



PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS
ESCOLA DE DIREITO, NEGÓCIOS E COMUNICAÇÃO
NÚCLEO DE PRÁTICA JURÍDICA
COORDENAÇÃO ADJUNTA DE TRABALHO DE CURSO
ARTIGO CIENTÍFICO

**O COMÉRCIO ELETRÔNICO E O DIREITO DO CONSUMIDOR
O ACESSO À INFORMAÇÃO E À PROTEÇÃO DE DADOS PESSOAIS**

ORIENTANDO – ABNER AUGUSTO NASCIMENTO DE JESUS
ORIENTADORA: PROFA. MA. TATIANA DE OLIVEIRA TAKEDA

GOIÂNIA-GO

2025

ABNER AUGUSTO NASCIMENTO DE JESUS

O COMÉRCIO ELETRÔNICO E O DIREITO DO CONSUMIDOR
O ACESSO À INFORMAÇÃO E À PROTEÇÃO DE DADOS PESSOAIS

Artigo Científico apresentado à disciplina de Trabalho de Curso II, da Escola de Direito, Negócios e Comunicação da Pontifícia Universidade Católica de Goiás. Prof^a. Orientadora: Ma. Tatiana de Oliveira Takeda.

GOIÂNIA-GO

2025

ABNER AUGUSTO NASCIMENTO DE JESUS

**O COMÉRCIO ELETRÔNICO E O DIREITO DO CONSUMIDOR
O ACESSO À INFORMAÇÃO E À PROTEÇÃO DE DADOS PESSOAIS**

Data da Defesa: ____ de maio de 2025.

BANCA EXAMINADORA

Orientadora: Profa: Ma. Tatiana de Oliveira Takeda

Nota

Examinadora Convidada: Profa. Ma. Neire Divina Mendonça

Nota

SUMÁRIO

RESUMO.....	5
INTRODUÇÃO.....	6
1 O COMÉRCIO ELETRÔNICO E O CONSUMIDOR.....	7
1.1 A DEFINIÇÃO DE COMÉRCIO ELETRÔNICO.....	7
1.2 AS CARACTERÍSTICAS E OS DESAFIOS DA VIRTUALIDADE.....	8
1.2.1 Características da Virtualidade.....	8
1.2.2 Desafios da Virtualidade.....	8
1.3 O DIREITO DO CONSUMIDOR NO CONTEXTO VIRTUAL.....	9
1.3.1 A Constituição Federal de 1988.....	10
1.3.2 O Código de Defesa do Consumidor.....	11
1.3.2.1 <i>Princípio da Vulnerabilidade do Consumidor</i>	12
2 A PROTEÇÃO DOS DADOS PESSOAIS NO COMÉRCIO ELETRÔNICO.....	13
2.1 A CAPACITAÇÃO DO CONSUMIDOR PARA UM <i>E-COMMERCE</i> SEGURO.....	13
2.2 OS DADOS PESSOAIS E A SUA IMPORTÂNCIA NO COMÉRCIO DIGITAL.....	14
2.3 OS RISCOS NO TRATAMENTO INADEQUADO DOS DADOS.....	15
2.4 A LEI GERAL DE PROTEÇÃO DE DADOS (LGPD).....	16
2.5 A RESPONSABILIDADE DAS EMPRESAS NA PROTEÇÃO DE DADOS PESSOAIS.....	17
2.6 AS DECISÕES DOS TRIBUNAIS SUPERIORES.....	18
3 O CENÁRIO CONTEMPORÂNEO CORRELACIONADO AOS DESAFIOS CONSUMERISTAS.....	22
3.1 NOVAS REGULAMENTAÇÕES E TECNOLOGIAS QUE IMPACTAM A SEGURANÇA DE DADOS PESSOAIS DOS CONSUMIDORES.....	22
3.2 FISCALIZAÇÃO.....	23
CONCLUSÃO.....	24
REFERÊNCIAS.....	25

O COMÉRCIO ELETRÔNICO E O DIREITO DO CONSUMIDOR O ACESSO À INFORMAÇÃO E À PROTEÇÃO DE DADOS PESSOAIS

Abner Augusto Nascimento de Jesus¹

RESUMO

O estudo abordou a temática do comércio eletrônico e a proteção dos direitos do consumidor, com ênfase no acesso à informação, na segurança dos dados pessoais e nos desafios enfrentados pelos consumidores no ambiente virtual. Para a confecção do presente estudo, utilizou-se o método indutivo, em razão da observação de casos concretos para produção das constatações apresentadas, bem como foi empreendida a pesquisa bibliográfica que abordou normas, julgados e doutrinas fundamentais na compreensão do objeto eleito. Os resultados baseados no desenvolvimento empreendido demonstraram a necessidade de um arcabouço jurídico atualizado e eficaz, que acompanhe as transformações do mercado digital e garanta a proteção dos direitos dos consumidores, bem como da importância do investimento em educação digital para os consumidores e a adoção de posturas proativas pelas empresas na proteção de dados.

Palavras-chave: Comércio Eletrônico; Direito do Consumidor; Proteção; Dados Pessoais; Acesso; Informação.

ELECTRONIC COMMERCE AND CONSUMER LAW

ACCESS TO INFORMATION AND PROTECTION OF PERSONAL DATA

ABSTRACT

The study addressed the theme of electronic commerce and the protection of consumer rights, with an emphasis on access to information, the security of personal data and the challenges faced by consumers in the virtual environment. The inductive method was used to prepare this study, based on the observation of specific cases to produce the findings presented, as well as bibliographical research that addressed fundamental norms, judgments and doctrines in the understanding of the chosen object. The results based on the development undertaken demonstrated the need for an updated and effective legal framework that keeps up with the transformations of the digital market and guarantees the protection of consumer rights, as well as the importance of investing in digital education for consumers and the adoption of proactive stances by companies in data protection.

Keywords: *Electronic Commerce; Consumer Law; Protection; Personal Data; Access; Information.*

¹ Acadêmico do Curso de Direito da PUC Goiás. Email: 20211000101890@pucgo.edu.br

INTRODUÇÃO

O estudo disporá sobre a temática do comércio eletrônico e a proteção dos direitos do consumidor com ênfase no acesso à informação e na segurança dos dados pessoais.

A evolução do *e-commerce* no Brasil, seus impactos na economia e os desafios enfrentados pelos consumidores no ambiente virtual justificam o estudo empreendido, considerando a crescente presença do comércio eletrônico na economia brasileira e a necessidade de se garantir a proteção dos consumidores em ambientes que podem apresentar riscos financeiros, sociais e econômicos.

O trabalho busca demonstrar como o ordenamento jurídico brasileiro, em especial o Código de Defesa do Consumidor e a Lei Geral de Proteção de Dados, tem se adaptado para garantir a proteção dos consumidores no ambiente virtual. Além disso, o estudo visa demonstrar os desafios enfrentados pelos consumidores no *e-commerce* e as medidas que podem ser adotadas para mitigar os riscos.

