

1. INTRODUÇÃO

O ambiente digital tem se tornado cada vez mais presente na vida cotidiana, facilitando uma ampla gama de atividades, desde compras on-line até a comunicação instantânea. No entanto, essa expansão trouxe consigo uma série de desafios, especialmente no que diz respeito à segurança dos consumidores. Com o aumento do uso da internet, surgiram novas formas de fraudes virtuais, que exploram a vulnerabilidade e a confiança dos consumidores, gerando impactos significativos tanto no âmbito pessoal quanto no econômico.

A facilidade com que as transações podem ser realizadas no ambiente virtual, aliada à dificuldade de verificar a autenticidade das informações e a identidade dos fornecedores, cria um cenário propício para a ocorrência de fraudes. Esse contexto impõe ao Direito do Consumidor a necessidade de se adaptar às novas demandas e de proporcionar uma proteção efetiva aos consumidores, que frequentemente se veem desamparados diante de práticas ilícitas que muitas vezes desconhecem.

Nesse sentido, o estudo da proteção jurídica do consumidor contra fraudes virtuais é de extrema relevância, pois busca compreender como a legislação vigente, em especial o Código de Defesa do Consumidor (CDC) e o Marco Civil da Internet, pode ser aplicada para coibir essas práticas e garantir a responsabilização dos agentes que delas se beneficiam. A complexidade do ambiente virtual e a constante evolução das técnicas fraudulentas exigem uma análise aprofundada dos mecanismos de proteção disponíveis, bem como das lacunas que ainda precisam ser preenchidas no ordenamento jurídico.

O objetivo central deste artigo é investigar as principais formas de fraudes virtuais que atingem os consumidores e avaliar como a legislação brasileira tem se posicionado frente a essas questões. Ao identificar os principais riscos e vulnerabilidades a que os consumidores estão expostos, pretende-se também propor medidas jurídicas e práticas que possam ser adotadas para mitigar esses riscos e fortalecer a proteção dos direitos dos consumidores no ambiente digital.

Para alcançar esses objetivos, o artigo adotará uma abordagem metodológica que combina a revisão bibliográfica com a análise jurisprudencial. A revisão bibliográfica permitirá uma compreensão abrangente dos conceitos e das normas que regem a proteção do consumidor no Brasil, enquanto a análise de casos concretos julgados pelos tribunais fornecerá *insights* sobre

como essas normas têm sido aplicadas na prática. Esse duplo enfoque visa a proporcionar uma visão completa e crítica do tema.

A escolha desse tema se justifica pela crescente incidência de fraudes virtuais e pelos prejuízos que elas causam aos consumidores, que vão desde perdas financeiras até danos emocionais e psicológicos. Além disso, a insuficiência de informações sobre as medidas de proteção disponíveis e a falta de conscientização dos consumidores sobre os riscos envolvidos evidenciam a necessidade de um estudo aprofundado que possa contribuir para o aprimoramento das políticas de defesa do consumidor.

Outro aspecto que reforça a importância deste estudo é a constante evolução do ambiente digital, que exige uma adaptação contínua das leis e das práticas de proteção. O rápido desenvolvimento de novas tecnologias e a criação de métodos cada vez mais sofisticados de fraude colocam o Direito do Consumidor diante de desafios inéditos, demandando respostas rápidas e eficazes que possam acompanhar essa evolução.

Por fim, este artigo, através dos métodos de pesquisa qualitativa e bibliográfica, propõe não apenas identificar os problemas existentes, mas também sugerir possíveis soluções que possam ser implementadas tanto pelos legisladores quanto pelos operadores do direito e pelos próprios consumidores. A criação de um ambiente virtual mais seguro depende da colaboração de todos os envolvidos, e a disseminação de informações sobre os direitos dos consumidores e as responsabilidades dos fornecedores é um passo fundamental nesse processo.

Portanto, ao abordar a proteção do consumidor contra fraudes virtuais, este estudo pretende contribuir para o fortalecimento da confiança nas relações de consumo no ambiente digital, promovendo uma maior segurança e transparência nas transações realizadas pela internet. Com isso, espera-se que os consumidores possam exercer seus direitos de forma plena e segura, sem temer os riscos de fraudes e abusos.

2. A VULNERABILIDADE DO CONSUMIDOR NO AMBIENTE VIRTUAL

O crescimento exponencial do comércio eletrônico e das transações on-line trouxe uma série de vantagens para os consumidores, como a conveniência, a variedade de opções e a competitividade dos preços. No entanto, esse mesmo ambiente virtual, que oferece tantas

facilidades, também apresenta desafios consideráveis, especialmente em termos de segurança e proteção dos direitos dos consumidores. A vulnerabilidade do consumidor no ambiente digital é uma questão central que deve ser abordada com rigor, uma vez que envolve riscos significativos de fraudes, abusos e violações dos direitos fundamentais.

O Código de Defesa do Consumidor (CDC) estabelece que o consumidor é parte vulnerável nas relações de consumo, especialmente quando se trata de contratos celebrados em ambientes virtuais. O artigo 4º, I, do CDC, destaca a necessidade de reconhecimento da vulnerabilidade do consumidor como princípio basilar das políticas públicas de consumo, reforçando a obrigação do Estado e dos fornecedores de adotarem medidas que protejam essa parte mais fraca da relação.

Importante destacar o posicionamento de Marcos Jorge Catalan:

Todo consumidor é vulnerável, pelo menos, perante o microsistema vigente e vulnerável porque faz parte de um grupo heterogêneo e pouco coeso, e por conta disto, acaba por se sujeitar às práticas negociais impostas por fornecedores que atuam corporativamente, mesmo quando agem de modo autônomo, pois nestes casos, em regra são bastante organizados. (CATALAN, 2008, p.15).

