

VULNERABILIDADE DO CONSUMIDOR NO CIBERESPAÇO E A LEI GERAL DE PROTEÇÃO DE DADOS

CONSUMER VULNERABILITY IN CYBERSPACE AND THE GENERAL DATA PROTECTION ACT

Vinicius de Assis Pinto¹
Carine Silva Diniz²

Resumo: Pretende-se neste trabalho discutir o estabelecimento dos meios virtuais enquanto nova modalidade de interação social, cultural, econômica e comercial. Tem-se que a relação estabelecida entre sociedade e o processo tecnológico apresenta altos níveis de dependência e risco frente ao compartilhamento de informações e estruturação de banco de dados. Diante desse contexto, o presente ensaio tem por objetivo analisar a vulnerabilidade do consumidor no ciberespaço, bem como as proteções legais a ele garantidas na Lei Geral de Proteção de Dados (LGPD) e no Código de Defesa do Consumidor (CDC). Ao longo do estudo, estabeleceu-se a diferenciação entre “crimes de comprometimento de dispositivos tecnológicos” e de “tráfico de dados pessoais”, apercebendo-se que o ambiente tecnológico é propício ao acometimento destas condutas que ocasionam perdas financeiras não só aos consumidores, mas, também aos prestadores de bens e serviços.

Palavras-chave: Direito do Consumidor; Tecnologia da Informação; Crimes Cibernéticos; LGPD; Vulnerabilidade.

Abstract: The aim of this work is to discuss the establishment of virtual media as a new modality of social, cultural, economic and commercial interaction. The relationship established between society and the technological process has high levels of dependency and risk when sharing information and structuring a database. Given this context, this essay aims to analyze the vulnerability of consumers in cyberspace, as well as the legal protections guaranteed by the General Data Protection Law (LGPD) and in the Consumer Defense Code (CDC). Throughout the study, a distinction was established between "crimes of compromising technological devices" and "trafficking in personal data", realizing that the technological environment is conducive to the

¹ Graduado em Direito do Centro Universitário Metodista Izabela Hendrix. E-mail: vinicius.assis0703@gmail.com

² Mestre em Direito Privado pela Pontifícia Universidade Católica de Minas Gerais. Pós-Graduada em Direito Público e Direito de Família e Sucessões. Coordenadora do Núcleo de Prática Jurídica do Centro Universitário Metodista Izabela Hendrix. Professora. E-mail: carine.diniz@izabelahendrix.metodista.br

involvement of these behaviors that cause financial losses not only to consumers, but also to providers of goods and services.

Keywords: Consumer Rights; Information Technology; cibercrimes; GDPR; Vulnerability.

Introdução

As relações interpessoais sofreram significativas modificações após o surgimento da *internet*, que se deu em meados da década de 60, e a sua disseminação mundo afora, na década de 90. Nesse contexto, o conceito de distância também se transformou. Assim, a comunicação física deixou de representar um problema nas relações sociais, muito menos no que se refere às transações comerciais. Outro ponto de destaque se concentra na velocidade e no fluxo de acesso e difusão das informações que, por sua vez, possibilitou a formação de banco de dados, abarcando infinitos tipos de armazenamento de informações das pessoas (SIQUEIRA *et al.*, 2021.)

No cenário atual, o espaço *online* ou cibernético é considerado o novo ambiente social, coexistente e definitivamente associado ao real, o que gera consequências e implicações nas interações humanas, sendo designado como a “Era da Informação”. Todavia, a facilidade em se comunicar de forma instantânea trouxe vantagens e desvantagens que não se limitam apenas ao uso particular da *internet*, mas também às organizações de todo mundo que a utilizam, por exemplo, na apresentação de produtos e serviços pelas plataformas digitais, como também no armazenamento dados da empresa e dos próprios clientes. Na adequação aos meios digitais, empresas privadas e entidades governamentais mantêm em seus sistemas inúmeras informações de consumidores, muitas das vezes por eles não autorizadas, o que leva ao questionamento de até que ponto se estende a privacidade no meio cibernético (NASCIMENTO *et al.*, 2017).

As informações introduzidas de maneira maciça em sistemas digitais e disponibilizadas por todo o mundo ocasionaram, indiscutivelmente, um progresso e melhoria nas relações interpessoais, bem como no modo de vida da sociedade. No entanto, o impacto provocado por tais processos é de difícil controle, gerando, assim, insegurança para os consumidores que podem ter suas informações compartilhadas, mesmo permissão. Nessa seara, surgem os crimes cibernéticos: há dados que indicam taxa muito alta de ocorrência destes delitos nos últimos anos. Para se ter uma ideia, no âmbito global aproximadamente 65% dos adultos já foram vítimas de crimes de caráter virtual. No Brasil, os dados retratam um cenário preocupante; 76% dos adultos brasileiros já foram vítimas de algum tipo de crime digital. Entre os países com maior incidência está a China, com 83% de casos em sua população adulta (NORTON, 2018).

Nessa contextura, o trabalho objetiva analisar a vulnerabilidade do consumidor no ciberespaço, as proteções dispensadas pela Lei Geral de Proteção de dados (LGPD) e o Código de Defesa do Consumidor. Para tanto, será explicado, de maneira sucinta, como se dá o tratamento de dados, quem são os sujeitos de direitos, mais especificamente no âmbito do consumo e, nos moldes da LGPD, como os fornecedores de serviços e produtos responderão pelos danos causados na violação de proteção de dados.

Finalmente, esclarece-se que para a confecção do trabalho, se valeu da metodologia bibliográfica de pesquisas exploratórias.

O ciberespaço e a inserção das TICS

Foi em 1894 que o termo ciberespaço foi mencionado pela primeira vez, por mais que a rede de *internet* ainda não existisse. Inicialmente era visto como: “um espaço não físico ou territorial composto por um conjunto de redes de computadores através das quais todas as informações (sob as suas mais diversas formas) circulam” (SANTOS, 2010, p. 18).

Para muitas pessoas, o ciberespaço é o reflexo do futuro aterrorizante e desumano que é apresentado nas ficções científicas. Nele haverá identificação de pessoas, análise de dados sem local estabelecido, memórias serão apagadas, haverá guerras de clones descontrolados em decorrência de interações diversas em tempo real (MACEDO, 2016). Trata-se de espaço observado como o lugar do saber, um ambiente de signos, uma forma de disseminação da comunicação e de ideias conjuntas humanas (SANTAELLA, 2014). Corresponde ao “espaço de comunicação aberto pela interconexão mundial dos computadores e das memórias dos computadores” (SIQUEIRA *et al.*, 2021, p.5). Tais fatores deixam claro que os computadores não representam um componente isolado, mas conectados a outras máquinas e dispositivos, com capacidade de transmissão global e velocidade para um grande processamento de dados.

