

Curso de Graduação em Direito

Artigo Original

## **CRIMES DIGITAIS E OS LIMITES DA LIBERDADE DE EXPRESSÃO NA INTERNET NO BRASIL**

DIGITAL CRIMES AND THE LIMITS OF FREEDOM OF EXPRESSION ON THE INTERNET IN BRAZIL

**Wesley Alves Barros Pereira e Natacha Catarine dos Santos Medeiros<sup>1</sup>**

**Raimundo José de Oliveira Barros<sup>2</sup>**

<sup>1</sup> Alunos Bacharelados em Direito.

<sup>2</sup> Professor Especialista do Curso em Graduação em Direito

### **RESUMO**

Os autores Wesley Alves e Natacha Medeiros, visam explorar o presente artigo “Crimes Digitais e os limites da liberdade de expressão na internet no Brasil”, objetivando a compreensão desse direito fundamental, com ênfase no contexto digital, questionando a eficácia tanto das regulamentações e legislações quanto aos desafios de equilíbrio entre a liberdade de expressão e o lado sombrio da internet. Não obstante, conscientizar o público, esclarecendo os limites envolvidos, identificando os desafios presentes, promovendo discussões acerca do direito constitucional, oferecendo contribuições aos debates acadêmicos e fomentando a conscientização acerca dos Direitos Digitais.

**Palavras-Chave:** Crimes Digitais; Liberdade de Expressão; Regulamentação; Internet;

### **ABSTRACT**

The authors Wesley Alves and Natacha Medeiros aim to explore this article "Digital Crimes and the limits of freedom of expression on the internet in Brazil", aiming to understand this fundamental right, with an emphasis on the digital context, questioning the effectiveness of both regulations and legislation regarding the challenges of balancing freedom of expression and the dark side of the internet. However, raise public awareness, clarify the limits involved, identify the challenges present, promote discussions on constitutional law, offer contributions to academic debates and raise awareness about Digital Rights.

Contato: wesleyalves@advwesleyalves.com.br | natacha.medeiros0133@sounidesc.com.br

## **1. INTRODUÇÃO**

No mundo interconectado de hoje, a internet tornou-se parte integrante de nossas vidas diárias. Além de seus inúmeros benefícios, em contrapartida, a internet também serve como plataforma para atividades criminosas, gerando um crescimento exponencial dos crimes digitais.

É importante examinar os limites da liberdade de expressão na internet.

No Brasil, é cristalino o avanço da tecnologia e principalmente ao aumento dos casos dos crimes digitais. Por outro lado, embora haja um acréscimo considerável em relação aos crimes cibernéticos, deve-se analisar o impacto ao direito constitucional de liberdade de expressão.

Que este artigo seja uma fonte de informação valiosa para aqueles interessados em compreender os diversos aspectos relacionados a liberdade de expressão no contexto digital no Brasil.

Convida-se o leitor a mergulhar nessa análise crítica e a refletir sobre as implicações desse tema para a segurança pública e para a sociedade como um todo.

Boa leitura!

## 2. METODOLOGIA

O presente trabalho foi desenvolvido por meio de pesquisas qualitativas baseadas em análises das leis brasileiras, o diploma legal Código Penal Brasileiro – CPB, artigos, matérias de sites e normas legais existentes sobre o tema.

## 3. FUNDAMENTAÇÃO TEÓRICA

Na era digital em que vivemos, a tecnologia tem sido uma benção e uma maldição. Enquanto ela proporciona facilidades, conectividade global e avanços revolucionários em todas as áreas, também abre portas para uma nova ameaça: os Crimes Digitais.

Nesse cenário em constante evolução, criminosos encontram na magnitude virtual um território propício para explorar e cometer uma infinidade de delitos que transcendem fronteiras físicas e legais.

O crime digital, também conhecido como cibercrime, abrange um amplo espectro de atividades ilegais realizadas através da Internet e de dispositivos conectados, desde ataques cibernéticos contra sistemas governamentais e corporativos até fraudes financeiras, roubo de identidade, disseminação de *malware* e até mesmo a exploração de vulnerabilidades em redes sociais, o crime digital se tornou uma realidade inegável e preocupante em todo o mundo.

