dano. Isso inclui casos em que os dados pessoais do consumidor são expostos em transações online.

Em casos onde mais de um fornecedor está envolvido, há **responsabilidade solidária**, ou seja, todos os fornecedores são responsáveis juntos. O consumidor pode escolher de quem cobrar pelos danos causados. Esse tipo de situação é comum em transações online, onde várias empresas e plataformas estão envolvidas.

Os tribunais brasileiros, como o Superior Tribunal de Justiça (STJ), têm aplicado essa regra para proteger o consumidor em casos de falhas de segurança, mesmo quando a fraude é feita por terceiros. Os fornecedores têm o dever de garantir a segurança dos dados e transações nas suas plataformas.

A legislação que apoia essa responsabilidade vem tanto do CDC quanto da Lei Geral de Proteção de Dados (LGPD), que exige que as empresas protejam os dados pessoais dos consumidores e adotem medidas para evitar problemas de segurança. Assim, os consumidores estão protegidos por essas leis no ambiente digital. A responsabilidade objetiva, solidária e baseada no princípio da vulnerabilidade do consumidor é uma ferramenta jurídica essencial para proteger os consumidores nas transações online.

# 3 ANÁLISE E DISCUSSÃO

Os crimes cibernéticos têm se tornado cada vez mais frequentes e complexos, afetando uma ampla gama de vítimas, desde indivíduos a grandes corporações. Um exemplo marcante é o ataque de ransomware sofrido pela empresa JBS em 2021. A JBS, uma das maiores processadoras de carne do mundo, teve seus sistemas de TI comprometidos, resultando na paralisação de várias plantas de processamento nos Estados Unidos, Canadá e Austrália. Os criminosos exigiram um resgate milionário em criptomoedas, que a empresa acabou pagando para recuperar o controle de seus sistemas. Esse incidente destacou a vulnerabilidade das infraestruturas críticas e a necessidade de medidas robustas de segurança cibernética.

Outro caso notório é o da Cambridge Analytica, que em 2018 foi acusada de coletar ilegalmente dados de milhões de usuários do Facebook sem consentimento, para influenciar processos eleitorais. Este caso evidenciou a fragilidade das plataformas de mídia social em proteger dados pessoais e a importância de uma legislação rigorosa de proteção de dados. A violação da privacidade dos usuários levou a um escrutínio global sobre as práticas de coleta e uso de dados das grandes empresas de tecnologia.

No Brasil, o caso da Netshoes em 2018 chamou a atenção. A empresa de e-commerce teve uma falha de segurança que expôs os dados de mais de 2 milhões de clientes. Informações como nomes, endereços, e-mails e históricos de compras foram acessadas indevidamente por hackers. Este incidente não só afetou a confiança dos consumidores na plataforma, mas também levantou questões sobre a responsabilidade da empresa em proteger os dados dos seus clientes.

Esses exemplos ilustram como diferentes tipos de fraudes cibernéticas e violações de dados podem impactar gravemente tanto empresas quanto consumidores. A análise desses casos revela padrões comuns, como a falta de medidas preventivas adequadas e a resposta lenta a incidentes. Além disso, destaca a necessidade urgente de um quadro regulatório mais eficaz e de uma cultura de segurança mais sólida nas empresas.

## 3.1 Desafios e Soluções: Discussão sobre os desafios na implementação de medidas de segurança e na legislação, com proposição de soluções

Um dos principais desafios na implementação de medidas de segurança cibernética é a constante evolução das ameaças. Hackers estão sempre desenvolvendo novas técnicas para burlar sistemas de segurança, o que exige que as empresas estejam continuamente atualizando suas defesas. No entanto, muitas empresas, especialmente pequenas e médias, carecem de recursos e expertise necessários para acompanhar essas mudanças, tornando-se alvos fáceis para ataques.

A legislação também enfrenta desafios significativos. Embora leis como a LGPD no Brasil e a GDPR na União Europeia representem grandes avanços na proteção de dados, sua implementação eficaz ainda enfrenta obstáculos. A aplicação dessas leis requer recursos significativos e a cooperação internacional, dado que os crimes cibernéticos muitas vezes cruzam fronteiras. Além disso, a falta de uniformidade nas leis de proteção de dados entre diferentes países pode complicar a resposta a incidentes globais.

Para mitigar esses desafios, é essencial que as empresas adotem uma abordagem proativa à segurança cibernética. Isso inclui a realização regular de auditorias de segurança, a implementação de protocolos de resposta a incidentes e a educação contínua dos funcionários sobre as melhores práticas de segurança. As empresas devem também investir em tecnologias avançadas de segurança, como inteligência artificial e machine learning, que podem ajudar a detectar e responder a ameaças em tempo real.

No âmbito legislativo, uma solução seria a harmonização das leis de proteção de dados a nível internacional. Organizações como a ONU e a Interpol podem desempenhar um papel crucial na facilitação da cooperação entre países e na criação de um quadro legal mais uniforme. Além disso, é necessário um aumento significativo nos recursos destinados à aplicação dessas leis, garantindo que as violações sejam tratadas de forma rápida e eficaz.