O espaço *online* é analisado como o novo ambiente social e paralelo que apresenta muitos desafios e consequências nas relações humanas. Com isso, tem-se a compreensão de *locus* que pertence a uma dimensão imaterial. Para Silva (2013) o ciberespaço seria como:

Espaço imaterial tecnologicamente construído na camada eletromagnética do planeta e pressuposto entre computadores conectados por modem e fibras óticas [...]. Tal espaço imaterial não tem, naturalmente, qualquer semelhança com o espaço geográfico. Trata-se de um espaço tempo, ou melhor, um espaço-velocidade [...]; como tal, não pode ser provocado empiricamente, embora seja real. (SILVA, 2013, p. 38).

Nessa realidade, novas expressões culturais surgiram, também conhecidas como a cibercultura e com ela novas formas de transações comerciais, econômicas e sociais. As mudanças estão sempre em constante fluxo, em permanente desterritorialização.

Quando se fala em ciberespaço é normal que muitos tenham uma concepção de algo não palpável, ou seja imaterial, lugar que não pode ser acessado por humanos, onde as interações no âmbito social, bem como cultural e econômico ao se instituírem se faz no campo imaginário, em outras palavras, em um ambiente futurístico.

Na concepção de Siqueira e Medeiros (2011), o espaço cibernético é um universo virtual no qual circulam informações por meio de interação através de computadores interligados. As interações humanas atualmente estão ligadas a esse espaço virtual transnacional de comunicação interativa. Nessa mesma linha, Monteiro e Fidencio (2013) destacam que o ciberespaço é uma região abstrata invisível e por ela circulam as informações que podem ser de diversos formatos e símbolos como sons, imagens, textos e movimentos. Constitui-se pela confluência digital unificada na agregação de diferentes formatos e mecanismos em um mesmo ambiente, isto é, corresponde a um

espaço abstrato introduzido no ambiente das TIC's³. Com isso, em meio ao processo evolutivo das tecnologias, hoje em dia, o ciberespaço não pode ser analisado apenas como um espaço de conexões diversas entre computadores, mas sim, abrangendo todos os dispositivos inseridas no contexto atual, tais como, *tablets*, *smartphones*, *laptops*, dentre outros dispositivos. E esse cenário propicia um ambiente de multiconectividades.

É preciso salientar, ademais, que por meio desse espaço, pode-se disponibilizar as informações que irão permitir a criação de novas tecnologias. O ciberespaço propiciou o nascimento de um novo paradigma no tocante a sociedade humana, um novo meio, um local ainda desconhecido, que começa a ser explorado. O ambiente provoca uma relação nova de tempo e espaço. Nesse novo processo, o tempo não se configura mais como linear já o espaço não é mais efetivo (MONTEIRO, 2007).

Diante disso, ressalta-se que, no contexto em que novas demandas sociais são concebidas, o acesso à *internet* é visto como um direito essencial de acordo com a Organização das Nações Unidas (ONU) (2011), fazendo com que a informação se torne chave para a evolução dos povos.

As redes informacionais

Quando se pensa em *web* ou rede é preciso ter em mente a ideia de cadeia conectada. Do latim *retis* a rede é mensurada por inúmeras linhas assim como fios que se misturam e se sustentam (MARTINO, 2014). Desde os primórdios, existem sistemas de redes, adaptados a seu tempo. Para se ter uma ideia, na civilização pré-colombiana eram usados sistemas de comunicação tendo como elo estradas e pontes que serviam como meio de ligação entre divisões do Império Incas. Entre as atribuições principais desse sistema de comunicação concentrava as ações de mensageiros que cruzavam as estradas com o intuito de levar informações para outros povos, significando o modelo antigo mais efetivo no que se refere a rede de comunicações (SIQUEIRA *et al.*, 2021).

No século XIX, ocorreram mudanças profundas em relação à comunicação. No âmbito mundial, por meio das redes informacionais que foram aperfeiçoadas com a criação do telégrafo e, principalmente, do telefone, sistema esse que possibilitou a redução da distância tendo como parâmetro uma nova compreensão no que tange a espaço-tempo que surgiu naquele período (SANTAELLA, 2014).

No século XX, em meados da década de 40, a evolução da indústria eletro e microeletrônica se tornou um marco importante para o início da terceira revolução industrial, assim como para sua solidificação, somando a uma percepção de progresso representada pela tecnologia (CARDOSO, 2016). Segundo Siqueira *et al.* (2021, p. 4), “Pouco tempo depois, foram se aperfeiçoando as indústrias automobilística, aérea e eletrônica com foco na computação, período em que se ampliam as redes de comunicação e aparecem os primeiros contornos do ciberespaço”.

A década de 70 marcou um processo evolutivo ainda maior: nesse período, houve difusão ampla das tecnologias da informação, potencializando o seu desenvolvimento dinâmico e se configurando em um novo modelo. Esse processo teve como pontos fundamentais a invenção dos computadores que ocorreu no período da Segunda Guerra Mundial, inicialmente com o intuito de formular cálculos e que logo depois

³ TIC's é a sigla para tecnologias da informação e da comunicação, se trata de recursos tecnológicos que oferecem automação e otimizam a comunicação, como computadores, celulares, hardware utilizados (ALGAR, 2022).

evoluiu para a criação de microprocessadores, bem como dispositivos de linguagem de comunicação. Com o passar do tempo, propiciou a comunicação entre máquinas e os seres humanos, criando uma maior acessibilidade para o seu uso, por mais que a população não tivessem tanto conhecimento sobre informática (SILVA, 2015).

Já na década de 80, a informática passou por uma “crise de identidade” que não era associada somente às questões técnicas no campo industrial, contexto esse que aproximava a sociedade das telecomunicações. Em paralelo, o avanço das tecnologias de telecomunicações associada ao aperfeiçoamento microeletrônico, possibilitou a ligação entre microcomputadores, utilizando de redes que eram conectadas e se comunicavam (ROZA, 2017).

Segundo Siqueira *et al* (2021):

[...] essa capacidade de desenvolvimento de redes só se tornou possível graças aos importantes avanços tanto das telecomunicações quando das tecnologias de integração de computadores em rede, ocorridos durante os anos 70. Mas, ao mesmo tempo, tais mudanças somente foram possíveis após o surgimento de novos dispositivos microeletrônicos e o aumento da capacidade de computação, em uma impressionante ilustração das relações sinérgicas da revolução da tecnologia da informação (SIQUEIRA *et al*, 2021, p.5).