No ambiente virtual, essa vulnerabilidade é exacerbada por uma série de fatores. A assimetria de informações, por exemplo, é um dos aspectos mais críticos. Enquanto os fornecedores, muitas vezes, possuem informações detalhadas sobre o comportamento e as preferências dos consumidores, estes, por sua vez, geralmente dispõem de informações limitadas sobre os fornecedores e sobre a qualidade dos produtos ou serviços ofertados. Essa disparidade coloca o consumidor em uma posição de desvantagem, tornando-o mais suscetível a práticas comerciais abusivas e fraudes.

Ademais, a rapidez e a impessoalidade das transações on-line contribuem para aumentar essa vulnerabilidade. Diferentemente das compras físicas, onde o consumidor pode verificar o produto antes de adquiri-lo, nas transações on-line, o comprador muitas vezes depende exclusivamente das informações fornecidas pelo vendedor. Isso abre espaço para a prática de fraudes, como a venda de produtos falsificados, a não entrega de mercadorias, ou a entrega de itens que não correspondem ao que foi anunciado.

A dificuldade de identificação dos fornecedores no ambiente virtual é outro fator que aumenta a vulnerabilidade do consumidor. Muitos sites de comércio eletrônico permitem que vendedores de diferentes partes do mundo ofereçam seus produtos sem que haja um controle rigoroso sobre a identidade e a idoneidade desses fornecedores. Isso pode levar o consumidor a realizar transações com empresas ou indivíduos fraudulentos, que muitas vezes desaparecem após o pagamento, sem entregar o produto ou serviço adquirido.

O CDC também aborda a questão da vulnerabilidade em seu artigo 6º, que lista os direitos básicos do consumidor, incluindo a proteção contra práticas comerciais desleais ou abusivas (inciso IV) e a obtenção de informações adequadas sobre os produtos e serviços oferecidos (inciso III). No ambiente virtual, garantir a transparência e a clareza das informações é um desafio constante, já que muitos fornecedores se aproveitam da dificuldade de fiscalização para omitir ou distorcer informações cruciais para a decisão de compra do consumidor.

Além do CDC, o Marco Civil da Internet (Lei nº 12.965/2014) reforça a proteção dos consumidores no ambiente digital ao estabelecer princípios, garantias e direitos relacionados ao uso da internet no Brasil. O artigo 7º do Marco Civil assegura aos usuários da internet a inviolabilidade da intimidade e da vida privada, bem como a proteção dos dados pessoais, que são frequentemente alvo de ataques cibernéticos e práticas fraudulentas. A violação desses direitos pode resultar em danos significativos para o consumidor, que podem incluir desde a utilização indevida de seus dados até fraudes financeiras de grande escala.

A vulnerabilidade do consumidor é ainda ampliada pela falta de conhecimento técnico sobre as ferramentas e os mecanismos de segurança digital. Muitos consumidores não estão familiarizados com práticas básicas de segurança, como a verificação de certificados de segurança em sites, o uso de senhas fortes, ou a necessidade de atualizar regularmente seus dispositivos para proteger-se contra *malware*. Essa falta de conhecimento técnico facilita a ação de fraudadores, que utilizam técnicas como *phishing*, engenharia social e outras formas de ataques cibernéticos para enganar os consumidores e roubar suas informações pessoais e financeiras.

Roberto Senise Lisboa sobre a vulnerabilidade do consumidor, ressalta que:

[...] pouco importa a situação econômica ou classe social do consumidor, bem como seu grau de instrução ou mesmo se a aquisição do produto ou do serviço

se deu para o exercício da atividade profissional do consumidor, ou não. A vulnerabilidade é qualidade indissociável do destinatário final do produto ou serviço [...]. É adjetivo que se encontra sempre ligado ao consumidor no sistema jurídico brasileiro, sem que qualquer ressalva tenha sido expressamente feita pelo legislador. (LISBOA, 2001, p. 86)

Outro aspecto relevante da vulnerabilidade do consumidor no ambiente virtual é a dificuldade de acesso à justiça em casos de fraudes ou disputas com fornecedores. Embora o CDC garanta o direito à reparação de danos (art. 6º, VI), na prática, muitos consumidores enfrentam obstáculos significativos para buscar a reparação de seus direitos. Isso inclui desde a dificuldade em identificar e localizar o fornecedor, especialmente quando este está localizado no exterior, até os custos e a complexidade de processar essas demandas judicialmente.

Não é por outra razão que Afrânio Carlos Moreira Thomaz afirma que:

Em nosso sentir, a vulnerabilidade do consumidor na relação de consumo é tida pelo CDC como verdadeira presunção absoluta, independentemente de sua situação econômica, social e cultural. Nesse contexto, podemos até nos deparar com situações em que a inferioridade técnica e econômica penda, excepcionalmente, para o lado do fornecedor. (THOMAZ, 2009, p.25).

A jurisprudência brasileira tem reconhecido a vulnerabilidade do consumidor no ambiente virtual, ampliando a aplicação dos princípios do CDC para abranger as transações realizadas na internet. O Superior Tribunal de Justiça (STJ) tem reiteradamente afirmado a responsabilidade objetiva dos fornecedores de produtos e serviços em casos de fraudes virtuais, reforçando a necessidade de proteção do consumidor e a aplicação rigorosa das normas de defesa do consumidor.

No entanto, apesar das proteções legais existentes, a vulnerabilidade do consumidor no ambiente virtual continua sendo uma preocupação crescente. As fraudes e as práticas comerciais desleais se adaptam rapidamente às novas tecnologias, muitas vezes ultrapassando as capacidades de fiscalização e regulação dos órgãos competentes. Isso exige uma constante atualização das normas e das práticas de defesa do consumidor, bem como uma maior cooperação internacional para combater fraudes transfronteiriças.