Este trabalho tem como principal caracter demonstrar o cenário contemporâneo do comércio eletrônico, a proteção dos dados dos consumidores que utilizam este tipo de comércio e qual o amparo da lei na proteção dos consumidores, o qual busca apresentar e analisar a legislação, a jurisprudência e as práticas relacionadas à proteção do consumidor no comércio eletrônico.

O método indutivo somado à pesquisa bibliográfica, incluindo-se doutrinas, artigos acadêmicos, normas legislativas e decisões judiciais propiciam a possibilidade de análise e reflexão crítica sobre um tema contemporâneo que gera dúvidas e não é acessível à maioria da população brasileira.

A Seção 1 discorrerá sobre a definição e as características do comércio eletrônico, bem como os desafios enfrentados pelos consumidores no ambiente virtual.

Por sua vez, a Seção 2 discorrerá acerca da proteção de dados pessoais no comércio eletrônico, abordando a legislação aplicável, os riscos envolvidos e as medidas de segurança que podem ser adotadas.

Por fim, a Seção 3 demonstrará a aplicabilidade do Código de Defesa do Consumidor (CDC) no comércio eletrônico, analisando a responsabilidade civil dos

fornecedores e os direitos dos consumidores em caso de descumprimento do contrato.

1. O COMÉRCIO ELETRÔNICO E O CONSUMIDOR

1.1 – A DEFINIÇÃO DE COMÉRCIO ELETRÔNICO

O comércio eletrônico ou *e-commerce* é uma modalidade de compra e venda de produtos e serviço, modalidade esta que revolucionou o mercado mundial com a possibilidade de comprar qualquer produto com um simples clique. A comodidade de comprar produtos, contratar um curso ou um prestador de serviços, tudo isso sem sair de casa. Tal modalidade de compra surgiu nos Estados Unidos, no final da década de 1960. A sua origem está relacionada com a utilização do *Electronic Data Interchange (EDI)*, ou Intercâmbio Eletrônico de Dados, por companhias de telefone e internet para compartilhar arquivos e documentos de negócios.

No Brasil, o *e-commerce* começou a ser desenvolvido na década de 1990, com a chegada da internet. A primeira loja virtual brasileira foi a *Booknet*, criada em 1995 por Jack London. Em 1998, a *GP Investments* comprou a *Booknet* e a reinaugurou com o nome Submarino.

A popularização dos *smartphones* e *tablets* em meados de 2010 ajudou o comércio eletrônico a crescer ainda mais. Atualmente, o *e-commerce* é uma das principais formas de compra e venda de produtos em todo o mundo.

Percebe-se o quanto o comércio eletrônico tem se expandido, mostrando seu potencial de gerar lucros para as empresas e valor para os consumidores. Porém, mesmo com essa perspectiva, a literatura mostra que ainda existem consumidores que não são adeptos às compras eletrônicas. Com o desenvolvimento desta modalidade de compras, emergiram também alguns riscos para o consumidor, um fator desfavorável, pois a segurança é tida como um aspecto de grande preocupação dos clientes (Azevedo; Coelho, 2014).

Com isso, as empresas possuem um grande desafio, demonstrar aos consumidores a confiança da compra *online*, em meio a uma internet repleta de golpes e produtos com qualidade questionáveis.

1.2 AS CARACTERÍSTICAS E OS DESAFIOS DA VIRTUALIDADE

A virtualidade, amplamente discutida no campo da filosofia da tecnologia e da cibernética, refere-se à existência e à interação em ambientes digitais que transcendem o físico. A partir da digitalização e da internet, a virtualidade passou a ter uma influência crescente na vida cotidiana, impactando desde o comércio eletrônico até as relações sociais.

Em seu contexto mais amplo, a virtualidade refere-se à criação de ambientes e interações que ocorrem em um espaço digital, geralmente mediado por tecnologias de informação e comunicação. No mundo virtual, as interações humanas não ocorrem de forma física, mas sim através de interfaces tecnológicas, o que confere à virtualidade algumas características e desafios únicos.

1.2.1 Características da Virtualidade

A virtualidade se define pela ausência de um espaço físico tangível. As interações ocorrem em uma dimensão digital, onde a presença física é remanescente por representações digitais, como por exemplo avatares, interfaces gráficas etc.

Uma das principais características da virtualidade é a alta interatividade. Os usuários podem interagir com conteúdo digital em tempo real, modificando e moldando suas experiências de acordo com suas preferências e necessidades. Além disso, ela promove a desconexão dos limites físicos e geográficos, possibilitando a comunicação e a interação entre pessoas de diferentes partes do mundo instantâneo.

O conteúdo digital e as interações na virtualidade podem ser armazenados, reproduzidos e acessados a qualquer momento. Isso significa que a realidade virtualizada pode continuar existindo independentemente da presença contínua dos usuários.

1.2.2 Desafios da Virtualidade

Deve ser levado em consideração que na virtualidade possui, também, os seus pontos negativos, os quais o usuário deve se atentar para que não sofra qualquer tipo de imprevisto.

Com o aumento da presença digital, um dos grandes desafios é garantir a proteção dos dados pessoais dos usuários. A virtualidade exige um tratamento cuidadoso das informações que são constantemente geradas e armazenadas.

Apesar das inovações tecnológicas, a ausência de interações físicas pode resultar em um senso de desconexão entre os indivíduos, o que pode impactar as relações humanas e a saúde mental, um ótimo exemplo foi durante a pandemia da COVID-19, onde houve um aumento exponencial do uso da internet, da interação do ser humano no ambiente virtual, momento do qual não era possível a interação por meio físico, onde no primeiro ano da pandemia de Covid-19, a prevalência global de ansiedade e depressão aumentou cerca 25% (vinte e cinco por cento), de acordo com estimativa da Organização Mundial da Saúde (Opas, 2022).

Nem todos têm o mesmo nível de acesso à tecnologia e à internet. Isso pode criar uma divisão digital, dificultando o acesso a esses ambientes virtuais para pessoas de baixa renda ou em regiões remotas.

A virtualidade levanta questões sobre jurisdição, leis de proteção de dados e regulação de comportamentos que ocorrem no ambiente digital. Determinar a responsabilidade em casos de fraudes, crimes virtuais ou violações de direitos autorais são apenas alguns dos desafios a serem enfrentados.

1.3 O DIREITO DO CONSUMIDOR NO CONTEXTO VIRTUAL

Com o crescimento exponencial do comércio eletrônico, o direito do consumidor no ambiente virtual ganhou uma importância significativa. O comércio digital apresenta novos desafios e exige uma adaptação das legislações para garantir a proteção dos consumidores em suas transações *online*. As questões relativas à informação, segurança, privacidade de dados e direitos nas compras *online* foram centrais no debate jurídico contemporâneo.

Essa evolução do processo produtivo causou um aumento progressivo dos riscos gerados aos consumidores, por meio de falhas resultantes desse processo. Nesse contexto, verificam-se o domínio do crédito, do marketing, da publicidade ilícita (abusiva e enganosa), das práticas abusivas, das cláusulas contratuais abusivas, da falta de informação adequada e do surgimento dos contratos de adesão, os quais diminuam ou impossibilitavam o exercício da liberdade contratual, bem como impunham dificuldades de acesso à justiça (Grinover, 2007, p. 6-7).