Para Siqueira *et al*. (2021):

O crescimento e popularização da rede mundial de computadores, especialmente a partir do final do século XX para o início do século XXI, se caracteriza por um fluxo de informações através daquela rede jamais antes verificada na humanidade, sendo que as atividades exercidas ou facilitadas pelas tecnologias atreladas à *internet* penetraram o próprio meio de vida das pessoas, impactando das mais diversas maneiras na sociedade (SIQUEIRA *et al*, 2021, p.5).

E com base em todo este arcabouço, é que foi possível, na década de 90, a consolidação da *internet* como rede global de computadores, disseminada por todo o mundo e com possibilidade de acesso de quaisquer pessoas ligadas ao computador, como também a uma linha telefônica individual (VELOSO, 2017).

Os crimes cibernéticos

As inovações tecnológicas e a globalização trouxeram consequências positivas e negativas à sociedade, uma vez que a utilização desse recurso também atrai toda a diversidade de pessoas, com os mais variados objetivos, e muitas delas usam as redes de computadores para cometer crimes, lesando tanto pessoas físicas como organizações empresariais, societárias ou governamentais (ARRUDA, 2019).

Com a popularização da *internet*, inúmeras novas condutas criminosas passaram a fazer parte do cotidiano social, não havendo regulamentação legal suficiente para coibir esse tipo de conduta. Os agentes encontraram no espaço *ciber* um campo livre a ser navegado: os delitos crescem a cada dia mais, em razão da liberdade de serem cometidos em qualquer localidade do planeta, sendo motivo de preocupação por parte das autoridades. A rede é utilizada pelos criminosos para se conectarem a dispositivos de empresas, organizações e em computadores pessoais, para terem acesso a dados confidenciais e utilizá-los para obter vantagens. Essa conduta criminosa é um dos reflexos negativos da inovação tecnológica.

Para Siqueira *et al* (2021)

Os crimes cibernéticos ou crimes de informática podem ser classificados como condutas que atentam contra dados e contra o computador (e através dele), ou seja, são aqueles crimes relacionados às informações arquivadas ou em trânsito por computador, sendo esses dados acessados ilicitamente, usados para ameaçar ou fraudar; para tal prática é indispensável a utilização de um meio eletrônico (SIQUEIRA, 2021, p. 11).

O Departamento de Justiça dos Estados Unidos divide os crimes cibernéticos em três categorias principais, quais sejam, os cibercrimes puros, mistos e comuns. Os puros são aqueles cujo computador é o alvo do criminoso. Os mistos são os cibercrimes em que se utiliza só sistema do computador como meio para a prática a ação. E os comuns são aqueles que o computador é usado para guardar informações ilegais e roubadas (DUARTE, 2022).

O Conselho da Europa, em 2001 na Convenção de Budapeste sobre Cibercriminalidade, tipificou algumas condutas como infrações contra a confidencialidade, integridade e disponibilidade dos dados e sistemas informáticos, como sendo: “acesso doloso e ilegal a um sistema de informática; interceptação ilegal de dados ou comunicações telemáticas; atentado à integridade dos dados, falsificação de dados, estelionatos eletrônicos” (VERÇOSA, 2010, p. 1)

Com isso, percebe-se a necessidade de adequação do direito no que concerne à proteção daqueles que utilizam os TIC's e que hoje é quase que indispensável na vida em sociedade. É indiscutível aproximar o direito das inovações tecnológicas, fortalecendo as proteções jurídicas dos usuários, em razão da criminalidade cibernética atual, visto que esses delitos têm atingido várias esferas da sociedade, seja corporativa, os órgãos de dados estatísticos, bancos, órgãos de inteligência de governo e demais entidades.

Em relação ao Brasil, uma das primeiras legislações nesse sentido foi a chamada Lei da Informática (Lei 7.646/87), assim intitulada devido ao fato de ser a primeira a tipificar uma conduta que, embora assemelhada à violação de direito autoral, constituía um crime informático em sentido próprio, declarado expressamente que o regime de proteção à propriedade intelectual de programas do computador era o direito do autor (BRASIL, 1987).

Em seguida, a Lei n. 9.609/98 dispôs sobre a propriedade intelectual, no que tange a rede de computadores, especificamente aos direitos autorais referentes a obras (BRASIL, 1998).

Em 2012, a Lei nº 12.737/2012, conhecida como Lei Carolina Dieckmann, acrescentou ao Código Penal Brasileiro, (artigo 154-A e 154-B). Ademais, foi alterada a redação dos artigos 266 e 298, passando a tipificar delitos especificamente virtuais (BRASIL, 2012).

Em 2022, o governo lançou plano tático de combate a crimes cibernético, a fim de prevenir e reprimir tais ações criminosas.

O plano Tático de Combate a Crimes Cibernéticos contém eixos temáticos que destacam a prevenção e a mitigação de ameaças cibernética; o gerenciamento de riscos e incidentes decorrentes da

criminalidade cibernética; o aprimoramento de infraestruturas críticas para combate a crimes cibernéticos; o amparo legal e regulamentar; as parcerias nacionais e cooperação internacional; a padronização e a integração informacional; além de pesquisa, desenvolvimento, inovação e educação para o enfrentamento a crimes cibernéticos (BRASIL, 2022, p. 4).

Apesar destas ações pontuais, Arruda (2019) destaca que o atual direito tem acompanhado de forma lenta as modificações sociais, especificamente, considerando a velocidade com que a tecnologia avança.

Em 2001, o então Procurador da República na Bahia, Vladimir Aras, fez um alerta sobre sua preocupação com os danos causados por parte das organizações criminosas no que tange a ocorrência de crimes virtuais. Segundo Aras:

as perdas com fraudes no ano passado atingiram R\$200 milhões. “No ano anterior, o prejuízo foi de R\$ 260 milhões e, em 1998, de R\$300 milhões”. A Abecs tem se preocupado com os cibercrimes praticados mediante o uso fraudulento de cartões de crédito e está introduzindo no mercado os cartões com chips eletrônicos, que têm alto nível de segurança (ARAS, 2001, p.28).

Importa ressaltar, ademais, que o aumento do uso da *internet* durante o período pandêmico levou indivíduos com pouca experiência para o ambiente *online*, tornando-se alvos fáceis aos ataques no ciberespaço. Conforme a *Fortiner Threat Intelligence Insider Latin America*, empresa que analisa a segurança cibernética e os seus incidentes, o Brasil sofreu em 2020 mais 3,4 bilhões de tentativas de ataque na *internet*. Também foi observado um crescimento maior, em 2020, das denúncias de crimes cibernéticos, em comparação com 2019. Os crimes mais comuns foram *phishing*⁴, golpes do cartão de crédito ou boleto bancário, *mobile malware*⁵, *WhatsApp* clonado⁶ e auxílio emergencial falso⁷ (SÁ; SILVA, 2020).