A responsabilidade dos fornecedores em adotar medidas de segurança adequadas é um ponto crucial na mitigação da vulnerabilidade do consumidor. De acordo com o CDC, os fornecedores devem garantir a qualidade e a segurança dos produtos e serviços oferecidos, o que inclui a

proteção contra fraudes e ataques cibernéticos. A falha em adotar medidas de segurança adequadas pode resultar na responsabilização dos fornecedores pelos danos causados aos consumidores, conforme previsto no artigo 14 do CDC.

Além das medidas de segurança, é fundamental que os fornecedores invistam em práticas de transparência e educação do consumidor. Isso inclui fornecer informações claras e acessíveis sobre os riscos associados às transações on-line e sobre as melhores práticas de segurança digital. A conscientização do consumidor sobre seus direitos e sobre como se proteger no ambiente virtual é uma ferramenta poderosa na redução de sua vulnerabilidade.

O papel das autoridades reguladoras e de fiscalização também é crucial na proteção do consumidor no ambiente virtual. Órgãos como a Secretaria Nacional do Consumidor (Senacon) e o Ministério Público têm um papel fundamental na investigação e na punição de práticas fraudulentas, bem como na promoção de políticas públicas voltadas para a segurança digital. A colaboração entre esses órgãos e as empresas de tecnologia pode resultar em soluções mais eficazes para a proteção dos consumidores.

Por fim, é importante ressaltar que a vulnerabilidade do consumidor no ambiente virtual não se limita apenas aos riscos financeiros. A exposição a práticas abusivas e a fraudes pode ter um impacto significativo na saúde emocional e psicológica dos consumidores, gerando ansiedade, estresse e desconfiança em relação ao uso da internet. Isso demonstra a importância de uma abordagem holística na proteção do consumidor, que leve em conta tanto os aspectos econômicos quanto os sociais e psicológicos.

A vulnerabilidade do consumidor no ambiente virtual é um tema complexo e multifacetado, que requer a atenção contínua de legisladores, fornecedores e autoridades de proteção ao consumidor. A legislação brasileira oferece uma base sólida para a proteção dos direitos dos consumidores, mas a eficácia dessas normas depende de sua aplicação rigorosa e da adaptação constante às novas realidades tecnológicas. A promoção de uma cultura de segurança digital e a conscientização dos consumidores são passos fundamentais para reduzir essa vulnerabilidade e garantir que o ambiente virtual seja um espaço seguro e confiável para todos.

3. FRAUDES VIRTUAIS E A LEGISLAÇÃO BRASILEIRA

As fraudes virtuais representam uma das maiores ameaças ao consumidor no ambiente digital, exigindo uma resposta jurídica eficaz e abrangente. No Brasil, a legislação consumerista, capitaneada pelo Código de Defesa do Consumidor (CDC), juntamente com normas específicas como o Marco Civil da Internet, busca oferecer uma proteção robusta aos consumidores contra essas práticas ilícitas. A resposta legislativa a essas fraudes é essencial para garantir a segurança das transações e a confiança no comércio eletrônico, elementos cruciais para o desenvolvimento sustentável do mercado digital.

O Código de Defesa do Consumidor, em seu artigo 6º, IV, assegura como direito básico do consumidor a proteção contra práticas comerciais abusivas ou fraudulentas. Essa disposição é fundamental no contexto das fraudes virtuais, onde a vulnerabilidade do consumidor é exacerbada pelas dificuldades de identificação dos agentes mal-intencionados e pela complexidade das transações realizadas em plataformas digitais. A previsão de responsabilidade objetiva dos fornecedores de produtos e serviços, conforme o artigo 14 do CDC, é um mecanismo crucial para a proteção dos consumidores, dispensando a necessidade de prova de culpa para a reparação dos danos causados por fraudes.

Além do CDC, o Marco Civil da Internet (Lei nº 12.965/2014) desempenha um papel significativo na proteção dos consumidores no ambiente digital. O artigo 7º do Marco Civil estabelece direitos fundamentais dos usuários da internet, incluindo a proteção dos seus dados pessoais e a garantia da privacidade. Esse dispositivo é de extrema importância no combate às fraudes virtuais, que muitas vezes se baseiam no uso indevido de dados pessoais coletados de forma ilícita ou por meio de engenharia social. A proteção dos dados pessoais é um dos pilares para a segurança no ambiente digital e para a prevenção de fraudes.

Thiago Ferreira Cardoso Neves, com propriedade sobre o tema, ao discorrer sobre o Marco Civil da Internet, destaca:

Uma das virtudes da Lei 12.965/2014 é a apresentação e a positivação de alguns conceitos básicos, até então de domínio exclusivo dos técnicos de informática, de modo a permitir um melhor e adequado tratamento jurídico de temas não afeitos ao meio jurídico. Com esse propósito, o art. 5º da LMC estabelece um rol de conceitos, que vão desde a própria internet, até outros mais complexos, como conexão e registro de acesso, o que revela importante

para facilitar a solução de conflitos que emanam das relações virtuais na grande rede. (NEVES, 2023, 109).

A responsabilidade dos provedores de serviços de internet, conforme prevista no Marco Civil da Internet, também é um ponto de destaque na legislação brasileira. O artigo 18 do Marco Civil determina que os provedores de conexão à internet não são responsáveis pelo conteúdo gerado por terceiros, salvo quando, após ordem judicial específica, não tomarem as providências para tornar indisponível o conteúdo infrator. No entanto, quando se trata de provedores de aplicações de internet, como plataformas de e-commerce, a responsabilidade pode ser mais direta, especialmente se houver falha na adoção de medidas de segurança adequadas para prevenir fraudes.

A Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709/2018, complementa o arcabouço jurídico de proteção contra fraudes virtuais ao estabelecer normas rigorosas para o tratamento de dados pessoais. A LGPD impõe obrigações aos controladores e operadores de dados, exigindo transparência, segurança e responsabilidade no tratamento das informações dos consumidores. A aplicação da LGPD é crucial para prevenir que dados pessoais sejam utilizados para fraudes e outras práticas ilícitas no ambiente digital, reforçando a proteção do consumidor contra violações de privacidade e segurança.

É preciso destacar, como diz Thiago Ferreira Cardoso Neves, que:

Em uma breve digressão histórica, é preciso observar que até o advento da Lei 12.965/2014 a questão revelava uma severa controvérsia, a qual era fruto, por certo, da ausência de regulação da matéria. A insegurança causada pela ausência de normatividade fazia com que a doutrina e a jurisprudência vacilassem entre a plena responsabilidade dos provedores por conteúdo postado por terceiro e a responsabilização condicionada. (NEVES, 2023, 129).

A jurisprudência brasileira tem evoluído para refletir a aplicação dessas normas em casos concretos de fraudes virtuais. O Superior Tribunal de Justiça (STJ), em diversas decisões, tem afirmado a necessidade de aplicação rigorosa das disposições do CDC e do Marco Civil da Internet, responsabilizando fornecedores e plataformas digitais por falhas na segurança que resultem em fraudes contra os consumidores. Essas decisões são fundamentais para consolidar a proteção jurídica do consumidor e para estabelecer precedentes que orientem a aplicação das leis no ambiente digital.

No entanto, apesar do robusto arcabouço legal, a prática demonstra que ainda existem desafios significativos na aplicação dessas normas. A rápida evolução das tecnologias e das técnicas de fraude exige uma constante atualização das leis e das práticas de fiscalização. A cooperação entre os diferentes órgãos de proteção ao consumidor, como a Secretaria Nacional do Consumidor (Senacon) e os Procons, bem como a integração com as autoridades de segurança pública, é essencial para uma resposta eficaz às fraudes virtuais.

Além disso, a conscientização dos consumidores sobre seus direitos e sobre as medidas de segurança que podem adotar é uma estratégia importante na prevenção de fraudes. A educação digital e a promoção de práticas seguras no uso da internet devem ser incentivadas, não apenas pelos órgãos governamentais, mas também pelos próprios fornecedores e plataformas digitais, que têm o dever de zelar pela segurança dos seus clientes.

Por certo, a legislação brasileira, através do CDC, do Marco Civil da Internet e da LGPD, oferece uma base sólida para a proteção dos consumidores contra fraudes virtuais. No entanto, a eficácia dessas normas depende da sua aplicação rigorosa e da adaptação constante às novas realidades do ambiente digital. O fortalecimento das práticas de segurança, a responsabilização dos agentes envolvidos e a conscientização dos consumidores são elementos chave para a construção de um ambiente digital mais seguro e confiável.

4. OS 5 PRINCIPAIS GOLPES VIRTUAIS QUE OS CONSUMIDORES COMUMENTE SÃO VÍTIMAS

No cenário atual da exposição dos consumidores ao ambiente virtual, sem dúvidas, é possível elencar diversas práticas abusivas e indutivas de golpe e fraudes praticadas contra os consumidores, que impõem um verdadeiro estado de alerta dos agentes envolvidos no sistema de proteção dos consumidores. Aqui vamos destacar apenas 5 dos principais golpes virtuais que os consumidores comumente são vítimas.

4.1 *Phishing*

Phishing é uma das técnicas de fraude virtual mais comuns e perigosas, que tem como objetivo roubar informações pessoais e financeiras dos consumidores. Os golpistas enviam e-mails, mensagens de texto ou comunicados em redes sociais que parecem ser de fontes confiáveis,

como bancos, empresas de cartões de crédito, ou plataformas de e-commerce. Essas mensagens geralmente contêm links que direcionam o usuário a sites falsos, que são réplicas quase perfeitas de páginas legítimas. Ao inserir suas credenciais de login, números de cartão de crédito, ou outras informações pessoais nesses sites, o consumidor acaba entregando esses dados aos golpistas.

O Código de Defesa do Consumidor (CDC) protege o consumidor contra práticas abusivas, incluindo aquelas que envolvem a captação fraudulenta de informações pessoais. O artigo 6º, III, do CDC garante ao consumidor o direito à informação clara e precisa sobre os produtos e serviços, o que também se aplica ao contexto virtual. No entanto, o *Phishing* explora a confiança do consumidor, apresentando informações falsas de maneira convincente, o que dificulta a identificação do golpe. As empresas que são alvos frequentes de *Phishing* têm a responsabilidade de informar seus clientes sobre os riscos e educá-los sobre como identificar e evitar essas fraudes.

O Marco Civil da Internet também desempenha um papel importante na proteção contra *Phishing*, ao estabelecer diretrizes sobre a segurança da informação e a privacidade dos dados pessoais. A responsabilidade dos provedores de serviços de internet em remover conteúdos fraudulentos, após notificação, ajuda a mitigar os danos causados por essas práticas. No entanto, a prevenção do *Phishing* depende fortemente da conscientização dos consumidores e da adoção de práticas de segurança, como verificar o endereço de e-mail do remetente e nunca clicar em links suspeitos.

A Lei Geral de Proteção de Dados (LGPD) também impõe obrigações rigorosas às empresas no tratamento dos dados pessoais, incluindo a exigência de que implementem medidas de segurança para proteger essas informações contra acessos não autorizados. Em casos de *Phishing*, as empresas que lidam com dados pessoais têm a obrigação de adotar medidas preventivas para evitar que suas plataformas sejam usadas como vetores de ataques. Isso inclui a implementação de autenticação de dois fatores e outras medidas de segurança cibernética para proteger as contas dos usuários.