No contexto virtual, o direito à informação é crucial, uma vez que o consumidor não tem acesso físico ao produto ou serviço. A legislação exige que os fornecedores disponibilizem informações claras e detalhadas sobre os produtos ou serviços oferecidos, como cláusulas de segurança, preços, características técnicas, prazo de entrega e políticas de devolução (Benjamin, 2019).

A publicidade enganosa no ambiente digital pode ser mais sutil e difícil de identificar. A internet permite a disseminação de informações de forma massiva, mas também torna mais difícil para o consumidor avaliar a veracidade dessas informações. Portanto, a proteção contra práticas abusivas é essencial, e as plataformas *online* são obrigadas a fornecer meios para reclamações e ressarcimentos.

A proteção ao consumidor *online* com o transcorrer dos anos se torna indispensável, de modo que houve a necessidade de nova adequação da legislação em vigência para que possa estar sempre renovada para as práticas de abusividade, crimes contra o consumidor e até mesmo propagandas enganosas.

1.3.1 A Constituição Federal de 1988

Em seu artigo 5º, inciso XXXII, a Constituição Federal de 1988 estabelece a quem cabe a responsabilidade de proteção ao consumidor ao dispor que “o Estado promoverá, na forma da lei, a defesa do consumidor”.

Ao incluir a defesa do consumidor em cláusula pétrea, ou seja, situação que não pode ser eliminada ou alterada por emenda, verificou-se a importância desse público junto ao ordenamento jurídico.

Demais disso, o texto Constitucional também cita o consumidor ao dispor sobre a ordem econômica. Veja-se o que estabelece o artigo 170:

Art. 170. A ordem econômica, fundada na valorização do trabalho humano e na livre iniciativa, tem por fim assegurar a todos a existência digna, conforme os ditames da justiça social, observados os seguintes princípios: (...)
V - Defesa do consumidor;

O artigo 170 da CF/1988 demonstra a defesa do consumidor como um dos pilares da economia, ao lado de outros princípios como a livre iniciativa e a função social da propriedade. Isso demonstra que, no Brasil, a proteção ao consumidor é um princípio estruturante da atividade econômica.

Entre as normas que compõem o Direito do Consumidor, todas são de interesse social, como afirma o próprio artigo 1º do Código de Defesa do Consumidor ao dispor sobre a proteção e defesa desse público, nos termos do artigo 5º, inciso XXXII, e artigo 170, inciso V, da Constituição Federal, bem como do artigo 48 de suas Disposições Transitórias.

1.3.2 O Código de Defesa do Consumidor

O comércio nada mais é do que uma forma de fornecer o trabalho ou produto, onde uma pessoa contrata o serviço ou adquire o produto, sempre havendo a troca de serviço/produto por remuneração. Essa é uma relação de consumo típica, onde há interesse de uma das partes em vender e da outra em comprar, com isso é findado o contrato de consumo.

Virtualmente não é diferente, onde a parte está obrigada a entregar o produto/serviço nos moldes de como foi apresentado para o consumidor no ato da compra. Nesse contexto, o CDC surge de maneira essencial para garantir os direitos do consumidor e também do vendedor.

O CDC representa um conjunto de normas responsáveis pela proteção e garantia dos direitos do consumidor, estabelecendo regras a serem respeitadas e seguidas.

Uma das principais obrigações previstas no CDC é o dever de informação, disposto no artigo 6º, inciso III, que determina que o consumidor deve ter acesso a informações claras, precisas e ostensivas sobre os produtos ou serviços ofertados, bem como sobre os riscos que possam apresentar. No comércio eletrônico, essa exigência ganha contornos ainda mais relevantes, considerando que o consumidor não tem contato físico com o produto ou com o fornecedor, dependendo exclusivamente das informações disponibilizadas no ambiente virtual.

O avanço do comércio eletrônico exigiu adaptações legislativas complementares ao CDC, como a Lei Geral de Proteção de Dados (Lei nº 13.709/2018), que reforça a proteção das informações pessoais dos consumidores. Ainda assim, o CDC permanece como base normativa fundamental para garantir a transparência e o equilíbrio nas relações de consumo digitais, promovendo segurança jurídica tanto para consumidores quanto para fornecedores.

1.3.2.1 Princípio da Vulnerabilidade do Consumidor

O Princípio da Vulnerabilidade do Consumidor é uma das bases estruturais do Código de Defesa do Consumidor e um conceito essencial no sistema de proteção ao consumidor. Esse princípio reconhece que o consumidor se encontra em uma posição de desvantagem em relação ao fornecedor, o que torna indispensável a aplicação de normas jurídicas que assegurem sua proteção.

Essa proteção ao consumidor é justificada pela posição de desigualdade encontrada por ele nas relações de consumo que o torna vulnerável, quer seja pela falta de conhecimentos específicos sobre o produto ou serviço que adquire, quer seja pela ausência de conhecimentos jurídicos pertinentes à relação consumerista, ou ainda, pela diferença econômica entre ele e quem detém os meios de produção. Fernandes (2015, p. 150) conceitua vulnerabilidade como:

O princípio pelo qual o sistema jurídico positivado brasileiro reconhece a qualidade ou condição daquele sujeito mais fraco na relação de consumo, tendo em vista a possibilidade de que venha a ser ofendido ou ferido, na sua incolumidade física ou psíquica, bem como âmbito econômico, por parte do sujeito mais potente da mesma relação.

O CDC presume que todo consumidor é vulnerável e, portanto, por exemplo, um empresário rico também é considerado vulnerável quando este adquirir um produto ou serviço como destinatário final, posto que, quem detém o conhecimento sobre o que ele consumiu é o fornecedor. Assim, como demonstra Arruda (1995, p. 45):

O princípio da vulnerabilidade e a qualidade intrínseca, ingênita, peculiar, imanente e indissolúvel de todos que se colocam na posição de consumidor, pouco importando sua condição social, cultural ou econômica [...] incidível do contexto das relações de consumo, não admitindo prova em contrário por se tratar de mera presunção legal.

A vulnerabilidade do consumidor é presumida no caso de pessoas físicas. Contudo, no que diz respeito às pessoas jurídicas, sua existência precisa ser analisada de forma específica em cada situação, como previsto no artigo 4º, inciso I, do CDC, onde fica demonstrado a vulnerabilidade do consumidor.

2. A PROTEÇÃO DOS DADOS PESSOAIS NO COMÉRCIO ELETRÔNICO

2.1 A CAPACITAÇÃO DO CONSUMIDOR PARA UM *E-COMMERCE* SEGURO

A educação digital é crucial, certo de que a humanidade está no século da informação, onde todo e qualquer dado pode valer muito para a pessoa certa.

Diante um cenário em que se verifica desinformação e riscos com relação ao mundo virtual, o conhecimento digital do consumidor é uma ferramenta de empoderamento que na defesa dessa parte hipossuficiente nas relações comerciais junto à *internet*. A educação do consumidor surge como uma necessidade para despertar na sociedade a importância da proteção de dados pessoais no ambiente digital, vez que as fraudes e os golpes são eminentes e corriqueiros.