Os incidentes destacam a importância da proteção dos dados pessoais, com o estabelecimento de políticas públicas e legislações aptas a combater tais condutas. Contudo, o ordenamento jurídico brasileiro ainda não está preparado para coibir esses delitos, visto que as legislações são recentes e o aparato jurídico ainda ineficiente para atender a crescente demanda. Mesmo assim, os criminosos da *internet*, quando identificados, sofrem sanções penais. Como ressalta Almeida et al (2015):

⁴ Golpes de *phishing* consiste em um ato criminoso que induz o indivíduo a disponibilizar suas informações pessoais, relacionadas a contas bancárias, assim como senhas de cartões de créditos, no momento que o indivíduo abre um link infectado (ARIANE, 2022)

⁵ Mobile malware são aplicativos maliciosos disponibilizados por exemplo, no Play Store. Por mais que em diversos casos o próprio Google busque excluí-los, durante o tempo que fica disponível para ser baixado tem potencial de prejudicar milhares de pessoas (IVAN, 2019)

⁶ WhatsApp clonado consiste no ato da aquisição da posse por um indivíduo não autorizado, sem a vítima ter conhecimento. O infrator ganha acesso a conta da vítima com a permissão para utilizá-la de várias formas (MARCELA, 2018).

⁷ Auxílio emergencial falso está associado a aplicativos com o mesmo nome do verdadeiro, porém, com algumas exigências que não são feitas de forma convencional, em muitos dos casos a vítima é direcionada para sites que não são seguros e nem faz parte do Governo Federal (SOFIA, 2021).

No tocante a atuação da polícia em crimes de computação, crime dessa natureza requer investigação especializada e ação efetiva. Infelizmente, não existem no Brasil policial preparado para combater esse tipo de crime, faltando, pois, visão, planejamento, prepara e treinamento (ALMEIDA *et al*, 2015, p. 5).

Note-se que os crimes cibernéticos muitas vezes encontram resistência na sua resolução justamente em razão da dificuldade de identificação do autor, que geralmente pratica o crime de forma anônima, ou, ao menos, “distante” do local de consumação delitual. Frise-se que essa dificuldade não é encontrada somente no Brasil, mas no mundo todo.

o grande problema da investigação, legislação pouco eficaz e o anonimato do agente delituoso, são sem dúvida fatores que contribuem para impunidade e faz com que esses delitos aumentem cada vez mais no país. A ausência de identidade física nesse ambiente favorece o anonimato eletrônico, o que demanda uma modificação de postura pela qual o Direito analisa os fenômenos pessoais dentro dessa seara. Dessa maneira, o direito brasileiro necessita de uma postura mais atenciosa quando se fala em crimes informáticos (ARRUDA, 2019, p.16).

Nosso país ainda caminha lentamente na discussão sobre cibersegurança. A legislação é pouco eficiente, havendo, ainda, um longo caminho a percorrer. No que diz respeito aos recursos e sistemas de investigação, tem-se que são pouco integrados e, muitas vezes, incapazes de identificar esses crimes. A falta de equipamentos, pessoas devidamente capacitadas e a pouca efetividade da legislação existente corroboram para os crimes digitais se alastrem cada vez mais rápido e de forma eficaz (ARRUDA, 2019). Vale destacar a escassez de delegacias especializadas na investigação de cibercrimes, em contraste com a quantidade de ocorrência delitual.

A desinformação da população sobre os problemas de segurança virtual também as torna mais vulneráveis. O Brasil apresenta políticas ineficazes de adequada conscientização coletiva. Além disso, as empresas e corporações desconhecem a importância de contratar ou capacitar profissionais para atuar na segurança dos dados e no combate à invasão de seus sistemas, bem como de denunciar a sua ocorrência. Isso reforça a necessidade de cooperação entre Estado e entidades no combate ao cibercrime:

A maioria das empresas virtuais que sofrem invasões não denuncia a ocorrência, haja vista que os dados furtados são de seus “clientes” e muitas vezes serão utilizadas por terceiros sem que estes percebam, pelo menos até que algo pior ocorra (...). Alguns têm medo de tornar a ocorrência pública por temerem que haja dano à marca, que passaria a imagem de ser insegura perante o universo dos consumidores (PINHEIRO, 2016, p. 108).

Denota-se que o Direito se encontra diante uma realidade que exige novos contornos legislativos na proteção dos consumidores conectados ao ciberespaço, bem como a tipificação dos crimes. A regulamentação jurídica é necessária para resguardar a população e frear os excessos.

Lei Geral de Proteção de Dados

Tem-se, ainda, que não apenas as condutas tipificadas como crimes podem gerar danos aos direitos do consumidor no âmbito do ciberespaço, como também condutas que se associem com o armazenamento, tráfego, cessão e compartilhamento de dados dos usuários de bens e serviços digitais (SIMÃO FILHO; SCHWARTZ, 2016, p. 313).

Tendo em vista a evolução tecnológica, e objetivando assegurar maior proteção das informações no contexto cibernético, em 2018 foi sancionada pelo então Presidente da República Michel Temer, a Lei nº 13.709, intitulada de Lei Geral de Proteção de Dados Pessoais (BRASIL, 2018). De acordo com Vitorio (2020):

A LGPD consiste na regulamentação da proteção de dados pessoais e privacidade dos indivíduos nas redes sociais e prevê a adoção de políticas e planos de proteção destes. Com ela, o usuário tem mais controle de para onde vão seus dados quanto inseridos em determinados sites, e poderá saber o que é feito com eles. Ela é baseada do Regulamento Geral de Proteção de Dados (GDPR, na sigla em inglês) e, na prática, dá aos consumidores mais controle e às empresas mais responsabilidade na adoção práticas mais transparentes na guarda e uso de dados (VITORIO, 2020, p. 2).

Por mais que existam no país normas que, de maneira direta e indireta, abordam a proteção e privacidade em relação a dados pessoais⁸, a LGPD trouxe novos elementos a incrementar este amparo, sendo mais pontual, englobando, inclusive, a proteção destas informações tanto de forma *online* quanto *off-line* e estendeu o seu alcance aos órgãos públicos e entes privados. (BRASIL, 2018). Assim, se destaca como um divisor de águas em relação às normas anteriores, conduzindo o Brasil, inclusive, à condição de maior competitividade no mercado internacional (BRASIL, 2018).