No âmbito jurídico brasileiro, os crimes digitais são tratados pelas seguintes leis: Lei sob nº. 12.737/2012, conhecida nacionalmente por Lei Carolina Dieckmann, que tipifica o delito de invasão de dispositivo informático; Lei sob nº. 13.185/2015, sendo a Lei que tipifica a conduta de *bullying*; Lei sob nº. 14.155/2021, sendo a Lei que define e torna mais grave os crimes de furto e estelionato praticados com o uso de dispositivos eletrônicos e comunicações; Lei sob nº. 13.441/2017, que prevê a

infiltração de agentes de polícia na internet com fulcro na investigação de crimes contra a dignidade sexual de crianças e adolescentes.

Além dessas leis específicas, existem outras normas legais que podem ser aplicadas aos crimes digitais, dependendo das circunstâncias e da natureza das ações criminosas. O Marco Civil da Internet, Lei sob nº. 12.965/2014, também estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil, incluindo questões relacionadas à privacidade, proteção de dados e responsabilidade dos provedores de serviços.

Outrossim, a liberdade de expressão é um direito constitucional que garante às pessoas o direito de expressar suas opiniões e ideias livremente, tal direito está tipificado na Constituição da República Federativa do Brasil.

Conforme estabelecido no artigo 5º da Constituição Federal:

“Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:

IV - é livre a manifestação do pensamento, sendo vedado o anonimato;”  
(BRASIL, 1988, cap. I. Art. 5. Inc. IV)

Na era da internet, esse direito se estende ao espaço virtual, permitindo que as pessoas expressem suas opiniões através de blogs, mídias sociais, fóruns e outras plataformas online. No entanto, a liberdade de expressão não é absoluta e pode encontrar limites legais e éticos.

Atualmente no Brasil, tem-se imposto limites na liberdade de expressão. Esses limites são muitas vezes pautados em princípios como o respeito aos direitos humanos, a proibição da disseminação de discurso de ódio, a proteção da privacidade e a prevenção de calúnias e difamações. Além disso, plataformas online também têm suas próprias políticas e termos de uso que podem impor restrições específicas à liberdade de expressão em seus espaços.

De maneira ampla, a liberdade de expressão está intrinsecamente ligada à manifestação de pensamento, ideologias e emoções, que são componentes essenciais da experiência humana.

O Direito à liberdade de expressão também vem assegurado através da Declaração Universal dos Direitos Humanos (DUDH), mais precisamente no art. 19.

Segundo Todos têm direito à liberdade de opinião e expressão, o direito de investigar e receber informações e opiniões, e o direito de disseminá-las, sem limitação de fronteiras, por quaisquer seja o meio de expressão (PINTO,2020).

Sendo assim, urge salientar a necessidade e a importância de leis e normas que assegurem a ordem da sociedade digital, punindo os infratores pela ilegalidade de seus atos, pois, a liberdade de expressão não deve desviar de sua idealização, garantindo o bem-estar e os avanços da sociedade brasileira (FERREIRA e WATANABE, 2022).

### 3.1 ENTENDENDO OS CRIMES DIGITAIS

Os crimes digitais referem-se a várias atividades ilegais cometidas usando a tecnologia digital ou pela internet. Esses crimes podem variar de *Hacking* e roubo de identidade a *cyberbullying* e assédio online. Com o avanço da tecnologia e a crescente dependência da sociedade em relação à internet, os crimes digitais tornaram-se uma preocupação significativa para indivíduos, empresas e governos, uma vez que o anonimato e a acessibilidade proporcionados pela internet tornaram mais fáceis para os indivíduos se envolverem em atividades criminosas.

De igual modo, a dependência da internet, haja vista que a evolução tecnológica trouxe à sociedade uma sujeição, uma vez que é utilizada 24hs do dia por grande parte dos cidadãos, de forma direta ou indireta, quando realiza transações bancárias/financeiras, interação social, entre outras formas.