A capacitação dos consumidores por meio da educação digital é vista como essencial para a proteção de seus dados pessoais no ambiente digital, pois, onde através do conhecimento, os indivíduos podem reconhecer os riscos, compreender os direitos e adotar as medidas mais seguras (SaferNet Brasil, n.d.).

Quando se trata do contexto educação, o governo se torna fundamental para a educação e capacitação. A Escola Nacional de Defesa do Consumidor (ENDC), vinculada à Secretaria Nacional do Consumidor (Senacon), cumprem um papel de destaque nesse cenário. A ENDC oferta cursos online gratuitos, com a emissão de certificados pela Universidade de Brasília (UnB), que abrangem temas relacionados com o direito do consumidor e à proteção de dados pessoais. Iniciativa essa que busca fornecer aos consumidores as ferramentas necessárias para navegar com mais segurança e destreza no ambiente virtual.

Além da ENDC e do Senacon, outras instituições públicas contribuem para a formação e educação digital do consumidor. O Ministério da Educação (MEC), disponibiliza cursos de especialização em educação digital, capacitando profissionais para atuar na formação de cidadãos digitais.

O acesso à educação digital permite que o consumidor compreenda os riscos que podem surgir diante a negligência nos devidos cuidados, bem como a importância de se precaver na proteção de informações sensíveis.

Iniciativas como o oferecimento de cursos, *workshop* e materiais informativos desempenham um papel fundamental para a capacitação do consumidor. Ao

proporcionar o conhecimento necessário sobre a navegação segura, proteção de dispositivos e privacidade, os eventos de cunho informativo colaboram para a educação digital do consumidor que passa a fazer suas compras com menos chances de serem lesados financeiramente.

O impacto da capacitação e educação digital dos consumidores se reflete com a queda brusca nas fraudes e na edificação de um ambiente de *e-commerce* mais seguro. Os consumidores bem informados e capacitados são menos propensos a cair em golpes, vez que passam a ter acesso ao conhecimento e às ferramentas de defesa, e promovem suas operações comerciais que são importantes para a economia global.

2.2 OS DADOS PESSOAIS E A SUA IMPORTÂNCIA NO COMÉRCIO DIGITAL

A Lei Geral de Proteção de Dados (LGPD), define os dados pessoais são informações que permitem identificar uma pessoa, de forma direta ou indireta.

Segundo o autor Danilo Donega, a definição de dados pessoais na LGPD é ampla e abrangente qualquer informação que possa levar à identificação de uma pessoa natural, que seja de forma direta ou indireta. Essa definição reflete a preocupação da lei em proteger a privacidade e a autonomia dos indivíduos em um mundo cada vez mais digital (Donega, 2021).

Em um mundo virtualizado, o acesso as informações pessoais emergem como um ativo de valor inestimável, o qual é capaz de direcionar o consumidor para estratégias de *marketing* utilizadas pelas empresas para alcançar o seu maior e principal objetivo, obter lucro.

A possibilidade de personalizar a experiência vivenciada pelo consumidor, com uma simples coleta de dados e informações, pode ser capaz de direcionar anúncios e produtos que mais tem relevância para aquele público alvo da campanha publicitária. Abordagens como essa são capazes de criar vínculos entre a empresa e o consumidor, proporcionando assim maior lealdade e nutrindo um relacionamento duradouro.

A coleta e o uso de dados de consumidores exigem um alto compromisso com a transparência e segurança dessas informações, bem como há de se observar com rigor o tratamento dos dados conforme determina a LGPD, garantindo a proteção e privacidade àquele.

A confiança dos consumidores é um ativo valioso para as empresas de comércio digital e a proteção de dados pessoais é fundamental para construir e manter esse vínculo (*MCKinsey & Company, 2021*).

Em suma, os dados repassados pelo consumidor são um recurso de valor imensurável para o comércio digital, vez que impulsiona, personaliza e otimiza a construção de um melhor vínculo entre consumidor e a empresa. Mas, para tanto, requer uma grande responsabilidade, ética e privacidade para com os dados fornecidos e a sua inobservância, nos moldes da LGPD e da legislação específica, pode gerar sanções para a empresa.

2.3 OS RISCOS NO TRATAMENTO INADEQUADO DOS DADOS

A negligência no gerenciamento dos dados e informações do consumidor poderá acarretar prejuízos financeiros e danos à reputação da empresa.

A exposição de dados pessoais, resultante de práticas inadequadas de tratamento, pode levar a graves violações de privacidade e facilitar o roubo de identidade, expondo os indivíduos a riscos significativos (*ANPD, 2021*).

O risco de acesso indevido a informações privilegiadas facilita o roubo de identidade, permitindo que criminosos se passem por outras pessoas para cometer fraudes, golpes e outros crimes cibernéticos.

Em caso de vazamento de dados as consequências podem ser prejudiciais à saúde da empresa, em razão da existência de processos individuais e coletivos, danos à reputação junto ao nicho trabalhado no comércio eletrônico e perda da confiança de seus clientes, parceiros e possíveis investidores.

O descumprimento do tratamento de dados imposto pela LGPD acarretará em sanções legais para a empresa, incluindo multas e outras penalidades prevista na Lei.

Diante das consequências geradas pelo tratamento inadequado dos dados de seus consumidores, se faz necessário que cada vez mais os empresários invistam na segurança virtual dos dados coletados e fornecidos por seus clientes. O cumprimento da lei, juntamente com o investimento em novas tecnologias de proteção é o meio fundamental para exaurir os riscos no vazamento de dados.

2.4 A LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

A Lei Geral de Proteção de Dados (Lei nº 13.709/2018) é um marco regulatório que estabelece as regras para o tratamento dos dados pessoais por pessoas físicas e jurídicas, a qual visa proteger os direitos fundamentais de liberdade e de privacidade.

Tal norma atua como uma proteção para os direitos pessoais, estabelecendo regras para a coleta, armazenamento, uso e compartilhamento das informações, tanto para documentos físicos quanto para documentos armazenados virtualmente.

Dentre os principais aspectos da LGPD estão:

O artigo 5º, inciso I, dispõe que os dados pessoais são qualquer informação relacionada à pessoa natural identificável ou identificada. Esses dados fazem referência a não somente CPF e certidão de nascimento, mas também a trata de dados mais sensíveis, como dados referentes a saúde;

O Princípio do Tratamento de Dados destaca a observância dos principais aspectos e necessidades, como a finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização.

A lei exige ainda que as instituições adotem medidas de segurança técnicas e administrativas para proteger e gerenciar os dados pessoais contra possíveis invasões ou fraudes.

A LGPD garante a fornecedor dos dados uma série de direitos, como o direito ao acesso, retificação, oposição, portabilidade e revogação do consentimento (artigo 18).

Ocorre que a preocupação com a privacidade e a proteção de dados tornou-se uma questão de extrema importância para todos os tipos de negócios, principalmente após a aprovação da LGPD (*Privacy Tools*, n.d.).