Tendo como base a LGPD, Nobre *et al.* (2018, p. 7) apontam alguns itens considerados fundamentais para sua efetivação, por abordar pontos cruciais da manipulação da informação, ou seja, como pode ser tratada, usada e compartilhada.

Os pontos destacados têm como objetivo estabelecer normas claras para as organizações em relação ao armazenamento, abordagem e o compartilhamento de

⁸ Por exemplo, o Marco Civil da Internet – Lei nº 12.965/14 tem como objetivo promover a regulação do uso da internet no Brasil. Todavia, a lei também possui dispositivos de proteção ao uso de dados que circulam na internet. Desta forma, prevê princípios, garantias, direitos e deveres para a utilização da internet no território brasileiro, ou seja, o seu foco não está associado de forma específica à proteção de dados. O artigo 3º da Lei nº12.965/14 colaciona os princípios que orientam o uso da internet no Brasil:

Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios:

I – garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal;

II – proteção da privacidade;

III – proteção dos dados pessoais, na forma da lei;

IV – preservação e garantia da neutralidade de rede;

V – preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas;

VI – responsabilização dos agentes de acordo com suas atividades, nos termos da lei;

VII – preservação da natureza participativa da rede;

VIII – liberdade dos modelos de negócios promovidos na internet, desde que não conflitem com os demais princípios estabelecidos nesta Lei. Parágrafo único. Os princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte. (BRASIL, 2014).

informações pessoais, estimulando, assim, o crescimento econômico e tecnológico, em um século marcado por inovações e com um grande tráfego de informações (AGOSTINELLI, 2018). Somando a isso, a LGPD tem como finalidade garantir à população a utilização de dados adquiridos por terceiros por meio de mecanismos mais seguros que ofereça proteção jurídica respaldada por lei.

Segundo Monteiro (2018), a LGPD trouxe como maiores vantagens os seguintes pontos:

- Unificar regras: regras únicas e harmônicas sobre o uso de dados pessoais, independente do setor da economia.
- Maior flexibilidade: autorizar formas mais flexíveis para o tratamento de dados pessoais, tais como legítimos interesses, que levam em consideração uma sociedade movida a dados em tempos de big data.
- Redução de custos: diminuir custos operacionais causados por incompatibilidades sistêmicas de tratamentos feitos por agentes diversos, além de fomentar uma maior qualidade dos dados em circulação no ecossistema como um todo.
- Adequar as regras no Brasil: tornar o Brasil apto a processar dados oriundos de países que exigem um nível de proteção de dados adequados, o que pode fomentar, principalmente, os setores de tecnologia da informação.
- Portabilidade: indivíduos poderão transferir seus dados de um serviço para outro, aumentando a competitividade no mercado (MONTEIRO, 2018, p. 04).

Nessa toada, são 65 artigos que atribuem à LGPD a responsabilidade de garantir a segurança da informação. Conforme já citado, a lei estabelece maior competitividade do país no mercado internacional, pois, implementa meios aptos a assegurar que os dados que aqui trafegam tenham maior proteção, exigindo que empresas busquem se adequar à nova realidade (NOBRE, *et al.* 2018).

Segundo o Serviço Federal de Processamento de Dados (SERPRO), a troca de dados é um fato que nos últimos anos tem se intensificado devido o avanço tecnológico:

Já dá para perceber que o tratamento de dados acontece a todo momento e local [...]. E ocorre na forma de coleta, registro, produção, recepção, organização, classificação, utilização, disponibilização, adaptação, alteração, reprodução, transmissão, distribuição, processamento, armazenamento, conservação, recuperação, comparação, interconexão, transferência, difusão, extração, eliminação de dados (SERPRO, 2021, p. 2).

Nota-se que o fluxo de dados ocorre de formas diversas, devido à necessidade que se impõe, gerando assim, um número muito grande de informações, sendo necessário a existência de mecanismos de a coibir que estes dados caiam em mãos erradas, ocasionado a prática de delitos aptos, inclusive, a causar danos irreversíveis à pessoa afetada. O *big data*⁹¹⁰, por exemplo, é um exemplo de ferramenta que consegue fazer essa seleção de dados.

⁹ O big data é uma ferramenta que engloba a coleta de dados como também promove o seu processamento, sendo fundamental para a gestão de dados, dada a sua grande funcionalidade.

Segundo o Serviço Federal de Processamento de Dados (SERPRO) os fundamentos da LGPD incluem:

- O respeito à privacidade, ao assegurar os direitos fundamentais de inviolabilidade da intimidade, da honra, da imagem e da vida privada;
- A autodeterminação informativa, ao expressar o direito do cidadão ao controle, e assim, a proteção de seus dados pessoais e íntimos;
- A liberdade de expressão, de informação, de comunicação e de opinião, que são direitos previstos na Constituição brasileira;
- O desenvolvimento econômico e tecnológico e a inovação, a partir da criação de um cenário de segurança em todo o país;
- A livre iniciativa, a livre concorrência e a defesa do consumidor, por meio de regras claras e válidas para todo o setor privado;
- Os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas (SERPRO, 2021, p. 2).

Tais fundamentos não só ressaltam aspectos relacionado a ética na convivência social, como também abrangem questões de transparência para a vida em sociedade, em que se deve respeitar a privacidade de cada cidadão.

Vulnerabilidade do Consumidor

A luz do Código de Defesa do Consumidor, o princípio da vulnerabilidade é norteador da legislação consumerista, ou seja, o intuito legal é proteger a parte mais frágil da relação de consumo, buscando o equilíbrio, tendo em vista que o consumidor é considerado como vulnerável perante o fornecedor.¹¹

Este é um assunto que vem ganhando atenção nos campos disciplinares do *marketing* e do comportamento do consumidor, pois, o fenômeno exige esforço de desembaraço e politização de suas complexidades já presentes em sua definição enquanto estado de impotência que surge do desequilíbrio nas interações de mercado ou do consumo de *marketing* e bens e serviços e os próprios consumidores (KONDER, 2015).

É notório que as compras *online* sejam entendidas enquanto mecanismo de contorno da distância física e/ou financeira no acesso de consumidores aos fornecedores. Existe ainda ações afirmativas que ressaltam a acessibilidade promovida por essa modalidade comercial aos indivíduos que são excluídos de participar plenamente no mercado físico (pessoas que sofrem de doenças crônicas e demais deficiências e incapacidades permanentes ou temporárias) (ELMS; TINSON, 2012).