4.2 Roubo de identidade

O roubo de identidade é uma das formas mais graves de fraude virtual, onde os golpistas obtêm acesso a informações pessoais do consumidor, como números de CPF, RG, dados bancários e outras informações sensíveis, e as utilizam para abrir contas bancárias, solicitar cartões de crédito, realizar compras ou até mesmo cometer crimes em nome da vítima. Este tipo de golpe pode ter consequências devastadoras, tanto financeiras quanto pessoais, para o consumidor, que pode passar anos tentando restaurar sua reputação e corrigir os danos causados.

A legislação brasileira, especialmente o CDC, oferece proteção contra o roubo de identidade ao estabelecer que o fornecedor é responsável pela segurança das informações pessoais dos consumidores. A responsabilidade objetiva prevista no artigo 14 do CDC implica que o fornecedor deve adotar todas as medidas necessárias para evitar o roubo de identidade, incluindo o uso de tecnologias de segurança avançadas e a realização de auditorias regulares de segurança. A falha em proteger essas informações pode resultar em sanções legais e na obrigação de indenizar o consumidor pelos danos sofridos.

Além do CDC, a LGPD desempenha um papel crucial na proteção contra o roubo de identidade, ao impor regras rigorosas sobre o tratamento de dados pessoais. A LGPD exige que as empresas adotem medidas técnicas e administrativas para proteger os dados pessoais contra acessos não autorizados, e prevê penalidades severas para as empresas que falharem em cumprir essas obrigações. Isso inclui multas e a possibilidade de proibição do tratamento de dados, o que pode ter um impacto significativo sobre as operações das empresas.

A recuperação do roubo de identidade é um processo complexo e demorado para o consumidor, que precisa lidar com instituições financeiras, empresas de crédito, e muitas vezes, com autoridades policiais. As empresas que lidam com dados pessoais devem estar preparadas para oferecer suporte ao consumidor nesse processo, facilitando a correção de dados e a contestação de operações fraudulentas. Além disso, é essencial que os consumidores sejam informados sobre os sinais de alerta de roubo de identidade e as medidas que podem tomar para se proteger, como monitorar regularmente suas contas e relatórios de crédito.

4.3 Golpes de compras on-line

Os golpes de compras on-line são uma das fraudes virtuais mais comuns, especialmente em um mercado digital cada vez mais dinâmico. Esses golpes ocorrem quando consumidores compram produtos em sites fraudulentos ou de vendedores inescrupulosos, mas nunca recebem os itens adquiridos, ou recebem produtos falsificados ou de qualidade inferior à anunciada. Em muitos casos, os sites fraudulentos imitam plataformas de comércio eletrônico legítimas, utilizando fotos e descrições detalhadas para enganar os consumidores. Outro aspecto deste golpe é o uso de falsas promoções e ofertas irresistíveis para atrair vítimas.

O CDC garante ao consumidor o direito à reparação dos danos causados por práticas comerciais enganosas ou abusivas, conforme o disposto nos artigos 18 e 20. A responsabilidade pelos produtos oferecidos, inclusive nas plataformas digitais, recai sobre o fornecedor que, ao enganar o consumidor, viola os princípios da boa-fé e da transparência, previstos no artigo 4º do CDC. A legislação brasileira, portanto, assegura que o consumidor que for vítima de golpes de compras on-line tem o direito de buscar a devolução dos valores pagos ou a substituição do produto, além de reparação por danos morais e materiais.

Além do CDC, o Marco Civil da Internet exige que as plataformas de e-commerce adotem medidas para garantir a segurança das transações realizadas em seus sites. Isso inclui a verificação da identidade dos vendedores e a implementação de sistemas de avaliação que permitam aos consumidores identificar vendedores confiáveis. O Marco Civil também prevê que as plataformas podem ser responsabilizadas se, após notificação, não tomarem as medidas adequadas para remover conteúdos ou vendedores fraudulentos de seus sistemas.

A prevenção dos golpes de compras online depende tanto da ação dos fornecedores quanto da conscientização dos consumidores. Os consumidores devem ser encorajados a verificar a autenticidade dos sites antes de realizar compras, buscar referências de outros clientes e desconfiar de ofertas que parecem boas demais para ser verdade. As empresas, por sua vez, devem investir em segurança cibernética e em mecanismos que permitam a rápida identificação e remoção de vendedores fraudulentos. A cooperação entre consumidores, fornecedores e autoridades é essencial para a criação de um ambiente de compras online mais seguro.

4.4 Falsos suportes técnicos

Os golpes de falsos suportes técnicos são uma forma de fraude onde os golpistas fingem ser representantes de empresas de tecnologia, como de provedores de internet, oferecendo suporte técnico para resolver problemas inexistentes no dispositivo do consumidor. Esse tipo de golpe geralmente começa com uma chamada telefônica ou uma mensagem *pop-up* que alerta o consumidor sobre um suposto problema grave, como um vírus ou falha de segurança. Os golpistas, então, convencem o consumidor a pagar por serviços falsos ou a conceder acesso remoto ao seu computador, o que permite a instalação de malware ou o roubo de informações pessoais.

O CDC, ao garantir a proteção do consumidor contra práticas abusivas e enganosas, também se aplica aos casos de falsos suportes técnicos. O artigo 6º, IV, do CDC, protege o consumidor contra coação e engano, que são características comuns nesses golpes. Além disso, o artigo 39 do CDC proíbe práticas abusivas que coloquem o consumidor em desvantagem, incluindo a indução ao erro sobre a necessidade de serviços desnecessários ou inexistentes.

O Marco Civil da Internet, ao assegurar a privacidade e a proteção dos dados pessoais, também oferece uma base para responsabilizar os golpistas e proteger os consumidores. Empresas que lidam com dados pessoais e oferecem serviços de suporte técnico legítimos têm a obrigação de educar seus clientes sobre como identificar e evitar esses golpes. A prevenção é crucial, e as empresas devem se esforçar para garantir que seus canais de suporte sejam claramente identificáveis e que os consumidores saibam que não devem conceder acesso remoto a seus dispositivos a terceiros sem verificação adequada.