O artigo 5º define os conceitos básicos como: dados pessoais, tratamento de dados e pessoa titular dos dados. Este artigo estabelece a essencialidade para interpretar as demais disposições da lei, garantindo clareza e uniformidade na aplicação das disposições da Lei.

Por sua vez, o artigo 9º garante ao titular do dado o direito de acessar qualquer informação sobre o tratamento de seus dados. Este artigo assegura a transparência e o controle do titular dos dados, permitindo que faça o acompanhamento e tenha maior compreensão de como está sendo utilizado e tratado.

A lei também estabelece um arcabouço de sanções administrativas para coibir o descumprimento das normas por ela impostas, buscando assegurar a proteção dos dados pessoais e responsabilizar as empresas que violarem as determinações impostas na Lei.

O artigo 52 detalha as sanções administrativas que a Autoridade Nacional de Proteção de Dados pode impor em casos de infrações. Dentre as penalidades previstas destacam-se a advertência, com indicação de prazo para a correção, a multa simples de 2% (dois por cento) do faturamento da empresa, multa diária, publicização da infração, bloqueio dos dados pessoais, eliminação dos dados etc. Além disso, a lei contempla a suspensão parcial do funcionamento do banco de dados, suspensão do exercício da atividade de tratamento de dados e a proibição total ou parcial de atividades relacionadas ao tratamento.

Já o artigo 53 define os critérios para a aplicação das sanções estabelecendo que a ANPD deve levar em consideração a gravidade da infração, a boa-fé do infrator, a vantagem obtida, a condição econômica do infrator, a reincidência, o grau do dano e a cooperação do infrator.

O artigo 54 disciplina sobre o processo administrativo para a aplicação das sanções, garantindo o direito ao contraditório e à ampla defesa. Esse artigo assegura que as organizações tenham a oportunidade de se defender e apresentar seus argumentos antes da implementação da penalidade, dando direito ao contraditório e a ampla defesa.

Além de penalidades administrativas, deve ser observado que em caso de descumprimento poderá acarretar responsabilidade civil e criminal, a depender da gravidade da infração. Portanto é de extrema importância que sejam seguidas todas as determinações impostas pela lei, para não acarretar qualquer tipo de penalidade.

2.5 A RESPONSABILIDADE DAS EMPRESAS NA PROTEÇÃO DE DADOS PESSOAIS

A LGPD estabelece um marco regulatório robusto para o tratamento de dados pessoais, atribuindo responsabilidades significativas às empresas que lidam com dados pessoais. O artigo 7º da LGPD estabelece um fundamento primordial para o tratamento dos dados pessoais, pois define as bases legais que autorizam o manuseio de dados, moldando o panorama das obrigações empresariais.

A LGPD, ao estabelecer as bases legais para o tratamento de dados pessoais, busca garantir que as empresas utilizem as informações de forma ética e responsável, respeitando os direitos dos titulares e evitando o uso abusivo dos dados (Doneda, 2021).

Essa busca por um tratamento ético e responsável implica que as empresas não podem coletar ou utilizar dados pessoais fornecidos de forma arbitrária. É necessário que haja uma justificativa legal para cada operação de tratamento, seja ela baseada no consentimento do titular dos dados, no cumprimento de uma obrigação legal, na execução de um contrato ou em definições previstas em lei.

As exigências previstas em lei, traduzem na necessidade de adotar medidas técnicas e organizacionais adequadas para proteger os dados ora fornecidos, evitando o vazamento de informações e outras formas de tratamento inadequado. Além disso, as empresas devem ser transparentes em relação às suas práticas de tratamento de dados, informando os titulares sobre como suas informações fornecidas serão utilizadas, armazenadas e se necessário compartilhadas.

As responsabilidades das empresas não se limitam à mera implementação de medidas de segurança e à transparência. É essencial que as empresas respeitem os direitos dos titulares dos dados, garantindo o acesso às informações, a correção de dados incorretos e eliminação de dados fornecidos desnecessariamente, entre outros direitos estabelecidos pela LGPD. O não cumprimento dessas obrigações podem acarretar em sanções administrativas.

A conformidade com a LGPD exige que as empresas implementem medidas de segurança robustas e demonstrem responsabilidade na gestão das informações pessoais, visando construir e manter a confiança dos consumidores (ANPD, 2020).

Em suma, a LGPD impõe um novo modelo para o tratamento de dados pessoais, exigindo que as empresas adotem posturas proativas na proteção dos dados e informações pessoais, priorizando a segurança, transparência e o respeito aos direitos dos titulares.

2.6 AS DECISÕES DOS TRIBUNAIS SUPERIORES

A jurisprudência do Superior Tribunal de Justiça (STJ) e o Supremo Tribunal Federal (STF) tem desempenhado um papel crucial na consolidação da proteção de

dados pessoais no Brasil, especialmente no que concerne às relações de consumo e ao tratamento de dados pessoais pelas empresas.

O STJ tem firmado entendimentos importantes sobre a aplicação da LGPD e a necessidade de adequação das empresas às normas de proteção de dados.

No julgamento do AREsp 2576503, de 11/02/2025, o STJ manteve a condenação de uma empresa por divulgar dados pessoais de um consumidor sem autorização. Este precedente destaca a responsabilidade das empresas na proteção dos dados de seus clientes e a importância do dever de informação. Por oportuno, indica-se o referido julgado:

EMENTA: CIVIL E PROCESSUAL CIVIL AGRAVO EM RECURSO ESPECIAL AÇÃO DE OBRIGAÇÃO DE FAZER CUMULADA COM INDENIZAÇÃO GESTÃO DE BANCO DE DADOS LEI N 12.414/11 ABERTURA DE CADASTRO DEVER DE INFORMAÇÃO DIVULGAÇÃO DE INFORMAÇÕES CADASTRAIS NECESSIDADE DE PRÉVIA AUTORIZAÇÃO DESCUMPRIMENTO AGRAVO CONHECIDO RECURSO ESPECIAL PARCIALMENTE PROVIDO.

(...)

(STJ; decisão monocrática, AREsp 2576503, Rel. Ministro Humberto Martins, julgado em 07/02/2025; publicado em 11/02/2025)

Nesta oportunidade, o Relator decidiu que:

(...) a hipótese dos autos não é de classificação da condição creditícia (credit score) da parte recorrente, mas sim de cadastro de dados pessoais (banco de dados), atividade essa que deve ser submetida às regras da Lei nº 12.414/2011. Ante o exposto, dou provimento ao recurso especial para julgar procedente o pedido da inicial, condenando a parte ora agravada ao pagamento de R\$ 3.000,00 (três mil reais) a título de danos morais ao recorrente, corrigidos monetariamente a partir desta data e com juros moratórios desde à citação (REsp n. 2.159.879, Ministro Marco Aurélio Bellizze, DJEN de DJe 01/10/2024.)

