

DESAFIOS LEGAIS DA INTERNET E REDES SOCIAIS: PRIVACIDADE, DIFAMAÇÃO, CYBERBULLYING, FAKE NEWS E RESPONSABILIDADE DAS PLATAFORMAS ONLINE NO CONTEXTO JURÍDICO BRASILEIRO

Artigo científico apresentado ao Centro Universitário São Lucas Ji-Paraná, para obtenção de grau na disciplina Trabalho de Conclusão de Curso, em Direito. Sob orientação do Prof. Esp. Teófilo Lourenço de Lima.

Ji-Paraná

2024

Dados Internacionais de Catalogação na Publicação - CIP

G639d Gonsalves, Weksiley Silva.

Desafios legais da internet e redes sociais: privacidade, difamação, cyberbullying, fake news e responsabilidade das plataformas online no contexto jurídico brasileiro. / Weksiley Silva Gonsalves. – Ji-Paraná, 2024.

24 p.

Artigo Científico (Curso de Direito) – Centro Universitário São Lucas Ji-Paraná, 2024.

Orientador: Prof. Esp. Teófilo Lourenço de Lima.

1. Privacidade. 2. Responsabilidade. 3. Fake news. I. Lima, Teófilo Lourenço de. II. Título.

CDU 34:004.738.5

DESAFIOS LEGAIS DA INTERNET E REDES SOCIAIS: PRIVACIDADE, DIFAMAÇÃO, CYBERBULLYING, FAKE NEWS E RESPONSABILIDADE DAS PLATAFORMAS ONLINE NO CONTEXTO JURÍDICO BRASILEIRO

Weksiley Silva Gonsalves¹
Teófilo Lourenço de Lima²

RESUMO: Os desafios legais da internet e redes sociais no Brasil envolvem questões complexas como privacidade, difamação, cyberbullying, fake news e a responsabilidade das plataformas online. A privacidade é uma preocupação central, especialmente com a coleta massiva de dados pessoais, o que levou à criação da Lei Geral de Proteção de Dados (LGPD). A difamação e o cyberbullying nas redes sociais também demandam atenção, pois a facilidade de disseminação de informações pode causar danos irreparáveis à reputação e bem-estar das pessoas. As fake news, por sua vez, desafiam o sistema jurídico, exigindo um equilíbrio entre a liberdade de expressão e a proteção contra a desinformação. Por fim, a responsabilidade das plataformas online é debatida, principalmente em relação ao controle e moderação de conteúdo, buscando-se um meio-termo entre a autorregulação e a intervenção estatal, conforme previsto no Marco Civil da Internet.

Palavras-chave: Privacidade, Responsabilidade, Fake news.

ABSTRACT: The legal challenges of the internet and social media in Brazil involve complex issues such as privacy, defamation, cyberbullying, fake news, and the responsibility of online platforms. Privacy is a central concern, especially with the mass collection of personal data, leading to the creation of the General Data Protection Law (LGPD). Defamation and cyberbullying on social media also demand attention, as the ease of disseminating information can cause irreparable harm to individuals' reputations and well-being. Fake news poses another challenge to the legal system, requiring a balance between freedom of expression and protection against misinformation. Finally, the responsibility of online platforms is debated, particularly regarding content control and moderation, seeking a middle ground between self-regulation and state intervention, as outlined in the Brazilian Internet Civil Framework.

Keywords: Privacy, Responsibility, Fake news.

¹ Acadêmico do 9º período do Curso de Bacharelado em Direito, pelo Centro Universitário São Lucas de Ji-Paraná – UniSL. E-mail: weksiley77@gmail.com

² Professor orientador, pós-graduado em Administração e Planejamento para Docentes pela Ulbra, 1996; pós-graduado em Inovação, Gestão e Práticas Docentes no Ensino Superior pela Faculdade Santo Agostinho, 2021; Licenciado em Pedagogia pela Universidade Federal de Rondônia, 1996; pós-graduando em Psicologia Jurídica e Forense pela Faculdade Unyleya; Bel. Em Direito pelo Centro Universitário São Lucas. E-mail: teofilolourenodelima@gmail.com.

1 INTRODUÇÃO

Com advento das novas tecnologias em vários âmbitos da sociedade muitas áreas sofreram transformações inimagináveis ao se comparar com antigo modelo praticado pela sociedade em décadas e séculos passados. Ao se fazer uma linha do tempo passando desde as primeiras civilizações na qual nascia os primeiros conceitos, princípios e normas jurídicas do que era certo ou errado, de onde vem a moral e a ética? Debates calorosos onde o principal intuito muitas vezes era o de apenas que algo contribuísse para elucidasse e contribuísse para o avanço daquilo que um dia se tornariam doutrinas, normas e leis.

As leis brasileiras atuais sobre privacidade online não estão completamente adaptadas para lidar com os desafios contemporâneos. Além do mais, o aumento da difamação e o cyberbullying nas redes sociais demandam uma revisão das legislações de proteção à reputação e integridade pessoal. Ademais, outro ponto que requer uma legislação minuciosa, com solidez nas jurisprudências que há de se surgir com o aumento desenfreado da disseminação de fake news nas plataformas digitais poderia ser mais efetivamente combatida por regulamentações específicas que também protejam a liberdade de expressão.

A crescente expansão das tecnologias digitais e o uso disseminado da internet e redes sociais têm transformado significativamente a sociedade contemporânea, trazendo consigo uma série de desafios legais que exigem uma análise aprofundada no contexto jurídico brasileiro. Diante desse cenário, a necessidade premente de compreender e abordar as questões jurídicas relacionadas à privacidade, difamação, cyberbullying, disseminação de fake news e a responsabilidade das plataformas online, visando contribuir para o desenvolvimento de políticas e regulamentações mais eficazes nesse âmbito.

Primeiramente, é crucial destacar a importância da proteção da privacidade dos indivíduos em um ambiente digital altamente interconectado. A internet e as redes sociais possibilitam o compartilhamento constante de informações pessoais, criando desafios significativos no que diz respeito à preservação da intimidade e dos direitos

individuais. Nesse contexto, torna-se fundamental examinar como as legislações existentes no Brasil abordam a proteção da privacidade online e identificar lacunas ou necessidades de atualização para garantir uma tutela efetiva dos dados pessoais dos usuários.

Em suma, dada a relevância e urgência de aprofundar o debate sobre os desafios legais associados ao uso da internet e redes sociais no Brasil, é essencial que esse diálogo envolva especialistas em direito digital, legisladores, profissionais da tecnologia e a sociedade civil. A análise dessas questões jurídicas não apenas contribuirá para o avanço teórico do campo do direito digital, mas também fornecerá subsídios para a elaboração de políticas públicas e regulamentações mais adequadas e eficazes, capazes de proteger os direitos fundamentais dos indivíduos e promover um ambiente digital mais seguro e ético no país.