No Brasil, o Governo Federal por meio do Decreto sob nº. 10.222/2020 lançou um plano tático de combate aos crimes cibernéticos, para proteger suas infraestruturas críticas, redes de computadores e dados contra ameaças cibernéticas.

Essa estratégia é essencial para proteger a infraestrutura crítica, a economia e a sociedade de ameaças cibernéticas em um mundo cada vez mais digitalizado. Ela envolve uma abordagem multidisciplinar que requer a colaboração de governos, empresas e sociedade civil.

### 3.1.1 Tipos de crimes digitais

Existem vários tipos de crimes digitais, também conhecidos como cibercrimes, que envolvem o uso da tecnologia e da internet para realizar atividades ilegais. Abaixo, conforme estudo realizado por <https://www.kaspersky.com> e <https://www.eset.com/us/>, colacionamos alguns dos principais tipos de crimes digitais:

1. **Phishing:** Ocorre quando um criminoso envia mensagens fraudulentas, geralmente por e-mail, fingindo ser uma entidade confiável para obter informações pessoais, como senhas e dados financeiros.
2. **Hacking:** Envolve a invasão não autorizada de sistemas de computadores, redes ou dispositivos para roubar informações, causar danos ou interromper serviços.
3. **Malware:** Refere-se a programas maliciosos, como vírus, *worms*, *trojans* e *ransomware*, que são projetados para danificar computadores, roubar informações ou bloquear o acesso a dados em troca de resgate.
4. **Roubo de Identidade:** Consiste em obter informações pessoais de terceiros para assumir sua identidade e cometer fraudes, como abrir contas bancárias, obter créditos ou fazer compras em nome da vítima.
5. **Cyberbullying:** É o uso de tecnologia para assediar, ameaçar ou intimidar outras pessoas, geralmente por meio de mensagens ofensivas, humilhação pública ou divulgação de informações pessoais.
6. **Fraude Financeira:** Engloba diversas práticas fraudulentas realizadas online, como golpes de Phishing, esquemas de pirâmide, fraudes de cartão de crédito e falsificação de transações financeiras.
7. **Difamação e Calúnia Online:** Compreende a disseminação de informações falsas e prejudiciais sobre alguém através da internet, podendo causar danos à reputação da vítima.
8. **Ameaças e Extorsão Online:** Inclui a utilização da internet para enviar ameaças ou extorquir dinheiro ou informações de uma pessoa ou organização.

**9. Pornografia Infantil Online:** Refere-se à criação, distribuição ou posse de material pornográfico envolvendo crianças, o que é estritamente ilegal em praticamente em todos os países.

**10. Violação de Direitos Autorais:** Envolve a distribuição não autorizada de material protegido por direitos autorais, como filmes, músicas ou software.

Esses são apenas alguns exemplos dos tipos de crimes digitais mais comuns, e novas formas de cibercrimes continuam surgindo à medida em que a tecnologia avança.

### 3.2 EVOLUÇÃO DAS NORMAS E SEUS IMPACTOS NOS CRIMES DIGITAIS

A evolução das normas e sua interação com os crimes digitais refletem a incessante busca por adequar o ordenamento jurídico às complexidades do mundo digital.

Preliminarmente, insta salientar que ao longo dos anos, o Brasil testemunhou o surgimento de leis e regulamentos que buscaram endereçar desafios específicos associados à criminalidade virtual, refletindo uma compreensão crescente da importância de proteção tanto de privacidade como da segurança cibernética.

Certamente, a evolução da esteira legal normativa na qual no Brasil, ficou estabelecido com a edição da Lei 12.965/2014 – Marco Civil da Internet. Esta legislação estabeleceu princípios fundamentais para a utilização da Internet no país, destacando a neutralidade da rede e a privacidade do usuário. Além disso, definiu parâmetros para a atuação estatal na preservação da segurança e na proteção de dados pessoais.

Posteriormente, com a edição da Lei sob nº. 14.155 implementada em 2021, foi possível assumir um papel central na regulamentação, onde modernizou o Código Penal Brasileiro e o Código de Processo Penal, visando enfrentar a conduta de invasão de dispositivos informáticos, ou seja, crimes cibernéticos. Isso demonstra a contínua preocupação legislativa em lidar com novas formas de criminalidade digital.