Ante o exposto, conheço do agravo e dou provimento ao recurso especial para julgar parcialmente procedente o pedido da inicial, condenando a parte recorrida a suspender a divulgação dos dados telefônicos do recorrente e ao pagamento de R\$ 3.000,00 (três mil reais) a título de danos morais, corrigidos monetariamente a partir desta data e com juros moratórios desde à citação.

Além disso, calha citar outra decisão no mesmo sentido, tal qual o REsp 2121904, de 11/02/2025. Veja-se:

EMENTA: CIVIL RECURSO ESPECIAL CONTRATO DE SEGURO DE VIDA RELAÇÃO DE CONSUMO CÓDIGO DE DEFESA DO CONSUMIDOR LEI GERAL DE PROTEÇÃO DE DADOS VAZAMENTO DE DADOS SENSÍVEIS RESPONSABILIDADE OBJETIVA. DANO MORAL PRESUMIDO RECURSO CONHECIDO EM PARTE DESPROVIMENTO.

1. Ação de obrigação de fazer c/c indenização por danos morais e materiais, da qual foi extraído o presente recurso especial, interposto em 28/6/2023 e concluso ao gabinete em 22/2/2024.
2. O propósito recursal é definir se, em contrato de seguro de vida, o vazamento de dados sensíveis do segurado gera: (a) dano moral presumido e (b) responsabilização objetiva da empresa seguradora.
3. Inexistência de negativa de prestação jurisdicional. Acórdão do Tribunal de origem devidamente fundamentado para solucionar integralmente a controvérsia submetida à sua apreciação.
4. Não há cerceamento de defesa nas hipóteses em que o julgador resolve a questão controvertida, de forma fundamentada, sem a produção da prova requerida pela parte, em virtude de considerar suficientes os elementos que integram os autos.
5. A matéria que não foi objeto de debate no acórdão recorrido, mesmo após a interposição de embargos declaratórios, não pode ser conhecida por meio de recurso especial. Súmula nº 211/STJ.
6. Cabe ao fornecedor o ônus de comprovar que cumpriu com seu dever de proteger dados pessoais do consumidor, sobretudo quando se tratam de dados sensíveis, nos termos do CDC (arts. 6º, VIII e 14, caput e §3º) e da LGPD (arts. 6º, X, 8º, §2º, 42, §2º e 48, §3º).
7. Há especial proteção legal aos chamados dados pessoais sensíveis: aqueles que, quando revelados, podem gerar algum tipo de discriminação, sobretudo os que incidem sobre "origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico" (art. 5º, II, da LGPD).
8. O tratamento de dados pessoais sensíveis observa requisitos significativamente mais rigorosos, sobretudo com a exigência, em regra, do consentimento específico e destacado do titular (art. 11 da LGPD).
9. Em contrato de seguro de vida, deve-se empreender um rigoroso esforço para a proteção dos dados pessoais, já que, para sua celebração, a seguradora, para a avaliação dos riscos, recebe dados sensíveis sobre aspectos pessoais, familiares, financeiros e de saúde do segurado.
10. O vazamento de dados pessoais sensíveis fornecidos para a contratação de seguro de vida, por si só, submete o consumidor a riscos em diversos aspectos de sua vida, como em sua honra, imagem, intimidade, patrimônio, integridade física e segurança pessoal.
11. Por isso, em seguro de vida, na hipótese de vazamento de dados sensíveis do segurado, verifica-se a responsabilização objetiva da seguradora e a caracterização de dano moral presumido.
12. Conforme entendimento desta Corte, a revisão da compensação por danos morais só é viável em recurso especial quando o valor fixado for exorbitante ou ínfimo, o que não se constata no recurso sob julgamento.
13. Hipótese em que o acórdão recorrido, ao manter a responsabilização da seguradora, reconheceu que: i) houve vazamento de dados pessoais do consumidor; ii) tais dados são classificados como sensíveis, de modo a abranger informações fiscais, bancárias e sobre a saúde do consumidor; iii) há nexos de causalidade entre o vazamento de dados sensíveis do consumidor e falhas na prestação do serviço pela recorrente, que não atendeu a seu dever de garantir a proteção dos dados sensíveis do consumidor.
14. Recurso especial parcialmente conhecido e, nessa extensão, desprovido. (STJ, 3ª Turma, REsp 2121904, Rel. Ministra Nancy Andrighi, Julgado em 11/02/2025; Publicado em 17/02/2025) (g.n.)

Importante destacar a conclusão da Relatora, ao entender que o vazamento de dados pessoais coloca o consumidor a riscos em diversos aspectos e que a responsabilização é objetiva, da seguradora, pois configura-se dano moral presumido.

O STF, por sua vez, tem reconhecido a proteção de dados pessoais como um direito fundamental, derivado do direito à privacidade e à intimidade. Como ocorreu no julgamento das ADIs 6387, 6388, 6389, 6390 e 6393, o Tribunal discutiu a constitucionalidade de medidas provisórias que alteravam a LGPD, mas foi em decisão proferida pelo Plenário, via da ADI 6.387/DF, que houve reafirmação sobre a importância da proteção de dados pessoais como um direito fundamental e acerca da necessidade de se garantir a segurança e a privacidade dos mesmos. Veja-se:

EMENTA: MEDIDA CAUTELAR EM AÇÃO DIRETA DE INCONSTITUCIONALIDADE REFERENDO MEDIDA PROVISÓRIA Nº 954/2020. EMERGÊNCIA DE SAÚDE PÚBLICA DE IMPORTÂNCIA INTERNACIONAL DECORRENTE DO NOVO CORONAVÍRUS (COVID-19). COMPARTILHAMENTO DE DADOS DOS USUÁRIOS DO SERVIÇO TELEFÔNICO FIXO COMUTADO E DO SERVIÇO MÓVEL PESSOAL, PELAS EMPRESAS PRESTADORAS, COM O INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA. FUMUS BONI JURIS. PERICULUM IN MORA. DEFERIMENTO.

1. (...); 2. (...); 3. (...); 4. (...); 5. (...):

6. Ao não apresentar mecanismo técnico ou administrativo apto a proteger, de acessos não autorizados, vazamentos acidentais ou utilização indevida, seja na transmissão, seja no tratamento, o sigilo, a higidez e, quando o caso, o anonimato dos dados pessoais compartilhados, a MP nº 954/2020 descumpra as exigências que exsurgem do texto constitucional no tocante à efetiva proteção dos direitos fundamentais dos brasileiros.

7. Mostra-se excessiva a conservação de dados pessoais coletados, pelo ente público, por trinta dias após a decretação do fim da situação de emergência de saúde pública, tempo manifestamente excedente ao estritamente necessário para o atendimento da sua finalidade declarada.

8. Agrava a ausência de garantias de tratamento adequado e seguro dos dados compartilhados a circunstância de que, embora aprovada, ainda não vigora a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), definidora dos critérios para a responsabilização dos agentes por eventuais danos ocorridos em virtude do tratamento de dados pessoais. O fragilizado ambiente protetivo impõe cuidadoso escrutínio sobre medidas como a implementada na MP nº 954/2020.