Embora a tecnologia tenha trazido avanços inegáveis, ela também gerou problemas complexos que desafiam as estruturas legais existentes. As leis atuais frequentemente não acompanham a rapidez das mudanças tecnológicas, deixando lacunas na proteção dos direitos fundamentais, como a privacidade e a honra. No cenário brasileiro, a falta de regulamentação específica para questões como o cyberbullying, a difamação online e a disseminação de fake news cria um ambiente propício para abusos e violações de direitos, ao mesmo tempo em que dificulta a responsabilização das plataformas digitais. Esse panorama evidencia a necessidade urgente de um marco jurídico robusto e atualizado que não apenas proteja os cidadãos, mas também assegure a liberdade de expressão de forma equilibrada e justa. É nesse contexto que a presente pesquisa se insere, buscando analisar e propor soluções que contribuam para o fortalecimento do direito digital no Brasil.

Os resultados desta pesquisa serão apresentados como trabalho de conclusão de curso em direito, sob a forma de artigo científico.

2 REDES SOCIAIS, COMPORTAMENTO HUMANO E O DIREITO

Desde os primórdios da humanidade, a interação entre os indivíduos tem sido uma necessidade fundamental para o desenvolvimento social, cultural e econômico

das sociedades. A evolução da comunicação humana acompanhou o avanço tecnológico, desde as formas mais rudimentares de comunicação oral e gestual até a complexidade das redes sociais e da internet. Essa jornada histórica testemunhou uma multiplicidade de desafios e oportunidades, especialmente com o advento da era digital e a crescente interconexão proporcionada pela internet e pelas redes sociais.

A comunicação sempre desempenhou um papel crucial na formação e manutenção das estruturas sociais. Nos tempos antigos, a comunicação era limitada a interações face a face e a mensagens transmitidas por mensageiros. Com o passar dos séculos, a invenção da escrita, da imprensa e, posteriormente, dos meios de comunicação eletrônicos, como o telefone e a televisão, revolucionou a maneira como as pessoas se comunicavam. No entanto, foi a chegada da internet e das redes sociais que trouxe uma transformação sem precedentes na comunicação humana.

As redes sociais, em particular, emergiram como plataformas poderosas que permitem a interação instantânea e global entre indivíduos. Essas plataformas não apenas facilitam a comunicação pessoal, mas também desempenham um papel significativo na disseminação de informações, na mobilização social e na formação de opiniões públicas. No entanto, essa nova era de comunicação digital também trouxe à tona uma série de questões jurídicas e éticas que precisam ser abordadas.

Do ponto de vista jurídico, as redes sociais apresentam desafios únicos em termos de privacidade, liberdade de expressão, responsabilidade civil e proteção de dados. A privacidade dos usuários é uma preocupação central, uma vez que as plataformas de redes sociais coletam e armazenam grandes quantidades de dados pessoais. A proteção desses dados é essencial para garantir que os direitos dos usuários sejam respeitados e que suas informações não sejam usadas de maneira inadequada ou sem consentimento.

Além disso, a liberdade de expressão nas redes sociais é um tema complexo. Embora essas plataformas ofereçam um espaço para a livre expressão de ideias e opiniões, elas também podem ser usadas para disseminar desinformação, discurso de ódio e outros conteúdos prejudiciais. A responsabilidade das plataformas de redes sociais em moderar e regular o conteúdo publicado por seus usuários é uma questão

delicada que envolve a necessidade de equilibrar a liberdade de expressão com a proteção contra abusos.

A responsabilidade civil das plataformas de redes sociais também é um aspecto importante a ser considerado. Em muitos casos, as plataformas podem ser responsabilizadas por conteúdos ilegais ou prejudiciais publicados por seus usuários. No entanto, a determinação da responsabilidade pode ser complexa, especialmente quando se trata de conteúdos gerados por terceiros. As leis e regulamentos que governam a responsabilidade das plataformas de redes sociais variam de país para país, e há um debate contínuo sobre a melhor maneira de abordar essa questão.

O advento da era digital trouxe consigo um vasto leque de desafios jurídicos no que tange à utilização da internet e das redes sociais. No contexto brasileiro, a rápida disseminação de informações, a interconexão global e a ubiquidade das plataformas online têm gerado uma série de questões legais complexas que demandam uma análise aprofundada.

A Teoria do Comportamento Planejado (TCP), desenvolvida pelo psicólogo Icek Ajzen, é uma extensão da Teoria da Ação Racional (TAR) (Fishbein e Ajzen, 1975) busca explicar como as intenções comportamentais são influenciadas por três fatores principais: atitude em relação ao comportamento, normas subjetivas e percepção de controle comportamental. Para Ajzen (1991), a intenção de realizar um comportamento é o preditor mais próximo da ação, sendo influenciada por esses três elementos. (Disponível em: <https://www.researchgate.net>. Acesso em: 30 de set. 2024).

A atitude em relação ao comportamento refere-se às crenças que a pessoa tem sobre as consequências de realizar a ação, que podem ser favoráveis ou desfavoráveis. As normas subjetivas estão relacionadas às crenças sobre a pressão social percebida para realizar ou não determinado comportamento. A percepção de controle comportamental reflete a percepção de facilidade ou dificuldade em executar o comportamento, influenciada pelas experiências passadas e pelos obstáculos antecipados. Assim, Ajzen afirma que "[...] quanto mais favorável for a atitude e as normas subjetivas, e maior o controle percebido sobre o comportamento, mais forte será a

intenção de realizá-lo" (1991, p. 181). A TCP tem sido amplamente aplicada em diversas áreas, como saúde, educação e negócios, para prever comportamentos individuais e coletivos.

A globalização desde as décadas passadas vem se tornando cada vez mais presente no vocabulário comum. Está saindo das manchetes de jornais e capas de revistas e chegando na palma das mãos dos cidadãos, e com simples “cliques” algo que teria um lapso temporal de vários dias ou até meses, e até anos para chegar ao seu destinatário, chega em questão de segundos em qualquer localidade do planeta. Mas essa mudança tem sido acompanhada de outros ramos? Um jargão comum ensinado já nos primeiros semestres do Curso de Direito é: “O Direito não socorre os que dormem.” Mas será que o Direito está acompanhando a globalização ou se encontra inerte com toda essa mudança de rumos da sociedade no que tange as Redes Sociais e sua segurança jurídica?