Para se proteger contra esses golpes, os consumidores devem estar cientes de que as empresas legítimas raramente entram em contato de forma proativa para resolver problemas técnicos, especialmente por telefone. É importante que os consumidores verifiquem a identidade do contato, evitem fornecer informações pessoais ou financeiras por telefone e nunca concedam acesso remoto a seus dispositivos a menos que tenham certeza da legitimidade do suporte. As empresas, por sua vez, devem fornecer canais seguros de suporte e promover a conscientização dos consumidores sobre os riscos associados a falsos suportes técnicos.

4.5 Golpe do boleto falso

O golpe do boleto falso é uma prática fraudulenta em que os golpistas geram boletos de pagamento que parecem legítimos, mas direcionam os pagamentos para contas de terceiros, em vez de para o fornecedor ou credor correto. Esse golpe pode ocorrer de várias maneiras: os criminosos podem enviar boletos falsos por e-mail, modificar boletos legítimos com softwares específicos ou até mesmo criar sites falsos de geração de boletos. O consumidor, ao pagar o boleto, acredita estar quitando uma dívida ou fazendo uma compra, mas o valor é desviado para a conta do golpista.

O CDC assegura ao consumidor o direito à informação adequada e clara, conforme o artigo 6º, III, e à proteção contra práticas enganosas, conforme o artigo 6º, IV. No caso do golpe do boleto falso, esses direitos são violados, uma vez que o consumidor é enganado por um documento que aparenta ser legítimo. O artigo 39 do CDC, que proíbe práticas abusivas, também é aplicável, pois os golpistas exploram a confiança do consumidor para obter vantagem indevida.

As empresas que emitem boletos devem adotar medidas rigorosas para proteger seus clientes contra esse tipo de fraude. Isso inclui a implementação de sistemas de verificação que permitam aos consumidores confirmar a autenticidade dos boletos antes de efetuar o pagamento. Além disso, a comunicação com os consumidores deve ser clara, orientando-os sobre os riscos e sobre como identificar possíveis fraudes. O Marco Civil da Internet e a LGPD também impõem às empresas a obrigação de proteger os dados pessoais dos consumidores e de tomar medidas contra a disseminação de boletos falsos em suas plataformas.

Para se proteger contra o golpe do boleto falso, os consumidores devem verificar cuidadosamente os dados do boleto, como o nome do beneficiário, o código de barras e o número do documento. Sempre que possível, é aconselhável pagar boletos diretamente nos sites dos fornecedores ou utilizar aplicativos de bancos que oferecem verificação automática de boletos. As empresas devem continuar a educar seus clientes sobre os riscos e fornecer ferramentas que ajudem a verificar a autenticidade dos documentos de pagamento, contribuindo para a redução dessa prática fraudulenta.

5. MEDIDAS PREVENTIVAS E REPRESSIVAS

O combate às fraudes virtuais e à proteção do consumidor no ambiente digital requer uma abordagem abrangente que combine medidas preventivas e repressivas. Essas medidas não apenas ajudam a evitar que os consumidores se tornem vítimas de fraudes, mas também garantem que, quando as fraudes ocorrem, os responsáveis sejam devidamente punidos e os consumidores, indenizados. A legislação brasileira, especialmente o Código de Defesa do Consumidor (CDC), juntamente com normas complementares, oferece uma estrutura legal sólida para a implementação dessas medidas, mas sua eficácia depende de uma aplicação rigorosa e de uma cooperação estreita entre todas as partes envolvidas.

No âmbito das medidas preventivas, a educação do consumidor é um elemento fundamental. Conforme estabelece o artigo 4º, IV, do CDC, a educação e a informação dos consumidores sobre seus direitos são essenciais para que eles possam fazer escolhas conscientes e seguras. Isso inclui a conscientização sobre os riscos associados ao ambiente digital, como a identificação de golpes virtuais e a adoção de práticas de segurança, como a utilização de autenticação de dois fatores, a verificação da autenticidade dos sites antes de realizar transações e a proteção dos dados pessoais. A educação do consumidor deve ser uma prioridade tanto para o Estado quanto para os fornecedores de produtos e serviços digitais.

As empresas que operam no ambiente virtual têm uma responsabilidade significativa na prevenção de fraudes. O CDC, em seu artigo 6º, III, garante ao consumidor o direito à informação clara e adequada, o que implica que os fornecedores devem fornecer informações precisas sobre os riscos de fraudes e sobre as medidas que estão tomando para proteger seus clientes. Além disso, o artigo 14 do CDC estabelece a responsabilidade objetiva dos fornecedores por danos causados ao consumidor, o que inclui a obrigação de adotar medidas de segurança adequadas para prevenir fraudes. Empresas que falham em implementar práticas de segurança robustas podem ser responsabilizadas por danos resultantes de fraudes.

A implementação de tecnologias de segurança é uma medida preventiva crucial. Provedores de serviços de internet e plataformas de e-commerce devem adotar soluções avançadas, como criptografia de dados, sistemas de detecção de fraudes e autenticação forte. O Marco Civil da Internet (Lei nº 12.965/2014) complementa essa obrigação ao estabelecer que os provedores de aplicações de internet devem garantir a proteção dos dados pessoais dos usuários e adotar

medidas para mitigar riscos. A falha em proteger os dados dos consumidores pode resultar em penalidades significativas, especialmente sob a Lei Geral de Proteção de Dados (LGPD), que impõe multas severas para violações de segurança.