9. O cenário de urgência decorrente da crise sanitária deflagrada pela pandemia global da COVID-19 e a necessidade de formulação de políticas públicas que demandam dados específicos para o desenho dos diversos quadros de enfrentamento não podem ser invocadas como pretextos para justificar investidas visando ao enfraquecimento de direitos e atropelo de garantias fundamentais consagradas na Constituição.

10. Fumus boni juris e periculum in mora demonstrados. Deferimento da medida cautelar para suspender a eficácia da Medida Provisória nº 954/2020, a fim de prevenir danos irreparáveis à intimidade e ao sigilo da vida privada de mais de uma centena de milhão de usuários dos serviços de telefonia fixa e móvel.

11. Medida cautelar referendada.

(STF; Plenário; ADI 6387/DF; Rel. Ministra Rosa Weber; julgado em 07/05/2020; publicado em 12/11/2020) (g.n.)

As decisões dos Tribunais Superiores têm contribuído para a consolidação de uma jurisprudência favorável à proteção de dados pessoais no Brasil. Essa jurisprudência tem servido de guia para as empresas na adequação de suas práticas de tratamento de dados e para os consumidores no exercício de seus direitos.

3. O CENÁRIO CONTEMPORÂNEO CORRELACIONADO OS DESAFIOS CONSUMERISTAS

3.1 – NOVAS REGULAMENTAÇÕES E TECNOLOGIAS QUE IMPACTAM A SEGURANÇA DE DADOS

O cenário digital contemporâneo é marcado por uma presente preocupação com a segurança e a proteção de dados pessoais. Diante desse contexto, novas regulamentações e o avanço tecnológico desempenham papéis cruciais na construção de um ambiente online mais seguro e confiável.

No Brasil, a Lei Geral de Proteção de Dados (LGPD) (Lei nº 13.709/2018) representa um marco regulatório fundamental. Ela estabelece diretrizes rigorosas para o tratamento de dados pessoais, impondo obrigações às empresas e garantindo direitos aos titulares dos dados. A LGPD visa proteger a privacidade e a autonomia dos indivíduos, exigindo que as organizações adotem medidas de segurança adequadas e sejam transparentes em relação às suas práticas de tratamento de dados (Doneda, 2021).

Em paralelo às regulamentações, o desenvolvimento de novas tecnologias tem impulsionado a segurança de dados. A criptografia, por exemplo, é uma ferramenta essencial para proteger informações confidenciais, codificando-as de forma que apenas usuários autorizados possam acessá-las. A inteligência artificial (IA) e o aprendizado de máquina (*machine learning*) também desempenham um papel crescente na detecção de ameaças cibernéticas e na identificação de padrões anômalos que possam indicar atividades maliciosas.

Uma iniciativa de grande importância nesse contexto é a aprovação pela Câmara dos Deputados do projeto que cria a Política Nacional de Educação Digital. Essa política visa promover a capacitação e o desenvolvimento de competências

digitais em toda a sociedade. A educação digital é fundamental para conscientizar os cidadãos sobre os riscos *online* e as melhores práticas para proteger seus dados pessoais. Ao capacitar os indivíduos, essa iniciativa contribui para a construção de uma cultura de segurança digital mais robusta, onde os usuários estão mais preparados para identificar e evitar ameaças.

A combinação de regulamentações como a LGPD, que estabelecem o marco legal para a proteção de dados, com o desenvolvimento e a implementação de tecnologias avançadas de segurança e com promoção da educação digital, representa um esforço conjunto para fortalecer a segurança de dados no ambiente digital. Essa aliança é essencial para garantir a confiança dos usuários e fomentar um ecossistema digital mais seguro e resiliente.

3.2 – FISCALIZAÇÃO

A crescente expansão do comércio eletrônico no Brasil trouxe consigo não apenas conveniência e variedade para os consumidores, mas também novos desafios relacionados à proteção de seus direitos, especialmente no que tange à privacidade e segurança de seus dados pessoais. A Lei Geral de Proteção de Dados (LGPD) surge como um instrumento fundamental para endereçar essas questões, e a fiscalização de sua aplicação no contexto do *e-commerce* é crucial para garantir a efetividade dos direitos do consumidor.

O artigo 55-A da LGPD estabelece criação da Autoridade Nacional de Proteção de Dados (ANPD) com o papel de fiscalizar e aplicar as sanções previstas na lei. Este artigo é o coração da atuação regulatória e de fiscalização, garantindo que as empresas, incluindo aquelas que operam no comércio eletrônico, cumpram as normas de proteção de dados. A ANPD possui competência para instaurar processos administrativos, investigar denúncias e, se constatadas infrações, aplicar as sanções cabíveis, assim como estabelecido no artigo 55-J da LGPD.

Será também de competência da Autoridade Nacional de Proteção de Dados o zelo pela proteção dos dados pessoais, nos termos da legislação, zelar pela observância dos segredos comerciais e industriais, responsável por elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade, promover na população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e das medidas de segurança, etc. Essas são apenas algumas das

competências que a LGPD estabelece para a Autoridade Nacional de Proteção de Dados.

A ausência de uma fiscalização efetiva no comércio eletrônico pode levar a práticas abusivas, como a coleta excessiva de dados, o uso indevido de informações pessoais para fins de *marketing* não consentido e a falta de medidas de segurança adequadas, expondo os consumidores a riscos de fraudes e vazamentos de dados. A atuação da ANPD, portanto é essencial para coibir essas práticas e garantir um ambiente de consumo online mais seguro e confiável.

A importância da fiscalização no contexto do *e-commerce* também se relaciona com a necessidade de reduzir o “abismo digital”, conforme apontado por estudos realizados pela PwC, onde ressalta que, embora a maioria da população tenha acesso à *internet*, a qualidade e capacidade de utilização efetiva ainda são limitadas para muitos. A falta de conhecimento e a desconfiança em relação à segurança *online* podem ser barreiras para a plena participação no comércio eletrônico. Uma fiscalização rigorosa e a aplicação efetiva da LGPD podem contribuir para aumentar a confiança dos consumidores e fomentar um ambiente digital seguro e inclusivo.

Desta forma, a atuação da ANPD garante que as empresas cumpram suas obrigação legais, promovendo um comércio eletrônico mais transparente, seguro e alinhado com os princípios da proteção de dados pessoais.

CONCLUSÃO

O presente estudo possibilitou a compreensão acerca da evolução do comércio eletrônico e sua grande importância para a economia brasileira e mundial, bem como a verificação jurídica do *e-commerce* que é uma modalidade de compra e venda de produtos e serviços que revolucionou o mercado mundial, onde o consumidor consegue comprar o que quiser sem sair de casa.

No decorrer do desenvolvimento constata-se que o comércio eletrônico também possui o seu lado negativo, no qual o consumidor deve estar sempre atento para não cair em golpes, fraudes ou ter seus dados vazados.

A pesquisa apresenta a necessidade de uma legislação consumerista atualizada e eficiente que acompanhe a evolução do comércio eletrônico e proteja os direitos dos consumidores no ambiente virtual.