2.1 A PRIVACIDADE DIGITAL E O CONTEXTO JURÍDICO BRASILEIRO

Um dos principais desafios enfrentados diz respeito à proteção da privacidade dos usuários, uma vez que o ambiente digital frequentemente expõe dados pessoais a riscos de violações e uso indevido. Além disso, a disseminação de conteúdo difamatório e a prática de cyberbullying representam ameaças à integridade e à reputação das pessoas, levantando questões sobre responsabilidade civil e criminal.

Outro aspecto crítico é a propagação de fake news e a desinformação nas redes sociais, que podem ter impactos significativos na esfera política, social e econômica. A identificação de responsáveis por disseminar informações falsas e a mitigação de seus efeitos tornam-se desafios complexos para as autoridades e legisladores.

No contexto jurídico brasileiro, os desafios relacionados à internet e às redes sociais são diversos e multifacetados, abrangendo questões como privacidade, difamação, cyberbullying, disseminação de fake news e a responsabilidade das plataformas online. Esses desafios têm se intensificado com o aumento exponencial do uso da internet e das redes sociais, o que tem levado à necessidade de uma análise jurídica aprofundada para enfrentá-los de forma eficaz.

Em sua obra *O Direito na Sociedade da Informação IV*, Roberto Senise Lisboa elenca pontos fundamentais que vislumbram sobre atos políticos que interferem de maneira direta e indireta na manutenção da democracia e os princípios fundamentais.

E dois direitos fundamentais, neste momento, ganham especial atenção: a liberdade de expressão e a privacidade. No tocante a este último, os fatos e estudos recentes cada vez mais revelam que a tutela ao direito à privacidade tem tomado rumos extremamente preocupantes. Isto porque, compreendida como raiz das liberdades públicas ou direitos fundamentais de primeira dimensão, a privacidade na Rede é talvez um dos direitos mais vilipendiados pelos seus players, seja eles privados, que mercantilizam o tráfego de dados pessoais sem pudor, ou pertencentes ao poder público, evidenciando a cada dia a fragilidade dos cidadãos perante a vigilância do Estado.⁹ Mas é no concernente à liberdade de expressão que este trabalho se delimitará. Afinal, conforme se asseverou, a Internet sempre carregou esperanças de ser um ambiente de grande desenvolvimento das liberdades comunicacionais em geral. Contudo, tal contexto encontra-se ameaçado pelo excesso de poderes tanto dos provedores privados como de certos atores do poder público, que agem contrariamente à lei – quando não se locupletam das lacunas deixadas pela falta de regulação específica – para vulnerar sensivelmente as liberdades comunicacionais. (2020, p.181).

Em 2011, um caso tomou conta de todos os noticiários brasileiros. A atriz Carolina Dieckmann teve seu computador invadido por hackers, que, após não atender as demandas impostas pelos criminosos por meio de extorsão, divulgaram 36 fotos íntimas em redes sociais. O caso tomou uma proporção gigantesca e resultou na criação de uma nova legislação. A Lei 12.737, sancionada em 30 de novembro de 2012, estabelece penas para a invasão de privacidade, visando proteger a integridade digital e a intimidade das pessoas, além de coibir a disseminação de conteúdo sem consentimento.

A invasão do computador de Carolina Dieckmann e a subsequente divulgação de suas fotos íntimas sem autorização geraram um debate nacional sobre a necessidade de uma legislação específica para crimes cibernéticos. Segundo reportagem do G1, "O avanço na legislação aconteceu depois que a atriz Carolina Dieckmann, em maio de 2012, teve fotos copiadas do computador pessoal e divulgadas na internet, sem autorização". (Disponível em: <https://g1.globo.com>. Acesso em 28 set. 2024). Esse incidente destacou a vulnerabilidade das informações pessoais na era digital e a necessidade de proteção legal contra tais violações.

A Lei 12.737/2012, popularmente conhecida como Lei Carolina Dieckmann, foi um marco na legislação brasileira ao tipificar crimes cibernéticos. De acordo com o Portal da Câmara dos Deputados, a lei " [...] 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: <https://www2.camara.leg.br>. Acesso em: 27 set. 2024). Essa legislação foi essencial para preencher lacunas legais existentes e fornecer um mecanismo de proteção contra a invasão de dispositivos informáticos.

A importância da Lei Carolina Dieckmann reside não apenas na proteção da privacidade individual, mas também na promoção de um ambiente digital mais seguro. Conforme destacado por Wagner Francesco (2014) a lei " [...]dispõe sobre a tipificação criminal de delitos informáticos, tipificando condutas que não eram previstas, de forma específica, como infração penal". (Disponível em <https://www.jusbrasil.com.br>. Acesso em 27 de se. 2024). Isso inclui a invasão de dispositivos informáticos, como computadores, celulares e tablets, sem autorização, com o objetivo de obter, adulterar ou destruir dados ou informações.

Além disso, a Lei 12.737/2012 estabelece penas rigorosas para os infratores, visando dissuadir a prática de crimes cibernéticos. A legislação prevê penas de detenção de três meses a um ano, além de multa, para aqueles que invadirem dispositivos informáticos alheios, conectados ou não à internet, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo. Em casos onde a invasão resulta na obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido, a pena é aumentada de um sexto a um terço.

A promulgação da Lei Carolina Dieckmann representa um avanço significativo na luta contra a violência virtual e a exploração da imagem pessoal. Ela reflete a necessidade de adaptação das normas jurídicas às novas realidades tecnológicas e sociais, garantindo que os direitos fundamentais à privacidade e à intimidade sejam protegidos no ambiente digital. Como afirma Rebeca Duran (2013) no artigo do The Brazil Business, "[...] o crime levou a um novo projeto legal sancionado pela Presidente

Dilma Rousseff que entrou em vigor em 2013". (Disponível em: <https://thebrazilbusiness.com>. Acesso em 27 set. 2024).

Em suma, a Lei 12.737/2012 é um marco na legislação brasileira, proporcionando uma resposta legal robusta aos desafios impostos pela era digital. Ela não apenas protege a privacidade e a integridade digital dos indivíduos, mas também estabelece um precedente importante para a criação de futuras legislações voltadas à segurança cibernética e à proteção dos direitos dos cidadãos no ambiente virtual.