É inquestionável que as vendas *online* tem se tornado preferência de muitos consumidores e crescido em todo mundo, vez que oferece diversidade de preço e de

¹⁰ A concentração de recursos computacionais permite a detecção, captura, coleta e processamento de dados em tempo real de bilhões de dispositivos conectados, atendendo a diversas aplicações, incluindo monitoramento ambiental, aplicações industriais, negócios e centrados no ser humano (ZASLAVSKY; PERERA; GEORGAKOPOULOS, 2013, p. 3).

¹¹ Art. 4º. A Política Nacional das Relações de Consumo tem por objetivo o atendimento das necessidades dos consumidores, o respeito à sua dignidade, saúde e segurança, a proteção de seus interesses econômicos, a melhoria da sua qualidade de vida, bem como a transparência e harmonia das relações de consumo, atendidos os seguintes princípios:

I – Reconhecimento da vulnerabilidade do consumidor no mercado de consumo. (BRASIL, 1990)

fornecedores, além da comodidade de realizar a compra em casa. Entretanto, muitas pessoas têm problemas com esta modalidade de consumo, sendo os mais frequentes a apropriação indevida de dados de cartões e contas bancárias, o não recebimento dos produtos e o recebimento de produtos falsos.

Tem-se que uma das formas mais comuns de criminosos acessarem os dados de cartões de crédito ou contas bancárias é *phishing*, que é uma técnica de fraude que acontece, em geral, por intermédio *sites* ou *e-mails* falsos de empresas de renome. O mais comum é que os conteúdos com *phishing* ofereçam promoções absurdas, se passando pela empresa verdadeira. Ao realizar a compra, os criminosos têm acesso aos dados da vítima, podendo, então, utilizar seus cartões de crédito e fazer transferências bancárias (NEVES, 2018).

Outra estratégia comum entre os criminosos é a criação de *sites* fraudulentos que não entregam as mercadorias. Nesse caso, a vítima faz o pagamento, mas não recebe o produto. Há também os *sites* que comercializam produtos como se fossem novos e originais, mas a vítima recebe um produto usado, falsificado e, muitas vezes, inútil (NEVES, 2018).

Vale lembrar que o Código de Defesa do Consumidor define que toda publicidade *online* deve ser entregue ao usuário com transparência, proibindo o uso de informação que possa induzir o consumidor ao erro. Além disso a LGPD determina regras sobre o uso de dados pessoais em todas as transações *online*¹².

A proteção legal no cyberspaço e suas limitações

Considerando o cenário exposto, é notável a imposição de uma postura regulamentária que viabilize maior proteção aos consumidores na *internet*. A vanguarda dessa ação estatal é representada principalmente pela *General Data Protection Regulation* (GDPR), documento da União Europeia e que influenciou os documentos legais de proteção de dados pessoais de vários outros países, especialmente o Brasil (MARINHO et al, 2021). Foi nesse contexto que a Lei Geral de Proteção de Dados (LGPD) (Lei n. 13.709/2018) foi elaborada (BRASIL, 2018):

o tratamento de dados pessoais é um tema relevante que indica a necessidade de maiores debates, especialmente em face da vulnerabilidade do cidadão frente os agentes de tratamento que possuem mais expertise de suas atividades, e até mesmo frente ao Estado. A economia digital e os benefícios diretos que proporciona, juntamente com as dificuldades de compreensão dos seus efetivos impactos são fatores que criam ônus adicionais para os titulares, de modo que muitas vezes não sabem como se proteger minimamente. Isso remete à possíveis ofensas aos titulares dos dados quando nos referimos aos diversos impactos que a atividade pode causar (MARCULINO, 2021, p. 26).

Isso posto, quando se trata de trocas comerciais, mesmo que em ambiente virtual, o Código de Defesa do Consumidor (CDC) (Lei N.º 8.078/1990) também é outra normativa inclusa na proteção dos usuários (BRASIL, 1990). E se a LGPD se associa mais a preocupação com dados e coleta, o CDC, por sua vez, assume a “fragilidade do consumidor frente ao poder econômico do fornecedor” como premissa determinada para a lei (MARCULINO, 2021, p. 27).

¹² Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:
(...)

VI – A livre iniciativa, a livre concorrência e a defesa do consumidor. (BRASIL, 2018).

Assim, ao incluir segmentos amplos como banco de dados e cadastro de consumidores, em seu artigo 43, de maneira diferente da preocupação ideológica da LGPD, o CDC assume caráter mais prático e, procura proteger o cidadão de sua diferença de poder frente ao fornecedor para garantir sua independência e autonomia para tomada de decisões comerciais. Dessa forma, vê-se certa complementariedade entre as duas normativas brasileiras quanto ao tema (DE LIMA, 2020).

Contudo, essa mutualidade apresenta limitações no contexto brasileiro, especialmente porque culturalmente existe certa interpretação jurídica de busca por aberturas e frestas legais em ambas as leis para proteção e aplicação em casos pontuais. Ademais, não existe um bom nível de consciência social acerca da importância de proteção de dados e, portanto, da relevância de não os oferecer levemente (MARCULINO, 2021).

Por último, mesmo que se pressuponha que o cidadão seja um indivíduo apto, consciente e independente para realizar suas trocas comerciais de maneira segura, não se pode perder de vista que, mesmo hipoteticamente, ele seria vulnerável no meio digital. Contudo, o que se percebe é que a hipótese não se mantém, pois, o perfil da inconsciência digital consumidor brasileiro na verdade, intensifica sua vulnerabilidade já existente (MARCULINO, 2021).

Ademais, por mais que existam leis protetivas, o consumidor ainda enfrenta desafios de como se dará o tratamento de dados pessoais. A transparência formal não é eficiente se as informações não forem acessíveis às diversas camadas da sociedade, especialmente aos consumidores hipervulneráveis, que nos termos do art. 39, IV, do CDC, são os idosos, as crianças, os analfabetos, as pessoas com deficiência mental, pessoas com saúde debilitada (BRASIL, 1990), e, em se tratando da realidade digital, aqueles sem conhecimento informático.

É preciso asseverar que a hipervulnerabilidade é a situação social fática e objetiva de agravamento da vulnerabilidade da pessoa física consumidora, por circunstâncias pessoais aparentes ou conhecidas do fornecedor, que geram a necessidade de oferecer maior proteção a estes indivíduos, inclusive no meio digital (SCHMITT, 2014, p.233). Nesse sentido:

O modus de vida atual não deixa margem de dúvidas acerca das dificuldades desses sujeitos de direitos, ante a potencialização de lesões aos seus interesses, advindas do crescimento do comércio eletrônico e do incremento do ambiente virtual na vida de relação, onde a velocidade das mudanças impõe barreira quase intransponível àqueles dotados de natural fragilidade física, psicológica ou até mental (SCHWARTZ, 2016).