Os impactos gerados tanto pelo Marco Civil da Internet como pela lei sob nº. 14.155/2021, trouxe alterações ao Código Penal, possibilitando a tipificação de crimes de invasão de dispositivos informáticos e sua divulgação, sem autorização, de informações obtidas por meio de invasão.

Não obstante, a supracitada Lei prevê, ainda, o aumento de pena se o crime for cometido contra idoso ou vulnerável, ou se resultar em prejuízo econômico à vítima.

Assim sendo, o impacto dessas Leis reside na criação de dispositivos legais específicos que lidam com invasões de dispositivos informáticos, conferindo uma maior clareza na definição dos crimes virtuais e estabelecendo penalidades.

### **3.2.1 Marcos Legais**

No Brasil, a expressão digital é regulamentada por diversos marcos legais que tratam de diferentes aspectos relacionados a internet, proteção de dados, crimes cibernéticos, neutralidade de rede e outros temas.

Para enfrentar os crimes digitais e defender a Liberdade de expressão, governos de todo o mundo estabeleceram marcos legais, como legislação e acordos internacionais. Essas estruturas visam encontrar um equilíbrio entre proteger os direitos individuais a Liberdade de expressão e garantir a responsabilização daqueles que se envolvem em atividades criminosas online. Por exemplo, a Convenção sobre a Cibercriminalidade, adotada pelo Conselho da Europa, fornece orientações para combater a Cibercriminalidade, respeitando simultaneamente os direitos humanos.

Alguns dos principais marcos legais da expressão digital no Brasil incluem:

- **Marco Civil da Internet (Lei nº 12.965/2014):** É uma das legislações mais importantes relacionadas à expressão digital no Brasil. Ele estabelece princípios, direitos e deveres para o uso da internet no país. Alguns de seus pontos-chave incluem a proteção da privacidade, a neutralidade de rede, a responsabilidade de provedores de serviços online e a garantia da liberdade de expressão online.
- **Lei Geral de Proteção de Dados (Lei nº 13.709/2018 - LGPD):** A LGPD regula o tratamento de dados pessoais no Brasil, incluindo aqueles coletados e processados na internet. Ela estabelece regras para a proteção da privacidade e os direitos dos titulares de dados, bem como obrigações para as empresas que lidam com informações pessoais.

- **Lei de Direitos Autorais (Lei nº 9.610/1998):** Essa lei trata dos direitos autorais no contexto digital, incluindo questões relacionadas à proteção de obras intelectuais na internet e a responsabilidade de provedores de serviços online.
- **Lei de Crimes Eletrônicos (Lei nº 12.737/2012 - Lei Carolina Dieckmann):** Essa lei introduziu punições específicas para crimes como invasão de dispositivos e violação de correspondência eletrônica.
- **Lei do Cadastro Positivo (Lei nº 12.414/2011):** Ela regula o uso de informações financeiras e de crédito na internet, permitindo a criação do cadastro positivo.
- **Lei do Marco Legal das Startups (Lei Complementar nº 182/2021):** Essa legislação visa incentivar o desenvolvimento de startups no Brasil, incluindo medidas relacionadas a investimentos, contratação de trabalhadores e ambiente regulatório.
- **Leis Estaduais e Municipais:** Além das leis federais, algumas unidades federativas e municípios brasileiros também têm regulamentações específicas relacionadas a expressão digital, como leis que tratam de proteção de dados, regulamentação de aplicativos de transporte de usuários (*uber, cabify, indriver, 99pop*), entre outros.

É importante notar que a legislação está sujeita a mudanças e evoluções, especialmente na era digital em constante transformação. Portanto, é fundamental manter-se atualizado sobre as leis e regulamentos relacionados à expressão digital no Brasil, especialmente se você estiver envolvido em atividades online.