Além das tecnologias de segurança, as empresas devem implementar políticas internas de prevenção a fraudes. Isso inclui a realização de auditorias regulares de segurança, a capacitação de funcionários para reconhecer e responder a atividades fraudulentas e a criação de canais de comunicação seguros para que os consumidores possam relatar suspeitas de fraudes. O CDC, ao garantir o direito do consumidor à proteção contra práticas abusivas e fraudulentas, reforça a importância dessas medidas preventivas no ambiente digital.

No que tange às medidas repressivas, o CDC, em seu artigo 56, prevê uma série de sanções administrativas que podem ser aplicadas contra fornecedores que violem os direitos do consumidor, incluindo multas, suspensão de atividades e, em casos mais graves, a cassação do alvará de funcionamento. Essas medidas são essenciais para garantir que as empresas que não cumprem suas obrigações de proteção ao consumidor sejam devidamente punidas. Além disso, o artigo 18 do Marco Civil da Internet estabelece que os provedores de aplicação podem ser responsabilizados civilmente por danos causados por conteúdos gerados por terceiros, caso não cumpram ordens judiciais para remoção de tais conteúdos.

O CDC estabeleceu a responsabilidade objetiva, como regra do sistema, como bem asseverado por Sérgio Cavalieri Filho:

[...] a responsabilidade estabelecida no CDC é objetiva, fundada no *dever e segurança* do fornecedor em relação aos produtos e serviços lançados no mercado de consumo, razão pela qual não seria também demasiado afirmar que, a partir dele, a responsabilidade objetiva, que era exceção em nosso Direito, passou a ter um campo de incidência mais vasto do que a própria responsabilidade subjetiva (CAVALIERI FILHO, 2003, p. 39, *grifos do autor*).

A cooperação entre diferentes órgãos e entidades é fundamental para a eficácia das medidas repressivas. A atuação conjunta da Secretaria Nacional do Consumidor (Senacon), dos Procons estaduais e municipais, do Ministério Público e das autoridades de segurança pública é crucial para a investigação e a punição de fraudes virtuais. Essa colaboração deve ser fortalecida por meio de acordos de cooperação, que permitam a troca de informações e a coordenação de ações para combater as fraudes de forma mais eficaz.

A repressão às fraudes virtuais também exige uma adaptação constante da legislação às novas realidades tecnológicas. O rápido avanço das tecnologias e das técnicas de fraude requer que o legislador esteja atento às mudanças e disposto a atualizar as normas para enfrentar novos desafios. Isso inclui a criação de novas tipificações penais para condutas específicas no ambiente digital e o fortalecimento dos mecanismos de cooperação internacional, uma vez que muitas fraudes virtuais envolvem atores localizados em diferentes países.

Além das sanções administrativas e civis, a legislação penal também tem um papel importante nas medidas repressivas contra fraudes virtuais. O Código Penal Brasileiro, em seus artigos 171 (estelionato) e 298 (falsificação de documento), pode ser aplicado em casos de fraudes virtuais, prevendo penas de reclusão e multa para os infratores. A aplicação dessas penas é fundamental para desincentivar a prática de fraudes e para proteger os consumidores.

A reparação dos danos causados ao consumidor é uma medida repressiva que também deve ser destacada. O CDC garante ao consumidor o direito à reparação integral dos danos causados por práticas fraudulentas, incluindo danos materiais e morais. A responsabilidade dos fornecedores por fraudes que ocorrem em suas plataformas deve ser aplicada de forma rigorosa, assegurando que os consumidores lesados sejam compensados adequadamente e que as empresas sejam incentivadas a adotar medidas preventivas mais eficazes.

O CDC instituiu como regra do sistema consumerista a responsabilidade objetiva e solidária. Desta forma, quando interpretamos conjuntamente os artigos 7º, parágrafo único com o § 1º do artigo 25, visualizamos a referida regra. Neste particular, relevante a transcrição dos dispositivos em comento:

Art. 7º - Os direitos previstos neste código não excluem outros decorrentes de tratados ou convenções internacionais de que o Brasil seja signatário, da legislação interna ordinária, de regulamentos expedidos pelas autoridades administrativas competentes, bem como dos que derivem dos princípios gerais do direito, analogia, costumes e equidade.

Parágrafo único. Tendo mais de um autor a ofensa, todos responderão solidariamente pela reparação dos danos previstos nas normas de consumo.

Art. 25 - É vedada a estipulação contratual de cláusula que impossibilite, exonere ou atenua a obrigação de indenizar prevista nesta e nas seções anteriores.

§ 1º Havendo mais de um responsável pela causação do dano, todos responderão solidariamente pela reparação prevista nesta e nas seções anteriores.

A responsabilidade civil das empresas no ambiente digital é amplamente respaldada pela jurisprudência brasileira, que tem consolidado o entendimento de que os fornecedores de produtos e serviços digitais devem garantir a segurança dos consumidores em suas plataformas. O Superior Tribunal de Justiça (STJ) tem reiteradamente afirmado a aplicação do CDC e do Marco Civil da Internet em casos de fraudes virtuais, reforçando a necessidade de proteção do consumidor e a aplicação rigorosa das normas de defesa do consumidor.

Por fim, é importante destacar a necessidade de um monitoramento contínuo das práticas de mercado e das tecnologias emergentes para identificar novos riscos e fraudes potenciais. A criação de grupos de trabalho e comissões especiais dentro dos órgãos de proteção ao consumidor pode contribuir para a identificação precoce de tendências fraudulentas e para o desenvolvimento de estratégias de combate mais eficazes. A prevenção e a repressão às fraudes virtuais dependem de uma abordagem proativa e de uma vigilância constante por parte de todos os atores envolvidos.

Por certo, as medidas preventivas e repressivas são complementares e essenciais para a proteção do consumidor contra fraudes virtuais. A legislação brasileira, representada pelo CDC, pelo Marco Civil da Internet e pela LGPD, oferece uma base sólida para essas medidas, mas sua eficácia depende de uma aplicação rigorosa, de uma cooperação eficaz entre diferentes órgãos e da adaptação constante às novas realidades tecnológicas.