Conforme o exposto, os aspectos jurídicos e normativos são essenciais para a proteção dos vulneráveis no cyberspaço, mas não são o suficiente. É necessário que o fornecedor e os que se encontram no mercado *online* sejam cooperativos, desenvolvendo suas plataformas e seu modo de comercializar considerando as vicissitudes consumeristas, especialmente, dos hipervulneráveis, promovendo, assim, inclusão e segurança desses indivíduos no mercado digital.

REFERÊNCIAS

ALMEIDA, J. J. *et al.* Crimes cibernéticos. **Ciências Humanas e Sociais Unit**. v. 2. n.3. p. 215-236. 2015.

ARAS, V. Crimes de informática. Uma nova criminalidade. **Jus Navigandi**, Teresina, ano 6, n. 51, 1 out. 2001.

ARRUDA, J. E. G. **Cibercrime no âmbito das relações empresariais**: a vulnerabilidade das empresas no tocante à impunidade do ordenamento jurídico. Caruaru, 2019. 26 f. Trabalho de conclusão de Curso (Bacharel em Direito) Centro Universitário Tabosa de Almeida – ASCES-UNITA, Caruaru, 2019.

AGOSTINELLI, J. A importância da lei geral de proteção de dados pessoais no ambiente online. **ETIC-ENCONTRO DE INICIAÇÃO CIENTÍFICA-ISSN 21-76-8498**, v. 14, n. 14, 2018.

BRASIL. **Lei nº 7.646, de 18 de dezembro de 1987**. Dispõe quanto à proteção da propriedade intelectual sobre programas de computador e sua comercialização no País e dá outras providências. Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l7646.htm. Acesso em: 25 jun. 2022.

BRASIL. **Lei nº. 8.078, de 11 de setembro de 1990**. Código de Defesa do Consumidor. Dispõe sobre a proteção do consumidor e dá outras providências. Brasília, 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/Leis/L8078.htm. Acesso em: 22 mar. 2022.

BRASIL. **Lei nº 9.609, de 19 de fevereiro de 1998**. Dispõe sobre a proteção da propriedade intelectual de programa de computador, sua comercialização no País e dá outras providências. Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9609.htm. Acesso em: 25 jun. 2022.

BRASIL. **Lei nº 12.737, de 30 de novembro de 2012**. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 12 mai. 2022.

BRASIL. **Lei nº 12.965, de 24 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da *Internet* no Brasil. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 14 de maio de 2022.

BRASIL. Casa Civil. **Lei no 13.709, de 14 de agosto de 2018**. Planalto. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Lei/L13709.htm. Acesso em: 14 de maio de 2022.

BRASIL. **Lei Geral de Proteção de Dados Pessoais**. Brasília, DF: Congresso Nacional, 2018. Planalto. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 14 de maio de 2022.

BRASIL. Segurança Pública. **Governo Federal lança Plano Tático de Combate a Crimes Cibernéticos**. Disponível em: <https://www.gov.br/pt-br/noticias/justica-e-seguranca/2022/03/governo-federal-lanca-plano-tatico-de-combate-a-crimes-ciberneticos>. Acesso em: 25 jun. 2022.

BATAT, W. Understanding the dimensions of young consumer vulnerability in the web 2.0 society. In: **Child and Teen Consumption CTC**. 2010. p. 250. Disponível em: <https://halshs.archives-ouvertes.fr/halshs-00527884/>. Acesso em: 12 mai. 2022.

BRAIAN, A. **Da aplicação da lei penal no espaço**. Arturbraian. 2016. Disponível em: <https://arturbraian.jusbrasil.com.br/artigos/202860569/da-aplicacao-da-lei-penal-no-espaco>. Acesso em: 14 de maio de 2022.

CAVERNA, K. **Marco Civil da Internet**. Klebercaverna. 2014. Disponível em: <http://klebercaverna.blogspot.com/2014/04/marco-civil-da-internet.html>. Acesso em: 14 de maio de 2022.

CARDOSO, M. O. **Indústria 4.0**: a quarta revolução industrial. 2016. 43 f. Trabalho de Conclusão de Curso (Especialização em Automação Industrial) - Universidade Tecnológica Federal do Paraná, Curitiba, 2016.

- DA SILVA, R. B.; DOS SANTOS, V. M.; DE ANDRADE, M. L. Direito do consumidor. *JICEX*, v. 3, n. 3, 2014.
- DE SÁ JUNIOR, S. R. C. **A regulação jurídica da proteção de dados pessoais no Brasil**. 2018. 45 f, Monografia (Especialista em Direito) Pontifica Universidade Católica do Rio de Janeiro – PUC-Rio, Rio de Janeiro, 2018.
- DE LIMA, C. R. P. **Comentários à Lei Geral de Proteção de Dados: Lei n. 13.709/2018, com alteração da Lei n. 13.853/2019**. Almedina, 2020.
- DE ALMEIDA, J. B. **Manual de direito do consumidor**. Saraiva Educação SA, 2017.
- DUARTE, L. B. **Infiltração policial no âmbito virtual como meio de combate à violação sexual de crianças e adolescentes: uma análise à luz da Lei nº 13.441/17**. 2022. 55 f. Monografia (Graduação em Direito) Centro de Ciências Sociais Aplicadas, Universidade Federal do Rio Grande do Norte, Natal, 2022.
- ELMS, J.; TINSON, J. Consumer vulnerability and the transformative potential of *Internet* shopping: An exploratory case study. *Journal of Marketing Management*, v. 28, n. 11-12, p. 1354-1376, 2012.
- FUNDAÇÃO EDUCACIONAL FORTUNATO RODRIGUES DO PRADO – FEFORP. **Iniciação e história da LGPD**. Feforp. 2021. Disponível em: <https://feforp.com.br/lgpd>. Acesso em: 14 de maio de 2022.
- HAMILTON, K.; DUNNETT, S.; PIACENTINI, M. **Consumer vulnerability: Conditions, contexts and characteristics**. Ed. Routledge, 2015.
- KONDER, C. N. Vulnerabilidade patrimonial e vulnerabilidade existencial: por um sistema diferenciador. *Revista de Direito do Consumidor*, v. 99, p. 101-123, 2015.
- MARINHO, G. et al. (Ed.). **Aspectos relevantes da Lei Geral de Proteção de Dados**. Editora Contracorrente, 2021.
- MARCULINO, K. S. **Vulnerabilidade do titular de dados pessoais e a responsabilidade dos agentes de tratamento**. 2021. 87 p. Trabalho de Conclusão de Curso (Bacharel em Direito) Universidade Federal do Rio Grande do Sul, Porto Alegre, 2021.
- MARTINO, L. M. S. **Teoria das mídias digitais: linguagens, ambientes e redes**. Editora Vozes Limitada, 2014.
- MACEDO, K. T. M. **Linchamentos virtuais: paradoxos nas relações sociais contemporâneas**. 2016. 131 f. Dissertação (Mestra em Ciências Humanas e Sociais Aplicadas) Universidade Estadual de Campinas, Limeira, 2016.
- MONTEIRO, S. D. O ciberespaço: o termo, a definição e o conceito. *Revista de Ciência da Informação*. v.8 n.3 Jun/07. 2007.
- MONTEIRO, S. D.; FIDENCIO, M. V. As dobras semióticas do ciberespaço: da web visível à invisível. *TransInformação*, v. 25, n. 1, p. 35-46, 2013.
- MONTEIRO, R.L. **Lei Geral de Proteção de Dados do Brasil – Análise**: Disponível em: <https://baptistaluz.com.br/institucional/lei-geral-de-protacao-de-dados-do-brasil-analise/>. Acesso em: 14 de maio de 2022.
- NASCIMENTO, C. R. et al. CRIMES CIBERNÉTICOS À LUZ DA LEI 12.737/2012: AVANÇOS E RETROCESSOS. *REVISTA DE TRABALHOS ACADÊMICOS-UNIVERSO RECIFE*, v. 4, n. 2, 2017.
- NOBRE, J. *et al.* Segurança da Informação para *Internet* das Coisas (IoT): uma Abordagem sobre a Lei Geral de Proteção de Dados (LGPD). *Revista Eletrônica de Iniciação Científica em Computação*, v. 17, n. 4, 2019.
- NORTON. Relatório de Crimes Cibernéticos NORTON: **O impacto humano**. Symantec. 2018. Disponível em: https://www.symantec.com/content/en/us/home_homeoffice/media/pdf/cybercrime_report/Norton_Portuguese-Human%20Impact-A4_Aug18.pdf. Acesso em: 22 de maio. 2022.