A privacidade na internet é um direito fundamental que enfrenta desafios significativos no contexto das redes sociais e da era digital. O rápido avanço da tecnologia tornou mais complexa a proteção da privacidade dos usuários, com a coleta indiscriminada de dados pessoais por parte das plataformas online e o compartilhamento desses dados com terceiros sem o devido consentimento. No Brasil, a proteção da privacidade é garantida pela Constituição Federal, pelo Marco Civil da Internet e pela Lei Geral de Proteção de Dados (LGPD), que estabelecem princípios e diretrizes para o tratamento adequado dos dados pessoais dos usuários.

A privacidade dos dados pessoais é um dos principais desafios legais no contexto das redes sociais. A Lei Geral de Proteção de Dados (LGPD), que entrou em vigor em setembro de 2020, estabelece diretrizes claras para o tratamento de dados pessoais no Brasil.

A Constituição Federal traz consigo diretrizes acerca dos direitos assegurados aos cidadãos, elencando-os de maneira concisa e explícita, sendo eles de caráter digital ou não. Nesse sentido, o caráter moral é norteado com direitos e garantias para que se mantenha os direitos e deveres preservados. O artigo 5º, XII da Carta Magna disserta sobre um dos princípios fundamentais no que cerne a privacidade:

Art.5.º, XII - É inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal (BRASIL, 1988).

Por ser uma rede global e de milhares de usuários, a internet acaba de se tornando um encaço quando se trata de individualizar e penalizar usuários que infringem as normas de privacidade de suas redes. Nos últimos anos o número de pessoas conectadas a rede global de acesso aumentou de maneira estrondosa.

O crescente número de usuários online se deu pelo isolamento social causado pela pandemia do Covid-19 que assolou o planeta em 2020. Com a quarentena necessária imposta por quase todos os governos, o tempo de uso das redes sociais e outros sites alcançou números estrondosos, quebrando recordes de dispositivos conectados à rede global de internet. Segundo Caio Belandi (2023), editor da Agência de Notícias do IBGE (Instituto Brasileiro de Geografia e Estatística), a proporção de usuários com faixa etária acima de 10 anos de idade aumentou de 84,7% em 2021 para 87,2% em 2023. Além disso, o PNAD Contínua afirma que 93,4% das pessoas utilizam a internet todos os dias. (Disponível em: <https://agenciadenoticias.ibge.gov.br>. Acesso em: 20 de set. 2024).

O livro “Direito Digital (2020)” de Patrícia Peck Pinheiro é uma referência importante nessa área, já que traz um entendimento claro e preciso para elucidação das mudanças de cenários que acontecem em todo tempo.

Desde os anos 1990 e principalmente após a expansão da internet no início dos anos 2000, fazia-se necessário tratar de forma estruturada da disciplina Direito Digital, que desde então teve um crescimento exponencial e permeou todas as demais áreas, de forma multidisciplinar. (Pinheiro, 2020, p. 15.)

O tratamento de dados tem como objetivo assegurar a segurança de ponta a ponta de todos os dados de usuários com acesso as redes.

Toda operação realizada com algum tipo de manuseio de dados pessoais: coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, edição, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração. (Pinheiro, 2020, p. 35).

A difamação é definida pelo Código Penal Brasileiro, no artigo 139, como a imputação de fato ofensivo à reputação de alguém. No contexto das redes sociais, a difamação assume características peculiares devido à velocidade e ao alcance das

informações disseminadas online. Um dos desafios da justiça brasileira é a quebra do anonimato, que nesses casos, é a base de apoio para criminosos do meio virtual

O ambiente digital amplifica a difamação devido à rapidez e ao alcance das redes sociais. A difamação e o cyberbullying são problemas sérios que afetam a integridade e a reputação das pessoas na internet e nas redes sociais. O anonimato proporcionado pela internet muitas vezes encoraja comportamentos agressivos e prejudiciais, tornando mais difícil responsabilizar os autores por seus atos. No contexto jurídico brasileiro, a difamação e o cyberbullying podem ser enquadrados como crimes contra a honra, sujeitos às penalidades previstas no Código Penal. Além disso, o Marco Civil da Internet estabelece mecanismos para a remoção de conteúdo difamatório e para a responsabilização dos provedores de internet que não cumpram com suas obrigações legais.

O sistema judiciário brasileiro tem adotado medidas duras e incisivas no que concerne o limite da liberdade de expressão sem ferir a honra de outrem. O equilíbrio entre esses temas tem ocasionado decisões favoráveis e desfavoráveis aos que tem buscado soluções no âmbito jurídico.

A LGPD (Lei nº 13.709/2018) é a principal legislação brasileira voltada para a proteção de dados pessoais. Ela estabelece diretrizes sobre como os dados devem ser coletados, armazenados e tratados, impondo responsabilidades tanto para as empresas quanto para os indivíduos que manipulam esses dados. A LGPD busca garantir a transparência e a segurança na manipulação de informações pessoais, visando proteger a privacidade dos cidadãos na era digital.

Apesar da LGPD, desafios persistem na aplicação prática da lei, especialmente no que se refere à fiscalização e ao cumprimento. O aumento de vazamentos de dados e a exploração indevida de informações pessoais pelas redes sociais são exemplos de questões ainda não plenamente resolvidas.

O grande impasse, é o de como definir uma barreira imaginária onde até que ponto é permitido se expressar sem que haja a quebra do direito constitucional previsto no artigo 5º, parágrafo IV: “É livre a manifestação do pensamento, sendo vedado

o anonimato”. É notório que de fato há respaldo na defesa do livre pensamento, todavia, o anonimato é o enalço para a liberdade ser plena em todos os sentidos. Em outras palavras seria dizer que: “Você é livre para dizer que quiser, porém, depende”.

2.2 O CYBERBULLYING NAS PLATAFORMAS DIGITAIS

Com um número expressivo de usuários diários, redes sociais ativas no território brasileiro como Instagram, Skype, Snapchat, Facebook, Whatsapp e entre outros, possuem termos e diretrizes de privacidade de dados que a grande maioria de seus assinantes não leem e nem fazem ideia do que está sendo aceito ao entrar nessas comunidades. Contando que a base do Direito e de qualquer outra troca de ideias e contratos é o princípio da boa-fé, mesmo concordando com os termos das plataformas digitais, ainda sim há a quebra das diretrizes com ataques virtuais.

O cyberbullying é a prática de atos agressivos, intencionais e repetitivos, realizados por meio da internet e das redes sociais, com o objetivo de causar sofrimento à vítima. Esse fenômeno tem impactos psicológicos profundos e pode levar a consequências graves, incluindo o suicídio. Os agressores muitas das vezes são adolescentes e até mesmo adultos que utilizam de perfis anônimos para disseminar ódio na internet.