### 3.3 LIBERDADE DE EXPRESSÃO NA INTERNET

A liberdade de expressão é um direito fundamental que permite aos indivíduos expressarem seus pensamentos, opiniões e crenças sem censura ou punição. No entanto, como acontece com qualquer direito, existem limitações para garantir um equilíbrio entre a liberdade de expressão e outros direitos fundamentais, visto que se trata de um tema complexo que levanta questões fundamentais sobre democracia, pluralidade e responsabilidade.

A internet coloca desafios únicos ao conceito de liberdade de expressão devido a rápida disseminação de informações, a dificuldade em regular o conteúdo on-line e ao potencial de uso indevido.

Uma das características distintivas da era da internet é a rapidez com que as informações podem ser disseminadas globalmente. Isso tem transformado significativamente a maneira como as pessoas se comunicam e interagem, possibilitando um alcance muito mais amplo para expressão de ideias. Logo, essa rápida disseminação também levanta preocupações sobre a propagação de informações errôneas, discursos de ódio e conteúdo prejudicial que podem se espalhar de maneira viral. Logo, percebemos que essa liberdade não é absoluta e enfrenta desafios significativos.

Em um contexto positivo, a internet permite que vozes anteriormente silenciadas sejam ouvidas, promovendo diversidade de perspectivas e a participação da sociedade. Plataformas como *Facebook*, *Twitter* e grupos de *WhatsApp*, oferecem um terreno fértil para debates e diálogos, fortalecendo os alicerces da sociedade democrática. A liberdade de expressão na internet, é um meio vital para o empoderamento e a inclusão.

No entanto, é sabido que esse cenário trás desafios significativos, visto que ocorre disseminação de informações falsas e, por muita das vezes, discurso de ódio, no qual são ameaças sérias à integridade da liberdade de expressão. A viralização rápida de conteúdos enganosos pode influenciar percepções públicas e minar a confiança tanto na pessoa a que lhe dirige quanto na informação propriamente dita. Levantando, então, uma questão crucial sobre a responsabilidade das plataformas digitais na moderação do conteúdo, conhecido popularmente como 'termos de uso'.

A crescente preocupação com a desinformação levou muitos a defenderem a necessidade de uma moderação mais rigorosa. Contudo, esse caminho apresenta seus próprios riscos, incluindo o potencial para censura injusta e restrição indevida à liberdade de expressão. Encontrar um equilíbrio entre a moderação responsável e a preservação da liberdade é um desafio constante no nosso ordenamento jurídico, visto que conforme preconiza o art. 5º inciso IV da Carta Magna.

Conforme estabelecido no artigo 5º da Constituição Federal “Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:

IV - é livre a manifestação do pensamento, sendo vedado o anonimato;” (BRASIL, 1988, cap. I. Art. 5. Inc. IV)

É mister salientar que não se pode de forma alguma admitir que um direito constitucional seja mitigado com alegações frágeis, ou seja, conforme aduzido em rede nacional pelo atual Ministro da Justiça o Excelentíssimo Senhor Flavio Dino de Castro e Costa, quando verberou “você serão obrigados a mudarem os termos de uso; eu não estou preocupado com os termos de uso de vocês; à partir daqui se os senhores não mudarem os termos de uso, arquem com as consequências; o tempo de auto regulação, da liberdade de expressão como valor absoluto, que É UMA FRAUDE, que é uma falcatrua, este tempo acabou no Brasil, foi sepultado, tenham clareza disso; se os senhores não derem respostas que nós consideramos como compatíveis e ajustadas, nós iremos tomar as providencias que a lei determina; as senhoras e os senhores viveram o processo eleitoral do ano de 2022 no Brasil; adotem isso como referência; é o que nós faremos com os senhores”.

Logo, percebe-se que tal conduta e posicionamento do atual ministro da justiça vai contra os termos da Constituição de 1988, quando há garantia à Liberdade de Expressão e principalmente com as atribuições do cargo ocupado, uma vez que tem por finalidade a solução dos assuntos relacionados com a ordem jurídica, livre exercício dos poderes constituídos, nacionalidade, cidadania, direitos políticos, garantias constitucionais, segurança interna, defesa dos interesses da União, dentre outros.