- PINHEIRO, P. P. **Proteção de Dados Pessoais: Comentários à Lei n. 13.709/2018-LGPD.** Saraiva Educação SA, 2020.
- PINHEIRO, P. P. **Direito digital.** Saraiva Educação SA, 2016.
- ROLIM, M. C. L. M.; GIBRAN, S. M. Lei Geral De Proteção De Dados (Lei Nº 13.709/2018) e Terceiro Setor: Principais Desafios E Alternativas Rumo À Adequação. **CAMPO JURÍDICO**, v. 9, n. 1, p. 723, 2021.
- ROZA, R. H. Revolução informacional e os avanços tecnológicos da informática e das telecomunicações. **Ciência da Informação em Revista**, v. 4, n. 3, p. 3-11, 2017.
- SANTOS, F. B. H. **O TWITTER como ferramenta de marketing em bibliotecas nacionais ibero-americanas.** 2010. 120 f. Trabalho de Conclusão de Curso (Bacharel em Biblioteconomia) Universidade Federal do Rio Grande do Sul, Porto Alegre, 2010.
- SANTAELLA, L. **Comunicação ubíqua: repercussões na cultura e na educação.** Pia Sociedade de São Paulo-Editora Paulus, 2014.
- SÁ, D. S. O. I.; SILVA, P. P. **Da ineficácia da lei carolina dieckmann na ocorrência de crimes virtuais.** animaeducacao. 2020. Disponível em: <https://repositorio.animaeducacao.com.br/bitstream/ANIMA/14143/1/Tcc%20definitivo%20enviado%20RUNA.pdf>. Acesso em: 20 de maio de 2022.
- SANTOS, C. O. **Lei Geral de Proteção de Dados Pessoais (LGPD), LEI Nº 13.709/2018: Direito à privacidade aplicada às redes sociais.** 2021. 32 f. Artigo (Bacharel em Direito) Universidade Católica de Goiás – (PUCGOIÁS), Goiânia. 2021.
- Serviço Federal de Processamento de Dados – SERPRO. **Detalhes sobre a lei que afeta seu dia a dia: mais sobre objetivo, abrangência e fundamentos da LGPD.** Serpro. 2021. Disponível em: <https://www.serpro.gov.br/lgpd/menu/tratamento-dos-dados/objetivo-e-abrangencia-da-lgpd>. Acesso em: 14 de maio de 2022.
- SILVA, J. R. R. **As tecnologias da informação e comunicação no ensino de Geografia: formação e prática docente.** 2015. 176 f. Dissertação (Mestrado em Ciências Humanas) - Universidade Federal de Uberlândia, Uberlândia, 2015.
- SILVA, G. C. **O ciberespaço como categoria geográfica.** 2013. 178 f. Dissertação (Mestrado em Geografia) Universidade de Brasília, Brasília, 2013
- SIQUEIRA, P. N. *et al.* A (hiper)vulnerabilidade do consumidor no ciberespaço e as perspectivas da LGPD. **Rev. Eletrônica Pesquiseduca.** V.13, N. 29, p.236-255, jan.-abril 2021.
- SIQUEIRA, H. S. G.; MEDEIROS, M. F. S. Somos todos ciborgues: aspectos sociopolíticos do desenvolvimento tecnocientífico. **Configurações**, n. 8, p. 11-32, 2011.
- SIMÃO, A. F.; SCHWARTZ, G. A. "Big Data" Big Problema! Paradoxo entre o direito à privacidade e o crescimento sustentável. **Conpedi Law Review.** V.2, n.3, p. 311-331. 2016.
- SIMÕES, A. G. A RELAÇÃO DE CONSUMO SOB O PARADIGMA DA CONSTITUIÇÃO ECONÔMICA. **Revista Intervenção, Estado e Sociedade**, v. 2, n. 1, p. 84-111, 2015.
- SOUZA T. **LGPD – LEI GERAL DE PROTEÇÃO AOS DADOS.** Dootax. 2019. Disponível em: <https://blog.dootax.com.br/lgpd-lei-geral-de-protecao-aos-dados/>. Acesso em: 14 de maio de 2022.
- SOARES, R. R. **Lei de proteção de dados – LGPD: Direito á privacidade no mundo globalizado.** 2020. 29 f. Monografia (Bacharel em Direito) Universidade Católica de Goiás – PUCGOIÁS, Goiânia, 2020.
- TAURION, C. **Big data.** Brasport, 2013.