O Brasil possui leis específicas que abordam o bullying e o cyberbullying. A Lei nº 13.185/2015, que institui o Programa de Combate à Intimidação Sistemática (Bullying), é um exemplo importante. Em seu artigo 1º, §1º define-se *bullying* todo ato de violência física ou psicológica, sendo intencional e repetitiva, ocorrendo sem motivação evidente.

Além disso, o Marco Civil da Internet (Lei nº 12.965/2014) estabelece que os provedores de serviços devem fornecer informações que permitam a identificação de usuários responsáveis por conteúdos ofensivos, após decisão judicial (Art. 10, § 3º). O marco civil contribuiu de maneira ímpar, pois possibilitou o debate e inclusão de leis importantes sobre o tema:

Ao regular inúmeros aspectos do dia a dia dos cidadãos, em constante diálogo com diversas leis que tratam das modernas relações sociais, como o Marco Civil da Internet e a Lei Geral de Proteção de Dados Pessoais, o Direito Digital ganhou a mais alta importância como disciplina autônoma. (Pinheiro, 2020, p. 25).

A liberdade de expressão tem respaldo pétreo na legislação, é o que define a liberdade de um povo, assim como, é o direito máximo de um Estado Democrático de Direito. A Lei nº 12.965 de 23 de abril de 2014, estabeleceu princípios direitos e garantias sobre o uso da internet no Brasil

Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos: I - inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação. (BRASIL. Lei Nº 12.965 de 23 de abril de 2014).

2.3 FAKE NEWS E A RESPONSABILIDADE DAS PLATAFORMAS

A disseminação de fake news representa um desafio significativo para a democracia e para a sociedade como um todo, especialmente no contexto das redes sociais e da internet. A propagação de informações falsas pode causar danos irreparáveis à reputação das pessoas e à estabilidade política do país. No Brasil, embora não exista uma legislação específica sobre fake news, diversas iniciativas têm sido adotadas para combater esse fenômeno, incluindo ações judiciais para a remoção de conteúdo falso, a promoção da educação midiática e a conscientização sobre a importância da verificação de fontes.

A responsabilidade das plataformas online pelo conteúdo disponibilizado em suas redes é um tema controverso no contexto jurídico brasileiro. Embora as plataformas sejam, em geral, protegidas pela legislação brasileira como meros intermediários, o Marco Civil da Internet estabelece que elas podem ser responsabilizadas civilmente por danos decorrentes de conteúdo gerado por terceiros se não cumprirem com as determinações legais, como a remoção de conteúdo ilegal após ordem judicial. Além disso, a LGPD impõe obrigações específicas às plataformas no que diz respeito à proteção dos dados pessoais dos usuários.

O Marco Civil da Internet (Lei nº 12.965/2014) é o principal instrumento legislativo brasileiro que regula os direitos e deveres no uso da internet. Ele estabelece uma

estrutura que visa garantir a neutralidade da rede, a privacidade e a liberdade de expressão no ambiente digital. No entanto, no que diz respeito à responsabilidade das plataformas, o art. 19 da lei adota o regime de responsabilidade subsidiária, ou seja, as plataformas só podem ser responsabilizadas civilmente por danos causados por terceiros se, após ordem judicial específica, não removerem o conteúdo ofensivo:

O provedor de aplicações de internet somente poderá ser responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomar as providências para, no âmbito e nos limites técnicos do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente. (BRASIL, 2014).

Outro marco legal relevante no contexto da responsabilidade das plataformas digitais é a Lei Geral de Proteção de Dados Pessoais (LGPD, Lei nº 13.709/2018). Embora a LGPD não trate diretamente do combate às fake news, a forma como as plataformas digitais lidam com os dados pessoais dos usuários tem implicações na disseminação de desinformação. A coleta massiva de dados pessoais e seu uso para direcionar publicidade personalizada, incluindo conteúdos políticos, foi central no escândalo da Cambridge Analytica, que evidenciou como dados de redes sociais podem ser manipulados para influenciar comportamentos eleitorais.

A Autoridade Nacional de Proteção de Dados (ANPD) tem a competência para fiscalizar e aplicar sanções às plataformas que descumprirem as regras estabelecidas pela LGPD. Nesse sentido, a ANPD pode atuar em casos onde a manipulação indevida de dados contribua para a disseminação de fake news, promovendo um maior controle sobre a forma como os dados são utilizados e como as plataformas conduzem suas práticas de direcionamento de conteúdo.

Além disso, as plataformas possuem mecanismos de controle interno, como algoritmos de moderação de conteúdo, que podem ser utilizados para identificar e limitar a disseminação de desinformação. Um dos principais pontos de crítica é que tais ferramentas podem, inadvertidamente, censurar conteúdos legítimos, comprometendo a liberdade de expressão garantida pelo artigo 5º, inciso IX, da Constituição Federal de 1988 (Brasil, 1988). Ademais, há o risco de reforço das chamadas "bolhas informacionais", que limitam a diversidade de pontos de vista e acabam por intensificar

a polarização social, um fenômeno agravado pelo funcionamento de sistemas que priorizam o engajamento sobre a pluralidade de informações.

O combate às fake news e a definição da responsabilidade das plataformas digitais são temas centrais para a manutenção da integridade democrática e a segurança informacional no Brasil. Embora o Marco Civil da Internet e a LGPD ofereçam um arcabouço jurídico relevante, ainda há lacunas na legislação brasileira que dificultam o enfrentamento adequado da desinformação. A adoção de políticas públicas que promovam a educação midiática, aliada a uma regulamentação mais eficaz, é essencial para conter os efeitos nocivos das fake news.

As plataformas digitais, como intermediárias do fluxo de informações, desempenham um papel crucial e devem ser responsabilizadas de forma proporcional e eficaz. O desenvolvimento de mecanismos de monitoramento e a maior transparência no uso de algoritmos de moderação são passos importantes na criação de um ambiente digital mais seguro e ético.

2.4 REDE SOCIAL X E O SUPREMO TRIBUNAL FEDERAL

No segundo semestre de 2024, repercutiu mundialmente a decisão monocrática do Ministro do STF (Supremo Tribunal Federal) Alexandre de Moraes, que determinou o bloqueio da rede social X (antigo Twitter) em todo território brasileiro, com multas chegando ao valor de R\$ 50.000,00 (cinquenta mil reais) para o usuário que contrariasse a decisão utilizando outros meios como de aplicativos VPNs que burlam o acesso através de rede privada virtual. Após a intimação o STF encaminhou uma ordem judicial junto a ANATEL (Agência Nacional de Telecomunicações), na qual foram solicitadas a suspensão imediata, completa e integral do funcionamento do X BRASIL INTERNET LTDA em todo o Brasil. (Disponível em: <https://noticias-stf-wp-prd.s3.sa-east-1.amazonaws.com>. Acesso em: 22 de set. 2024).