6. CONCLUSÃO

O ambiente digital, com todas as suas facilidades e inovações, traz consigo desafios significativos para a proteção dos consumidores, que se encontram cada vez mais vulneráveis a uma série de fraudes virtuais. Este artigo se propôs a investigar a extensão dessa vulnerabilidade e a eficácia das medidas legislativas e práticas adotadas para proteger os consumidores nesse contexto. Ao longo do estudo, ficou evidente que, apesar de existir um robusto arcabouço jurídico no Brasil, representado principalmente pelo Código de Defesa do Consumidor (CDC), pelo Marco Civil da Internet e pela Lei Geral de Proteção de Dados (LGPD), a realidade prática ainda impõe desafios consideráveis.

No capítulo que abordou a vulnerabilidade do consumidor no ambiente virtual, constatou-se que a assimetria de informações, a rapidez das transações e a dificuldade de identificar fornecedores são fatores que exacerbam essa vulnerabilidade. O consumidor, frequentemente, se vê desprotegido diante da complexidade das transações digitais e da sofisticação das fraudes, o que reforça a necessidade de uma proteção jurídica mais ativa e de uma educação contínua para que possa se defender nesses ambientes.

Ao analisar os principais golpes virtuais que vitimam os consumidores, o artigo identificou fraudes como o *Phishing*, o roubo de identidade, e os golpes de compras on-line, entre outros, como as principais ameaças. Cada uma dessas fraudes explora uma fraqueza específica do consumidor e do sistema de proteção existente, demonstrando que, embora as ferramentas jurídicas estejam disponíveis, a prevenção e a conscientização são fundamentais para mitigar os riscos. As empresas, por sua vez, têm um papel essencial na implementação de medidas de segurança e na garantia de transparência nas transações.

A análise das fraudes virtuais em relação à legislação brasileira demonstrou que o CDC e o Marco Civil da Internet oferecem uma base legal sólida para a proteção dos consumidores, mas a eficácia dessas leis depende de sua aplicação prática e da adaptação às novas formas de fraudes que surgem com a evolução tecnológica.

O estudo também destacou a importância de medidas preventivas e repressivas no combate às fraudes virtuais. A prevenção, baseada na educação do consumidor e na adoção de tecnologias de segurança por parte das empresas, é crucial para evitar que fraudes aconteçam. Já as medidas repressivas, como as sanções administrativas e civis previstas no CDC, são fundamentais para garantir que os responsáveis por fraudes sejam punidos e que os consumidores lesados sejam adequadamente indenizados. A cooperação entre diferentes órgãos e a adaptação constante das normas são essenciais para enfrentar os desafios impostos pelas fraudes digitais.

Com base na análise realizada, é possível concluir que a proteção do consumidor no ambiente virtual é um desafio contínuo que exige a combinação de esforços legislativos, judiciais, empresariais e educativos. A legislação existente oferece um bom ponto de partida, mas é necessário que ela seja constantemente atualizada e que sua aplicação seja rigorosa para acompanhar as rápidas mudanças no ambiente digital. As empresas têm um papel fundamental

na proteção dos consumidores, devendo investir em segurança e em práticas transparentes, enquanto os consumidores precisam ser educados sobre os riscos e sobre como se proteger.

Por fim, é importante ressaltar que a confiança do consumidor no ambiente digital é um dos pilares para o desenvolvimento sustentável do comércio eletrônico e das transações online. A proteção jurídica, aliada a práticas empresariais responsáveis e a uma educação digital eficaz, é fundamental para garantir que essa confiança seja mantida e que o ambiente digital continue a ser um espaço de inovação e crescimento, beneficiando tanto consumidores quanto fornecedores.

REFERÊNCIAS BIBLIOGRÁFICAS

BRASIL. Lei Nº 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. Brasília, DF: Diário Oficial da União, 1990.

BRASIL. Lei Nº 12.965, de 2014. Dispõe sobre o Marco Civil da Internet, DF: Diário Oficial da União, 2014.

BRASIL. Lei Nº 13.709, de 2018. Dispõe sobre a Lei Geral de Proteção de Dados (LGPD) e dá outras providências. Brasília, DF: Diário Oficial da União, 2018.

CATALAN, Marcos Jorge. **Brasil: a hermenêutica contratual no Código de Defesa do Consumidor.** In Revista electrónica de Derecho del Consumo y de la Alimentación nº 19 (2008). Disponível em < <http://aibadaredeco.googlepages.com/ex01aiba.pdf>. > Acesso em 08.maio.2009, p. 15.

CAVALIERI FILHO, Sérgio. **Programa de Responsabilidade Civil.** 5ª ed. São Paulo: Malheiros, 2003.

DINIZ, Maria Helena. **Curso de direito civil brasileiro,** 7º volume: responsabilidade civil. 22 ed. Ver. Atual. e ampl. de acordo com a reforma do CPC e com o projeto de lei n. 276/2007. São Paulo: Saraiva, 2008.

GONÇALVES, Carlos Roberto. **Responsabilidade Civil.** 8ª ed. São Paulo: Saraiva. 2003.

LISBOA, Roberto Senise. Responsabilidade civil nas relações de consumo. São Paulo: Revista dos Tribunais, 2001.

NUNES, Luiz Antônio Rizzatto. **Curso de direito do consumidor.** São Paulo: Saraiva, 2004.

NEVES, Thiago Ferreira Cardoso. **Responsabilidade civil dos provedores de internet;** in Manual de Direito na Era Digital: Foco; São Paulo, 2023.

THOMAZ, Afrânio Carlos Moreira. Lições de direito do consumidor. Rio de Janeiro: Lumen Juris, 2009.