#### 3.4 O LADO SOMBRIO DA EXPRESSÃO DIGITAL

Ao mesmo tempo em que a internet permite a liberdade de expressão, ela também facilita a proliferação de discurso de ódio, conteúdo extremista e desinformação. O anonimato fornecido pelas plataformas online permite que os indivíduos se envolvam em *cyberbullying*, assédio e difamação, levando a danos consideráveis para indivíduos e comunidades. Esse lado obscuro da expressão

digital ressalta a necessidade de estabelecer limitações para manter um ambiente online seguro e inclusivo.

O uso excessivo de redes sociais e a exposição constante a conteúdo digital podem ter impactos negativos na saúde mental, incluindo ansiedade, depressão e baixa autoestima, em razão disso, é importante tomar medidas para mitigar seus impactos negativos.

No entanto, também trouxe à tona algumas preocupações e desafios, que podem ser considerados o "lado sombrio" da expressão digital. Alguns desses desafios incluem:

- **Privacidade e Segurança:** O uso intensivo da internet muitas vezes requer a divulgação de informações pessoais. Isso pode resultar em preocupações com a privacidade, especialmente quando empresas coletam dados sem o consentimento adequado dos usuários. Além disso, a exposição a ameaças digitais, como *hackers*, *phishing* e roubo de identidade, pode comprometer a segurança online das pessoas.
- **Vício Digital:** O uso excessivo de dispositivos eletrônicos e redes sociais pode levar ao vício digital, afetando a saúde mental e o bem-estar das pessoas. O constante acesso à internet pode dificultar a desconexão e o descanso, levando ao estresse e à ansiedade.
- **Cyberbullying:** A facilidade de comunicação digital também trouxe à tona o problema do *cyberbullying*, que é o uso da internet para assediar, intimidar ou difamar outras pessoas. Isso pode ter consequências devastadoras para as vítimas, especialmente adolescentes.
- **Desinformação e Fake News:** A disseminação de informações falsas e desinformação nas redes sociais é um problema crescente. Isso pode influenciar a opinião pública, afetar a credibilidade das fontes de notícias e causar divisões na sociedade.
- **Isolamento Social:** Embora a internet tenha o potencial de conectar pessoas em todo o mundo, também pode levar ao isolamento social, à medida que as interações online substituem as interações face a face. Isso pode afetar a qualidade dos relacionamentos e a saúde emocional.

- **Dificuldades de Aprendizado:** A dependência excessiva de tecnologias digitais pode prejudicar a concentração e a capacidade de aprendizado, especialmente entre crianças e adolescentes.
- **Impacto Ambiental:** A produção e o descarte de dispositivos eletrônicos contribuem para a poluição ambiental e o esgotamento de recursos naturais.
- **Desigualdade Digital:** Nem todos têm igual acesso à expressão digital, o que pode criar desigualdades sociais e econômicas. A falta de acesso à internet e dispositivos eletrônicos pode limitar oportunidades educacionais e econômicas.

Portanto, embora a expressão digital tenha trazido muitos benefícios, é importante estar ciente desses desafios e trabalhar para abordá-los de maneira responsável, promovendo a segurança, a ética e a inclusão no ambiente digital, para garantir que a expressão digital ocorra em um ambiente mais seguro e saudável.

### 3.5 DESAFIOS PARA EQUILIBRAR A LIBERDADE DE EXPRESSÃO E A REGULAÇÃO DO CRIME DIGITAL

Muitos crimes digitais ocorrem devido à falta de conscientização e educação sobre segurança cibernética. Investir em programas de conscientização e educação pode ajudar a prevenir muitos crimes digitais antes mesmo que ocorram.

É importante mencionarmos sobre a aplicação das leis, tendo em vista que, estabelecer penas proporcionais para crimes digitais é um desafio. As penalidades devem ser eficazes o suficiente para desencorajar a criminalidade, mas não tão severas a ponto de violar os princípios de justiça e direitos humanos.

A aplicação da lei deve ser imparcial e justa, independentemente da origem étnica, gênero, orientação sexual ou outras características pessoais. A regulação do crime digital deve ser projetada para evitar discriminação e preconceito.