Para tanto, o trabalho demonstra a importância do CDC e da LGPD nesse contexto, ressaltando o papel de ambas na garantia da segurança jurídica e na promoção de relações de consumo equilibradas no comércio eletrônico.

No entanto, apesar dos avanços na legislação e na jurisprudência, ainda há desafios a serem superados haja vista que, todos os dias, as práticas criminosas se revolucionam, e da mesma forma deve ocorrer com o ordenamento jurídico, capaz de proteger, fiscalizar e autuar os responsáveis por transgredirem os direitos dos consumidores.

Deste modo, é necessário que haja um maior investimento em educação digital para os consumidores, a fim de que estes possam se proteger de forma eficaz no ambiente virtual, além da necessidade de conscientizar os consumidores sobre o risco em fornecer informações pessoais para sites. Além disso, é fundamental que as empresas adotem posturas proativas na proteção de dados, priorizando a segurança e a transparência em suas operações.

REFERÊNCIAS

AGÊNCIA GOV. **Escola Nacional de Defesa do Consumidor abre inscrições para cursos on-line.** 2025 Disponível em: <https://agenciagov.ebc.com.br/noticias/202501/escola-nacional-de-defesa-do-consumidor-abre-inscricoes-para-cursos-on-line>. Acesso em: 25 fev. 2025.

AGÊNCIA CÂMARA DE NOTÍCIAS. **Câmara aprova projeto que cria a Política Nacional de Educação Digital.** 2022 Disponível em: <https://www.camara.leg.br/noticias/931141-CAMARA-APROVA-PROJETO-QUE-CRIA-A-POLITICA-NACIONAL-DE-EDUCACAO-DIGITAL>. Acesso em: 12 out. 2024.

ARRUDA, Thereza. **Código do consumidor comentado.** 2 ed. Cidade: São Paulo. Revista dos Tribunais, 1995.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **Guia de boas práticas para agentes de tratamento de dados pessoais.** 2020. Disponível em: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-de-boas-praticas>. Acesso em: 17 nov. 2024.

_____. **Guia de segurança da informação para agentes de tratamento de pequeno porte.** Disponível em: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-de-seguranca-da-informacao-para-agentes-de-tratamento-de-pequeno-porte>. Acesso em: 20 out. 2024.

AVELAR, Dayanne. **E-commerce e direito do consumidor: aplicações do CDC em vendas online.** Migalhas, abr. 2024. Disponível em: <https://www.migalhas.com.br/depeso/405269/e-commerce-e-direito-do-consumidor-aplicacoes-do-cdc-em-vendas-online>. Acesso em: 17 nov. 2024.

AZEVEDO, Cristiano Oliveira; ODONE, Marcos Paulo; COELHO, Marcos Antônio Pereira. Estudo sobre a evolução do comércio eletrônico, suas formas de pagamentos digitais e suas preocupações quanto à segurança e a privacidade. **XI EVIDOSOL e VIII Ciltec-Online**, jun. 2014.

BENJAMIN, Antônio Herman de Vasconcellos e. **Manual de Direito do Consumidor.** 5 ed. São Paulo: Revista dos Tribunais, 2019.

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil de 1988.** Brasília: Senado Federal, Subsecretaria de Edições Técnicas, 2024.

BRASIL. **Lei nº 8.078, de 11 de setembro de 1990.** Dispõe sobre a proteção do consumidor e dá outras providências. Diário Oficial da República Federativa do Brasil, Brasília, 12 set. 1990. Seção 1, p. 1. Disponível em: http://www.planalto.gov.br/ccivil_03/Leis/L8078.htm. Acesso em: 25 fev. 2025.

CHAVES, Sílvia Fernandes. **A vulnerabilidade e a hipossuficiência do consumidor nas contratações eletrônicas.** Barueri (SP): Manole, 2015.

COFEN, **Conselho Federal de Enfermagem. Brasil vive uma segunda pandemia, agora na Saúde Mental.** 2022. Disponível em: <https://www.cofen.gov.br/brasil-enfrenta-uma-segunda-pandemia-agora-na-saude-mental/>. Acesso em: 25 fev. 2025.

DONEDA, Danilo. **A Lei Geral de Proteção de Dados Pessoais Comentada.** São Paulo: Thomson Reuters Brasil, 2021.

GOB.BR. **Educação digital é tema de especialização oferecida pelo MEC.** 2025. Disponível em: <https://www.gov.br/mec/pt-br/assuntos/noticias/2025/fevereiro/educacao-digital-e-tema-de-especializacao-oferecida-pelo-mec>. Acesso em: 14 mar. 2025.

GRINOVER, Ada Pellegrini, *et al.* **Código brasileiro de defesa do consumidor: comentado pelos autores do anteprojeto.** 9 ed. rev., atual. e ampl. Rio de Janeiro: Forense Universitária, 2007.

MARQUES, Cláudia Lima. **Contratos no Código de Defesa do Consumidor: o novo regime das relações contratuais.** 6 ed. São Paulo: Revista dos Tribunais, 2017.

MCKINSEY & COMPANY. **The consumer-data opportunity and the privacy imperative**. 2020. Disponível em: <https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/the-consumer-data-opportunity-and-the-privacy-imperative>. Acesso em: 12 dez. 2024.

NET, Safer. **Precisamos de mais educação digital**. 2021. Disponível em: <https://new.safernet.org.br/content/precisamos-de-mais-educacao-digital>. Acesso em: 12 mar. 2025.

OLIVEIRA, N. M. LEVY, Pierre. O que é o virtual. São Paulo: ed. 34, 1996. **Perspectivas em Ciência da Informação**, 3(1), São Paulo 2007. Disponível em: <https://periodicos.ufmg.br/index.php/pci/article/view/23252>. Acesso em: 01 mar. 2025.

OPAS, **Organização Pan-Americana da Saúde. Pandemia de COVID-19 desencadeia aumento de 25% na prevalência de ansiedade e depressão em todo o mundo**. 2022. Disponível em: <https://www.paho.org/pt/noticias/16-3-2022-pandemia-covid-19-desencadeia-aumento-25-na-prevalencia-ansiedade-e>. Acesso em: 15 dez. 2025.

PRIVACY TOOLS. **Educação em privacidade e a proteção da identidade dos clientes**. N.D. Disponível em: <https://www.privacytools.com.br/educacao-em-privacidade-e-a-protacao-da-identidade-dos-clientes/>. Acesso em: 20 out. 2024.

PWC BRASIL. **O abismo digital no Brasil**. 2022. Disponível em: <https://www.pwc.com.br/pt/estudos/preocupacoes-ceos/mais-temas/2022/o-abismo-digital-no-brasil.html>. Acesso em: 27 fev. 2025.

SUPERIOR TRIBUNAL DE JUSTIÇA (STJ). **In re ipsa: os entendimentos mais recentes do STJ sobre a configuração do dano presumido**. 2022 Disponível em: <https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/2022/11092022-In-re-ipsa-os-entendimentos-mais-recentes-do-STJ-sobre-a-configuracao-do-dano-presumido.aspx>. Acesso em: 19 nov. 2024.