A colaboração entre o setor público e privado é outra estratégia fundamental. Governos e empresas devem trabalhar juntos para compartilhar informações sobre ameaças e desenvolver melhores práticas de segurança. Iniciativas como centros de

resposta a incidentes cibernéticos e fóruns de segurança podem facilitar essa colaboração e melhorar a capacidade de resposta a ataques.

A educação do consumidor também é crucial. Campanhas de conscientização podem ajudar os consumidores a reconhecer e evitar fraudes online, fortalecendo a primeira linha de defesa contra crimes cibernéticos. Informar os consumidores sobre a importância de práticas seguras, como o uso de senhas fortes e a verificação de autenticidade de sites, pode reduzir significativamente a vulnerabilidade a ataques.

As empresas devem adotar uma postura transparente em relação à segurança cibernética. Isso inclui comunicar claramente as políticas de privacidade e as medidas de segurança adotadas, bem como notificar prontamente os consumidores em caso de incidentes de segurança. A transparência não só aumenta a confiança dos consumidores, mas também demonstra o compromisso da empresa com a proteção de seus dados.

# CONSIDERAÇÕES FINAIS

A digitalização das transações comerciais trouxe conveniência e eficiência, mas também aumentou a exposição a fraudes e crimes cibernéticos. As ameaças evoluem rapidamente, desafiando a legislação e a segurança oferecida pelos fornecedores. A confiança dos consumidores depende diretamente da percepção de segurança nas plataformas digitais.

Este estudo destacou a importância da responsabilidade dos fornecedores em garantir a segurança das transações online. É essencial que as empresas adotem medidas preventivas robustas e estejam preparadas para oferecer reparações adequadas em casos de fraudes. A clareza nos direitos e responsabilidades dos consumidores é crucial para promover práticas empresariais mais éticas e transparentes.

A legislação atual, como o Código de Defesa do Consumidor e a Lei Geral de Proteção de Dados, fornece uma base importante, mas deve ser continuamente aprimorada para acompanhar a evolução tecnológica. Além disso, a educação dos consumidores sobre os riscos cibernéticos e as melhores práticas de segurança é fundamental para reduzir a vulnerabilidade.

Para finalizar, ficou claro que a proteção dos consumidores no ambiente digital é uma responsabilidade compartilhada entre legisladores, empresas e consumidores. Este estudo espera contribuir para um ambiente digital mais seguro e confiável, onde todos possam realizar transações com maior segurança e confiança.

# RESPONSIBILITY OF SUPPLIERS IN PROTECTING AGAINST FRAUD AND CYBERCRIMES IN ONLINE TRANSACTIONS

## ABSTRACT

As online transactions increase, protecting against fraud and cybercrimes has become crucial. This study examines the responsibility of suppliers to ensure the security of these transactions, emphasizing the importance of laws such as the Consumer Defense Code (CDC) and the General Data Protection Law (LGPD). The study reviews real cases and suggests solutions to enhance consumer protection. The findings indicate that suppliers must implement effective security measures, and educating consumers is key to reducing risks. It concludes that supplier responsibility is essential for maintaining trust in digital platforms, and a joint effort between laws, companies, and consumers is needed for a safer digital environment.

**Keywords:** Supplier responsibility. Cybercrimes. Consumer protection. Online fraud. Digital security.

**:**

# REFERÊNCIAS

CASSANTI, M. de O. Crimes virtuais, vítimas reais. 1. ed. Rio de Janeiro: Brasport, 2014.

CAVALIERI FILHO, Sérgio. Programa de responsabilidade civil. 9ª ed. São Paulo: Atlas, 2010.

CRESPO, Marcelo Xavier de Freitas. Crimes Digitais. São Paulo: Saraiva, 2011.

FARIAS, Cristiano Chaves de. ROSENVALD, Nelson. BRAGA NETTO, Felipe Peixoto. Curso de Direito Civil: Responsabilidade civil. 9 ed. atual. e amp. São Paulo: Editora Jus Podvim, 2022.

FJLKESTEIN, Maria Eugênia Reis. SACCO NETO, Fernando. Manual de direito do consumidor. Rio de Janeiro: Elsevier, 2010.

GONÇALVES, Carlos Roberto. Direito Civil Brasileiro - Responsabilidade Civil. Volume IV . São Paulo: Saraiva, 2014.

NEVES, Daniel Amorim Assumpçào; TARTUCE, Flávio. Manual de direito do consumidor: direito material e processual. 3" Ed. Rio de Janeiro: Forense; São Paulo: Método. 2014.

SOARES, Flaviana Rampazzo. Dever de cuidado e responsabilidade das instituições financeiras. Responsabilidade civil nas relações de consumo. FILHO, Carlos Edison Rego Monteiro, MARTINS, Guilherme Magalhães, ROSENVALD, Nelson e DENSA, Roberta. Iberc. Foco. 2022.

VIEIRA, Bernardo Mafia. Novas alternativas de proteção do consumidor no comércio eletrônico. JusNavigandi. Disponível em: https://jus.com.br/artigos/28716/novas-alternativas-de-protecao-do-consumidor-no-comercio-eletronic. Acesso em 10 mar 2024.