### 3.6 CONVENÇÃO AMERICANA DOS DIREITOS HUMANOS (PACTO DE SÃO JOSÉ DA COSTA RICA)

O pacto de San José da Costa Rica, formalmente conhecido como Convenção Americana sobre Direitos Humanos, não aborda especificamente os crimes digitais, pois foi adotado em 1969, período anterior à popularização da internet e das tecnologias digitais. No entanto, a Convenção estabelece princípios

gerais que podem ser aplicados ao contexto dos crimes digitais, especialmente no que diz respeito à proteção dos direitos humanos.

Por exemplo, o direito à privacidade é protegido pelo art. 11 da convenção, o que pode ser relacionado à proteção de dados pessoais e à inviolabilidade da correspondência eletrônica. Além disso, o art. 13 protege a liberdade de pensamento e expressão, o que é relevante para discussões sobre a liberdade na internet e os limites da censura online.

Para questões específicas sobre crimes digitais, outros instrumentos internacionais e legislações nacionais são mais diretamente aplicáveis, como a Convenção sobre o Cibercrime (Convenção de Budapeste), que o Brasil **não é signatário**, e o Marco Civil da Internet (Lei nº 12.965/2014), já citado no presente artigo, bem como o Código Penal Brasileiro, que tipifica delitos que podem ser cometidos por meios digitais

#### **4. CONSIDERAÇÕES FINAIS**

Os crimes digitais apresentam desafios significativos à liberdade de expressão na internet no Brasil. É imperativo que as sociedades encontrem um equilíbrio entre a proteção dos direitos individuais e a prevenção de danos ocasionados com as práticas dos cibercrimes. O marco legal, a legislação atual e o uso responsável da internet podem ajudar a combater os crimes digitais, salvaguardando ao mesmo tempo a liberdade de expressão. Alcançar esse equilíbrio é crucial para garantir um ambiente online seguro e inclusivo para todos.

Por fim, a discussão sobre crimes digitais e os limites da liberdade de expressão na internet no Brasil requer a participação de diversas partes interessadas, incluindo governo, empresas de tecnologia, sociedade civil e usuários, com o objetivo de garantir a segurança e o respeito pelos direitos humanos no cenário digital, salvaguardando os direitos fundamentais conforme a Constituição Federal de 1988.

## REFERÊNCIAS

BRASIL. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/ato2015-2018/2015/lei/l13185.htm](https://www.planalto.gov.br/ccivil_03/ato2015-2018/2015/lei/l13185.htm). Acessado em 31.ago.2023.

Artigo 13. Liberdade de pensamento e de expressão. Autor: Supremo Tribunal Federal – STF – Disponível em: <https://www.stf.jus.br/arquivo/cms/jurisprudencialInternacional/anexo/Artigo13.pdf>. Acessado em 10/11/2023 às 01h45min.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil** – Brasília, DF: Presidência da República [2023] Disponível em: [https://www.planalto.gov.br/ccivil\\_03/constituicao/constituicao.htm](https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm). Acessado em 01.ago.2023 às 02h14min.

BRASIL. Decreto nº. 10.222/2020 – Disponível em [https://www.planalto.gov.br/ccivil\\_03/ato2019-2022/2020/decreto/d10222.htm](https://www.planalto.gov.br/ccivil_03/ato2019-2022/2020/decreto/d10222.htm). Acessado em 02.08.2023 às 08h49min.

BRASIL. **Lei 12.737 de 30 de novembro de 2012. (Lei Carolina Dieckmann)**. 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, ano 232 p. 1, col. 3 Disponível em: [https://www.planalto.gov.br/ccivil\\_03/\\_ato2011-2014/2012/lei/l12737.htm](https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm). Acessado em 31.ago.2023.