A decisão judicial se deu no dia 30 de agosto de 2024, devido ao descumprimento da ordem judicial que determinava o bloqueio de perfis que supostamente disseminavam Fake News, e publicações de mensagens de teor de extremo ódio contra autoridades e entidades onde afrontam o Estado Democrático de Direito brasileiro.

Com o não atendimento dos pedidos da Suprema Corte, decidiu então pelo bloqueio da rede social em todo o Brasil até que a empresa X do Brasil apresentasse um representante legal para a obtenção de esclarecimentos dos desrespeitos as decisões judiciais brasileiras, como a ocultação do ordenamento jurídico brasileiro.

O Relator Sr. Ministro Alexandre de Moraes através da Petição nº 12.404 em seu relatório esclarece as razões pelas quais levaram a intimação até o bloqueio da rede social X de Elon Musk:

A SUSPENSÃO IMEDIATA, COMPLETA E INTEGRAL DO FUNCIONAMENTO DO X BRASIL INTERNET LTDA em território nacional, até que todas as ordens judiciais proferidas nos presentes autos sejam cumpridas, as multas devidamente pagas e seja indicado, em juízo, a pessoa física ou jurídica representante em território nacional. No caso de pessoa jurídica, deve ser indicado também o seu responsável administrativo.

[...]

(3) A APLICAÇÃO DE MULTA DIÁRIA de R\$ 50.000,00 (cinquenta mil reais) às pessoas naturais e jurídicas que incorrerem em condutas no sentido de utilização de subterfúgios tecnológicos para continuidade das comunicações ocorridas pelo X, tal como o uso de VPN (virtual private network), sem prejuízo das demais sanções civis e criminais, na forma da lei. (BRASIL. Supremo Tribunal Federal, p 8.). (Disponível em: <https://portal.stf.jus.br>. Acesso em 22 de set. 2024).

Após tentativas de contato com representantes legais da rede social X, deu-se início ao julgamento de maneira Virtual na Primeira Turma do Supremo Tribunal Federal no dia 02 de setembro de 2024. A Sessão Virtual teve quatro votos que acompanharam o Relator, na qual foram os votos dos Min. Flávio Dino, Min. Cristiano Zanin, Min. Carmén Lúcia. Acompanhou o Relator com ressalvas o Min. Luiz Fux. O voto do Relator Min. Alexandre de Moraes seguiu da seguinte maneira:

DIANTE DE TODO O EXPOSTO, presentes os requisitos legais necessários, *fumus boni iuris* – consistente nos reiterados, conscientes e voluntários descumprimentos das ordens judiciais e inadimplemento das multas diárias aplicadas, além da tentativa de não se submeter ao ordenamento jurídico e Poder Judiciário brasileiros, para instituir um ambiente de total impunidade e “terra sem lei” nas redes sociais brasileiras, inclusive durante as eleições municipais de 2024 –, bem como o *periculum in mora* – consistente na manutenção e ampliação da instrumentalização da X BRASIL, por meio da atuação de grupos extremistas e milícias digitais nas redes sociais, com massiva divulgação de discursos nazistas, racistas, fascistas, de ódio, antidemocráticos, inclusive no período que antecede as eleições municipais de 2024, DETERMINO: (1) A SUSPENSÃO IMEDIATA, COMPLETA E INTEGRAL DO FUNCIONAMENTO DO “X BRASIL INTERNET LTDA” em território nacional, até que todas as ordens judiciais proferidas nos presentes autos sejam cumpridas, as multas devidamente pagas e seja indicado, em juízo, a pessoa física ou jurídica representante em território nacional. No caso de pessoa jurídica, deve

ser indicado também o seu responsável administrativo, O Presidente da Agência Nacional de Telecomunicações (ANATEL), CARLOS MANUEL BAI-GORRI deve ser intimado, inclusive por meios eletrônicos, para que adote IMEDIATAMENTE todas as providências necessárias para a efetivação da medida, comunicando-se essa CORTE, no máximo em 24 (vinte e quatro) horas. (2) A INTIMAÇÃO, para cumprimento no prazo de 5 (cinco) dias, devendo comunicar imediatamente o juízo, das empresas: (2.1) APPLE e GOOGLE no Brasil para que insiram obstáculos tecnológicos capazes de inviabilizar a utilização do aplicativo “X” pelos usuários do sistema IOS (APPLE) e ANDROID (GOOGLE) e retirem o aplicativo “X” das lojas APPLE STORE e GOOGLE PLAY STORE e, da mesma forma, em relação aos aplicativos que possibilitam o uso de VPN (‘virtual private network’), tais como, exemplificativamente: Proton VPN, Express VPN, NordVPN, Surfshark, TOTALVPN, Atlas VPN, Bitdefender VPN; (2.2) Que administram serviços de acesso a backbones no Brasil, para que neles insiram obstáculos tecnológicos capazes de inviabilizar a utilização do aplicativo “X”; (2.3) Provedoras de serviço de internet, na figura de seus Presidentes, exemplificativamente ALGAR TELECOM, OI, SKY, LIVE TIM, VIVO, CLARO, NET VIRTUA, GVT, etc..., para que insiram obstáculos tecnológicos capazes de inviabilizar a utilização do aplicativo “X”; e (2.4) Que administram serviço móvel pessoal e serviço telefônico fixo comutado, para que neles insiram obstáculos tecnológicos capazes de inviabilizar a utilização do aplicativo “X”; (3) A APLICAÇÃO DE MULTA DIÁRIA de R\$ 50.000,00 (cinquenta mil reais) às pessoas naturais e jurídicas que incorrerem em condutas no sentido de utilização de subterfúgios tecnológicos para continuidade das comunicações ocorridas pelo “X”, tal como o uso de VPN (‘virtual private network’), sem prejuízo das demais sanções civis e criminais, na forma da lei. Intime-se ELON MUSK, “TWITTER INTERNATIONAL UNLIMITED COMPANY” (CNPJ nº 15.493.642/0001-47), “T. I. BRAZIL HOLDINGS LLC” (CNPJ nº 15.437.850/0001-29), “X BRASIL INTERNET LTDA.” (CNPJ nº 16.954.565/0001-48), “STARLINK BRAZIL HOLDING LTDA.” (CNPJ nº 39.523.686/0001-30) e “STARLINK BRAZIL SERVIÇOS DE INTERNET LTDA.” (CNPJ nº 40.154.884/0001-53), inclusive por meios eletrônicos. Retiro o sigilo da presente decisão, tornando-a pública. Cumpra-se, imediatamente. Ciência, IMEDIATA, à Procuradoria-Geral da República”. Em face, porém, do caráter cautelar da decisão e da possibilidade da própria empresa X BRASIL INTERNET LTDA. ou de ELON MUSK, ao serem intimados, efetivarem o integral cumprimento das decisões judiciais, em decisão posterior, SUSPENDI A EXECUÇÃO DO REFERIDO ITEM 2, até que haja manifestação das partes nos autos, evitando eventuais transtornos desnecessários e reversíveis à terceiras empresas.

