

MARCO CIVIL DA INTERNET: CRIMES CONTRA A PROTEÇÃO DA INTIMIDADE

BRAZIL'S INTERNET BILL OF RIGHTS: CRIMES AGAINST THE PROTECTION OF INTIMACY AND PRIVACY

Victoria Beatriz da Silva Pizzano¹

Williane Tibúrcio Facundes²

PIZZANO, Victoria Beatriz da Silva; FACUNDES, Williane Tibúrcio. **Marco Civil da Internet**: crimes contra a proteção da intimidade. 23 páginas. Trabalho de Conclusão de Curso de graduação em Direito – Centro Universitário UNINORTE, Rio Branco. 2026.

RESUMO

O presente Trabalho de Conclusão de Curso tem como objetivo analisar o papel do Marco Civil da Internet na proteção da intimidade e da privacidade dos usuários no ambiente digital, com enfoque nos crimes que violam esses direitos fundamentais. Diante do avanço tecnológico e da ampliação do uso da Internet, observa-se o aumento significativo de condutas ilícitas que envolvem a invasão de dispositivos eletrônicos, a divulgação não autorizada de dados pessoais e o assédio virtual. Nesse contexto, o estudo busca compreender como o ordenamento jurídico brasileiro, especialmente a Lei nº 12.965/2014 (Marco Civil da Internet), o Código Penal e a Lei Geral de Proteção de Dados, atuam na tutela da intimidade. A pesquisa aborda o conceito jurídico de intimidade, sua relevância na era digital e os principais tipos de crimes praticados no meio virtual, analisando também as consequências jurídicas nas esferas civil e penal. Além disso, são examinados casos emblemáticos e entendimentos jurisprudenciais que contribuíram para o fortalecimento da proteção da privacidade no Brasil. Por fim, o trabalho apresenta propostas de aprimoramento legislativo e destaca a importância da educação digital e do fortalecimento das instituições de fiscalização como medidas essenciais para a efetiva proteção da intimidade dos indivíduos no ambiente online.

Palavras-chave: Marco Civil da Internet; intimidade; privacidade; crimes digitais; proteção de dados;

ABSTRACT

This Undergraduate Thesis aims to analyze the role of the Brazilian Internet Bill of Rights (Marco Civil da Internet) in the protection of intimacy and privacy of users in the

¹ Discente do 9º período do Curso de Bacharelado em Direito pelo Centro Universitário UNINORTE.

² Docente do Centro Universitário Uninorte. Graduada em Direito pela U:VERSE. Especialista em Psicopedagogia pela Universidade Várzea-grandense e Direito Digital e Educação Especial e Inclusiva pela Faculdade Metropolitana. Graduada em Letras Vernáculas pela Universidade Federal do Acre - UFAC.

digital environment, with emphasis on crimes that violate these fundamental rights. In view of technological advancement and the increasing use of the Internet, there has been a significant growth in illicit practices involving the invasion of electronic devices, unauthorized disclosure of personal data, and online harassment. In this context, the study seeks to understand how the Brazilian legal system, especially Law No. 12,965/2014 (Brazilian Internet Bill of Rights), the Criminal Code, and the General Data Protection Law, operates to safeguard intimacy. The research addresses the legal concept of intimacy, its relevance in the digital era, and the main types of crimes committed in virtual environments, also analyzing the legal consequences in both civil and criminal spheres. Furthermore, emblematic cases and judicial precedents are examined, highlighting their contribution to strengthening privacy protection in Brazil. Finally, the study presents proposals for legislative improvement and emphasizes the importance of digital education and the strengthening of supervisory institutions as essential measures for the effective protection of intimacy in the online environment.

Keywords: Brazilian Internet Bill of Rights; intimacy; privacy; digital crimes; data protection;

INTRODUÇÃO

A Internet tornou-se parte essencial da vida cotidiana, sendo utilizada para comunicação, trabalho, estudo e acesso à informação, o que transformou significativamente as relações sociais e jurídicas. Com o crescimento do uso das tecnologias digitais, também aumentaram os riscos relacionados à exposição indevida de informações pessoais e à violação da intimidade dos usuários. A facilidade de compartilhar conteúdos e dados no ambiente virtual contribuiu para o surgimento de diversas práticas ilícitas, como a invasão de dispositivos eletrônicos, a divulgação não autorizada de dados pessoais, o assédio online e outras formas de ataques à privacidade. Esses comportamentos atingem diretamente direitos fundamentais previstos na Constituição Federal de 1988, especialmente aqueles relacionados à intimidade, à vida privada, à honra e à imagem das pessoas. Diante desse cenário, tornou-se necessária a criação de normas capazes de regular o uso da Internet e garantir maior proteção aos usuários. Nesse contexto, foi instituído o Marco Civil da Internet, por meio da Lei nº 12.965/2014, que estabeleceu princípios, direitos e deveres para o uso da rede no Brasil, buscando promover um ambiente digital mais seguro e equilibrado. Além disso, outras legislações, como a Lei Geral de Proteção de Dados e dispositivos do Código Penal, passaram a complementar essa proteção, especialmente no combate aos crimes digitais. O presente trabalho tem como objetivo analisar a importância do Marco Civil da Internet na proteção da intimidade, com foco