BRASIL. **Lei 13.185 de 6 de novembro de 2015.** (Lei Antibullying). Institui o Programa de Combate à Intimidação Sistemática (Bullying). Diário Oficial da União:

BRASIL. Lei 13.441/2017 – Disponível em [https://www.planalto.gov.br/ccivil\\_03/Ato2015-2018/2017/Lei/L13441.htm](https://www.planalto.gov.br/ccivil_03/Ato2015-2018/2017/Lei/L13441.htm). Acessado em 01. ago.2023

BRASIL. Lei 14.155/2021 – Disponível em [https://www.planalto.gov.br/ccivil\\_03/ato2019-2022/2021/lei/l14155.htm](https://www.planalto.gov.br/ccivil_03/ato2019-2022/2021/lei/l14155.htm). Acessado em 31. ago.2023

BRASIL. Lei Marco civil – Disponível em: [https://www.planalto.gov.br/ccivil\\_03/ato2011-2014/2014/lei/l12965.htm](https://www.planalto.gov.br/ccivil_03/ato2011-2014/2014/lei/l12965.htm) Acessado em 01.08.2023 às 02h02min.

BRASIL. Lei nº 13.709/2018- [https://www.planalto.gov.br/ccivil\\_03/ato2015-2018/2018/lei/l13709.htm](https://www.planalto.gov.br/ccivil_03/ato2015-2018/2018/lei/l13709.htm)[https://www.planalto.gov.br/ccivil\\_03/ato2015-2018/2018/lei/l13709.htm](https://www.planalto.gov.br/ccivil_03/ato2015-2018/2018/lei/l13709.htm)- Acessado em 13/09/2023 às 09h02min.

BRASIL. Lei nº 9.610/1998- [https://www.planalto.gov.br/ccivil\\_03/leis/l9610.htm](https://www.planalto.gov.br/ccivil_03/leis/l9610.htm)- Acessado em 13/09/2023 às 09h33min.

BRASIL. Projeto de Lei nº. 3.463/2023 – Disponível em: <https://www12.senado.leg.br/noticias/materias/2021/05/28/lei-com-penas-mais->

[duras-contra-crimes-ciberneticos-e-sancionada](#). Acessado em 01.09.2023 às 18h51min.

Da moderação de conteúdo à liberdade de expressão: até onde e de que forma regular? - Disponível em: <https://irisbh.com.br/da-moderacao-de-conteudo-a-liberdade-de-expressao-ate-onde-e-de-que-forma-regular/> Acessado em 11/09/2023 às 15h53min.

Eset. Furto de Identidade – Disponível em <https://www.eset.com/br/furto-identidade/>. Acessado em 01.08.2023 às 03h30min.

História do Ransomware – Disponível em: <https://br.malwarebytes.com/ransomware/>. Acessado em 01.08.2023 às 03h17min.

<https://stats.cert.br/phishing/#categorias-all> Acessado em 22/11/2023 às 14h44min.

<https://www12.senado.leg.br/noticias/materias/2021/05/28/lei-com-penas-mais-duras-contra-crimes-ciberneticos-e-sancionada#:~:text=A%20lei%20acrescentao%20C%C3%B3digo,a%20oito%20anos%20e%20multa.-> Acessado em 12/09/2023 às 23h10min.

Kaspersky. Roubo de Identidade e Fraude de Identidade: O Que Fazer se a Sua Identidade For Roubada – Disponível em <https://www.kaspersky.com.br/resource-center/threats/what-to-do-if-your-identity-is-stolen-a-step-by-step-guide>. Acessado em 01.08.2023 às 03h44min.

Lado negro da Internet esconde fraudes, pedofilia e experimentos humanos-<https://canalcienciascriminais.com.br/lado-negro-da-internet-esconde-fraudes-pedofilia-e-experimentos-humanos/> - Acessado em 11/09/2023 às 16h12min.

Lei com penas mais duras contra crimes cibernéticos é sancionada-Senado Federal, Convenção Sobre o Crime Cibernético, 18 de dezembro de 2021 – Disponível em <https://legis.senado.leg.br/norma/35366124/publicacao/35367771>. Acessado em 04h15min.

Zamora, Wendy. Sob o capuz: por que dinheiro, poder e ego levam hackers ao cibercrime – Disponível em: <https://www.malwarebytes.com/blog/news/2018/08/under-the-hoodie-why-money-power-and-ego-drive-hackers-to-cybercrime>. Acessado em 01.08.2023 às 02h49min.