Diante de todo o exposto, VOTO NO SENTIDO DE REFERENDAR A DECISÃO no tocante à: (A) SUSPENSÃO IMEDIATA, COMPLETA E INTEGRAL DO FUNCIONAMENTO DO X BRASIL INTERNET LTDA em território nacional, até que todas as ordens judiciais proferidas nos presentes autos sejam cumpridas, as multas devidamente pagas e seja indicado, em juízo, a pessoa física ou jurídica representante em território nacional. No caso de pessoa jurídica, deve ser indicado também o seu responsável administrativo; (B) APLICAÇÃO DE MULTA DIÁRIA de R\$ 50.000,00 (cinquenta mil reais) às pessoas naturais e jurídicas que incorrerem em condutas para fraudar a decisão judicial, com a utilização de subterfúgios tecnológicos (como por exemplo o VPN, entre outros) para a continuidade de utilização e comunicações pelo “X”, enquanto durar a suspensão, sem prejuízo das demais sanções civis e criminais, na forma da lei.

É o voto. (BRASIL. Supremo Tribunal Federal, **Voto Min. Alexandre de Moraes**. p. 39 - p.42. (Disponível em: <https://portal.stf.jus.br>. Acesso em 22 de set. 2024).

A decisão tem gerado diversos debates jurídicos sobre o critério utilizado pelo Ministro Alexandre de Moares do Supremo Tribunal Federal, pois até mesmo entre

magistrados não há consenso até onde vai a imposição de limites para que não haja litígio entre liberdade de expressão e o ordenamento jurídico brasileiro. O fato é que no cenário atual, não há um martelo batido sobre a constitucionalidade da ação, visto que, não há uma jurisprudência formada sobre o assunto.

No entanto, após várias tentativas de acordo, no último dia 08 de outubro de 2024, houve então a conclusão do litígio entre a Rede Social X de Elon Musk e o STF. Após o pagamento da multa imposta pelo Relator o Sr. Ministro Alexandre de Moraes, a rede social voltou a operar em todo território nacional. Informações trazidas pelo site oficial do Supremo Tribunal Federal:

Empresa cumpriu condições estipuladas pelo relator, ministro Alexandre de Moraes, e a plataforma poderá voltar a ser utilizada pelos brasileiros. [...] O bloqueio da rede social havia sido determinado pelo ministro no dia 30/8. Na ocasião, ele determinou que a suspensão da rede social seria mantida até que as decisões judiciais da Corte fossem cumpridas. A medida foi referendada pela Primeira Turma do STF. Em 27/9, o X comprovou ter cumprido integralmente duas condicionantes para a retomada das atividades: o bloqueio de perfis que disseminavam informações falsas e a nomeação de um representante legal no país, exigência da legislação brasileira para o funcionamento de empresas estrangeiras no país. Depois disso, pagou integralmente as multas devidas, que totalizavam R\$ 28,6 milhões. (Disponível em: <https://noticias.stf.jus.br>. Acesso em: 13 de out. 2024).

3 CONSIDERAÇÕES FINAIS

A pesquisa abordou a profunda transformação que as novas tecnologias e o advento da era digital têm provocado na sociedade, especialmente no que se refere aos desafios jurídicos. A análise das questões relacionadas à privacidade, difamação, cyberbullying, fake news e responsabilidade das plataformas online evidenciou a necessidade urgente de adaptação e atualização das legislações brasileiras para acompanhar a rápida evolução do ambiente digital.

A internet, ao mesmo tempo em que amplia as possibilidades de comunicação e interação, expõe os indivíduos a riscos significativos, como a violação da privacidade e a difamação, que muitas vezes ocorrem em um contexto de anonimato. A propagação desenfreada de fake news e a prática de cyberbullying são problemas que afetam não apenas a honra e a integridade das pessoas, mas também a própria estabilidade

social e democrática do país. Esses desafios evidenciam a insuficiência das regulamentações atuais, que precisam ser revistas e fortalecidas para garantir a proteção eficaz dos direitos fundamentais.

A Constituição Federal de 1988, em seu artigo 5º, inciso X, consagra o direito à privacidade e à inviolabilidade da intimidação, vida privada, honra e imagem das pessoas, garantindo indenização em caso de violação. Ocorre que, no ambiente digital, a tutela desses direitos enfrentados dificuldades específicas. As redes sociais, por exemplo, permitem uma disseminação ampla e rápida de informações que, muitas vezes, podem escapar ao controle do usuário, sendo comum o compartilhamento de conteúdo pessoal sem o devido consentimento, o que reforça a necessidade de aprimoramento na legislação, principalmente não que tange à eficácia dos mecanismos de defesa dos direitos dos cidadãos no ambiente digital.

Em segundo lugar, a questão da difusão e do cyberbullying no ambiente online apresenta desafios tanto no campo civil quanto no penal. O Código Penal Brasileiro, em seus artigos 138 a 140, trata dos crimes contra a honra, abrangendo a calúnia, a difamação e a injúria. No entanto, o ambiente digital acrescenta uma dimensão de complexidade a esses crimes, uma vez que o anonimato e a facilidade de divulgação de informações podem amplificar os danos causados às vítimas. As redes sociais, em particular, têm se tornado palco de agressões verbais, ataques à confiança e disseminação de informações falsas, gerando graves consequências à honra e à dignidade das pessoas. O Marco Civil da Internet (Lei nº 12.965/2014), embora preveja diretrizes para responsabilização dos provedores de serviços de internet, ainda precisa de maior efetividade na identificação e proteção dos autores de tais crimes, especialmente no que tange à quebra do anonimato e à celeridade dos procedimentos judiciais.