nos crimes praticados no ambiente digital, bem como compreender as consequências jurídicas dessas condutas. O tema se mostra relevante diante do aumento dos casos de violação da privacidade e dos impactos que essas práticas causam na vida das vítimas, demonstrando a necessidade de constante atualização e aprimoramento das normas jurídicas voltadas à proteção da intimidade na era digital.

1 O MARCO CIVIL DA INTERNET

Neste capítulo, vamos apresentar o Marco Civil da Internet, que é uma lei muito importante para o uso da Internet no Brasil. Essa lei foi criada para garantir direitos e deveres para os usuários, provedores e o governo, tornando a Internet um ambiente mais seguro, justo e democrático. O Marco Civil estabelece princípios como a neutralidade da rede, a proteção da privacidade e a liberdade de expressão, que são fundamentais para que todos possam acessar a Internet de forma livre e sem discriminação. Além disso, essa lei define regras sobre como os dados dos usuários devem ser tratados e quais responsabilidades os provedores têm em relação ao conteúdo que circula na rede. Neste capítulo, vamos entender melhor o que é o Marco Civil da Internet, por que ele foi criado e quais são os seus principais pontos.

1.1 HISTÓRICO E EVOLUÇÃO LEGISLATIVA

A ideia de criar o Marco Civil começou por volta de 2009, quando o governo e especialistas perceberam que a Internet estava crescendo muito no Brasil e precisava de regras próprias. Houve uma consulta pública online, o que foi bem inovador, pois qualquer pessoa podia dar opinião sobre o que a lei deveria ter. Depois de muitos debates no Congresso, o texto foi aprovado em 2014. Um ponto importante é que ele surgiu em um momento em que também se discutia crimes cibernéticos, mas o objetivo do Marco Civil não era punir, e sim garantir direitos e estabelecer princípios básicos para o funcionamento da rede. Desde então, a lei já recebeu atualizações, principalmente para lidar com a proteção de dados e com novas tecnologias que mudaram a forma como usamos a Internet.

1.2 PRINCÍPIOS FUNDAMENTAIS

Entre os princípios do Marco Civil, alguns se destacam. A neutralidade da rede é um deles: significa que as operadoras de Internet não podem dar prioridade para

um site ou aplicativo em detrimento de outro, mantendo a Internet igual para todos. Outro princípio é a proteção da privacidade e dos dados pessoais, garantindo que informações dos usuários só sejam usadas com consentimento e de forma transparente. Há também a liberdade de expressão, que protege o direito de cada pessoa se manifestar online, mas deixando claro que quem publica é responsável pelo que escreve. Além disso, o acesso à Internet é visto como essencial para o exercício da cidadania, reforçando a ideia de que ela é um serviço básico.

No geral, o Marco Civil da Internet é uma lei que tenta equilibrar direitos e deveres. Ele não é perfeito e precisa ser constantemente revisado por causa das mudanças rápidas no mundo digital, mas foi um passo importante para que a Internet brasileira seja mais segura, livre e democrática.

1.2.1 Neutralidade da Rede

A neutralidade da rede é um princípio fundamental para o funcionamento da Internet como a conhecemos hoje. Ela garante que todos os dados que trafegam pela rede sejam tratados de forma igualitária, sem que os provedores de Internet possam privilegiar ou bloquear determinados conteúdos, serviços ou aplicações. Isso significa que, independentemente do site ou serviço que o usuário queira acessar, a velocidade e a qualidade da conexão devem ser as mesmas.

Sendo assim, um provedor não pode deixar o acesso a um serviço de streaming mais lento para favorecer outro concorrente que pague mais. A neutralidade da rede é importante porque promove a liberdade de expressão, a inovação e a concorrência justa entre empresas. Sem esse princípio, os provedores poderiam controlar o que os usuários veem e acessam, o que poderia prejudicar a diversidade de informações e o acesso democrático à Internet. No Brasil, a neutralidade da rede foi garantida pelo Marco Civil da Internet, que entrou em vigor em 2014, e que é considerado um marco legal para a proteção dos direitos dos usuários na Internet.