O cyberbullying, especificamente, é uma prática crescente e preocupante, que tem gerado debates em diversas esferas, inclusive no Judiciário. A Lei nº 13.185/2015, que institui o Programa de Combate à Intimidação Sistemática (Bullying), menciona o bullying virtual como uma prática que deve ser combatida, mas a aplicação efetiva dessa ainda carece de instrumentos mais específicos. Além disso, é fundamental que o Marco Civil da Internet e a LGPD atuem em conjunto para garantir que os provedores

de serviços de internet adotem políticas efetivas de monitoramento e controle de conteúdo abusivo, forneçam informações que permitam a identificação dos responsáveis, sem que isso represente uma violação dos direitos fundamentais, como a liberdade de expressão.

Sendo assim, esta pesquisa incumbiu-se de responder ao problema central de como o advento tecnológico, com seus impressionantes avanços, pode ser equilibrado com o aumento dos crimes virtuais, a fim de garantir que os usuários possam desfrutar da internet e das redes sociais de maneira segura e confiável em todos os nichos. Através da análise das lacunas legais, dos desafios enfrentados na proteção dos direitos fundamentais, e da necessidade de regulamentações mais robustas, conclui-se que, embora a tecnologia traga inúmeros benefícios, é essencial que o desenvolvimento jurídico acompanhe essa evolução para assegurar um ambiente digital mais seguro e ético.

Dessa forma, a pesquisa contribui para a criação de soluções que possam minimizar os riscos e maximizar as oportunidades proporcionadas pela era digital, promovendo a segurança e a confiança necessárias para que todos possam usufruir plenamente dos recursos tecnológicos. Nesse sentido, é fundamental a adoção de medidas legislativas e regulatórias adequadas, bem como o fortalecimento dos mecanismos de fiscalização e cumprimento da lei, a fim de garantir uma internet e redes sociais que promovam o respeito aos direitos humanos e à dignidade das pessoas.

Outro ponto crucial discutido foi a propagação de notícias falsas e os impactos que a desinformação pode causar, principalmente no contexto de eleições e eventos políticos de grande relevância. A liberdade de expressão, garantida pelo artigo 5º, inciso IV, da Constituição Federal, é um direito fundamental que deve ser preservado. No entanto, o uso irresponsável desse direito, especialmente no ambiente digital, pode gerar prejuízos irreparáveis. A divulgação de informações falsas ou distorcidas pode influenciar o processo eleitoral, criar crises políticas.

Destaca-se a necessidade de políticas públicas educacionais para crianças em escolas, para que se desenvolva o hábito de uso correto das redes sociais já nas primeiras idades. O acesso ao Direito Digital já nas primeiras séries, será de grande

valia para o crescimento sustentável de ambientes digitais seguros e respeitáveis. O impacto disso a longo prazo, é a diminuição de registros de ocorrências de quebras de privacidade bem como os casos de difamação e o cyberbullying.

Além disso, a responsabilidade das plataformas online é um tema que demanda maior clareza e rigor na legislação. Embora essas plataformas sejam essenciais para a comunicação digital, elas também precisam ser responsabilizadas pelos conteúdos prejudiciais veiculados em suas redes, garantindo um equilíbrio entre a liberdade de expressão e a proteção contra abusos.

5 REFERÊNCIAS

AJZEN, Icek. The theory of planned behavior. *Organizational Behavior and Human Decision Processes*, v. 50, n. 2, p. 179-211, 1991. Disponível em: https://www.researchgate.net/publication/272790646_The_Theory_of_Planned_Behavior. Acesso em: 30 set. 2024.

BRASIL. BELANDI, Caio. Estatísticas Sociais (ed.). **161,6 milhões de pessoas com 10 anos ou mais de idade utilizaram a Internet no país, em 2022**. 2023. Disponível em: <https://agenciadenoticias.ibge.gov.br/agencia-noticias/2012-agencia-de-noticias/noticias/38307-161-6-milhoes-de-pessoas-com-10-anos-ou-mais-de-idade-utilizaram-a-internet-no-pais-em-2022#:~:text=A%20por%C3%A7%C3%A3o%20de%20pessoas%20com,62%2C1%25%20em%202022>. Acesso em: 20 set. 2024.

BRASIL. Casa Civil. Constituição 1988. Constituição da República Federativa do Brasil. 5 out. 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm. Acesso em: 18 abril. 2024.

BRASIL. Código de processo penal. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm. Acesso em: 22 junho. 2024.

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. Diário Oficial da União: seção 1, Brasília, DF, p. 1, 30 nov. 2012. Disponível em: <https://www2.camara.leg.br/legin/fed/lei/2012/lei-12737-30-novembro-2012-774695-norma-pl.html>. Acesso em: 27 set. 2024.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Marco Civil da Internet. Diário Oficial da União, Brasília, DF, 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 30 set. 2024.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União, Brasília, DF, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 30 set. 2024.

BRASIL. Superior Tribunal Federal. **STF autoriza retorno imediato do X e determina que Anatel adote providências para retomada do serviço**. Disponível em: <https://noticias.stf.jus.br/postsnoticias/stf-autoriza-o-retorno-imediato-do-x-e-determina-que-anatel-adote-providencias-para-a-retomada-do-servico/>. Acesso em: 13 de out. 2024.

BRASIL. Superior Tribunal Federal. Petição nº 12.404, Relatório do Ministro Alexandre de Moraes, 2024. Disponível em: <https://portal.stf.jus.br/processos/detalhe.asp?incidente=6888934>. Acesso: 22 setembro. 2024.

GRAELL, Fernanda; VINCAIX, Marcus. **Lei Carolina Dieckmann completa 10 anos como marco no combate a crimes cibernéticos**. 2022. Disponível em: <https://g1.globo.com/tecnologia/noticia/2022/12/02/lei-carolina-dieckmann-completa-10-anos-como-marco-no-combate-a-crimes-ciberneticos.ghhtml>. Acesso em: 28 set. 2024.

FRANCESCO, Wagner. **O que você precisa saber sobre a Lei 12.737/2012, conhecida como “Lei Carolina Dieckmann”**. 2014. Publicado por: Wagner Francisco. Disponível em: <https://www.jusbrasil.com.br/artigos/o-que-voce-precisa-saber-sobre-a-lei-12737-2012-conhecida-como-lei-carolina-dieckmann/152372896>. Acesso em: 27 set. 2024.

LISBOA, Roberto Senise. O Direito na Sociedade da Informação IV: Movimentos Sociais, Tecnologia e a Atuação do Estado. Almedina Brasil, 2020.
PINHEIRO, Patrícia Peck. Direito Digital. Saraiva Educação SA, 2021.

DURAN, Rebeca. **Digital Crime in Brazil**. 2013. Disponível em: <https://thebrazilbusiness.com/article/digital-crime-in-brazil>. Acesso em: 27 set. 2024.