1.2.2 Privacidade e Proteção de Dados Pessoais

A privacidade e a proteção dos dados pessoais são temas cada vez mais relevantes na sociedade atual, principalmente devido ao crescimento do uso da Internet e das tecnologias digitais. Dados pessoais são informações que identificam ou podem identificar uma pessoa, como nome, endereço, CPF, dados bancários, entre

outros. Com a digitalização, muitas dessas informações são coletadas, armazenadas e utilizadas por empresas e governos para diferentes finalidades, como marketing, análise de comportamento e prestação de serviços.

Por isso, é fundamental que existam regras claras para garantir que esses dados sejam tratados com segurança e que os direitos dos usuários sejam respeitados. A Lei Geral de Proteção de Dados (LGPD), que entrou em vigor no Brasil em 2020, é a principal legislação que regula o uso de dados pessoais. Ela estabelece direitos para os titulares dos dados, como o direito de acesso, correção e exclusão das informações, e obrigações para as empresas, que devem garantir a transparência e a segurança no tratamento desses dados. A proteção da privacidade é essencial para evitar abusos, fraudes e garantir a confiança dos usuários no ambiente digital.

1.3 ESTRUTURA NORMATIVA E PRINCIPAIS DISPOSITIVOS

A estrutura normativa que regula o uso da Internet no Brasil é composta por diversas leis e regulamentos que buscam proteger os direitos dos usuários e estabelecer responsabilidades para os provedores de serviços e o Estado. O principal marco legal é o Marco Civil da Internet (Lei nº 12.965/2014), que define princípios, garantias, direitos e deveres para o uso da Internet no país. Entre os seus principais dispositivos estão a garantia da neutralidade da rede, a proteção da privacidade e dos dados pessoais, a liberdade de expressão e a responsabilidade dos provedores em relação ao conteúdo gerado pelos usuários. Além do Marco Civil, a Lei Geral de Proteção de Dados (LGPD - Lei nº 13.709/2018) complementa essa estrutura ao focar especificamente na proteção dos dados pessoais, estabelecendo regras para coleta, armazenamento, tratamento e compartilhamento dessas informações. Outras normas importantes incluem o Código de Defesa do Consumidor, que protege os usuários em relações comerciais online, e as regulamentações da Agência Nacional de Telecomunicações (Anatel), que regulam os serviços de telecomunicações e Internet no país. Essa estrutura normativa é essencial para garantir uma Internet segura, acessível e justa, promovendo o desenvolvimento tecnológico e a proteção dos direitos dos cidadãos.

2 INTIMIDADE E PROTEÇÃO DE DADOS NO CONTEXTO DIGITAL

Como podemos analisar a intimidade e a proteção dos dados pessoais no

mundo digital, que é um assunto muito importante hoje em dia. Com o avanço da tecnologia e o uso cada vez maior da Internet, muitas informações pessoais acabam sendo compartilhadas ou armazenadas em ambientes digitais. Por isso, entender o que é intimidade e como proteger esses dados é fundamental para garantir que a privacidade das pessoas seja respeitada. Vamos ver o que significa intimidade, como ela pode ser afetada no contexto digital e por que é tão importante cuidar dessas informações para evitar problemas como invasão de privacidade, fraudes e outros riscos. Esse tema é essencial para que possamos usar a Internet de forma mais segura e consciente.

2.1 CONCEITO DE INTIMIDADE

A intimidade é um direito fundamental que diz respeito à esfera privada de cada indivíduo, envolvendo aspectos pessoais, sentimentos, pensamentos e informações que a pessoa deseja manter reservados. No contexto jurídico, a intimidade está relacionada à proteção da vida privada contra invasões indevidas, garantindo que ninguém possa expor ou utilizar informações pessoais sem consentimento. Com o avanço da tecnologia e a popularização da Internet cada vez maior o conceito de intimidade ganhou novas dimensões, pois muitas informações que antes eram restritas ao ambiente físico passaram a ser compartilhadas ou armazenadas no meio digital. Isso inclui mensagens, fotos, dados pessoais e até mesmo hábitos de navegação. A proteção da intimidade, portanto, envolve assegurar que essas informações não sejam acessadas, divulgadas ou utilizadas de forma indevida, preservando a dignidade e a autonomia do indivíduo. No livro *A Evolução da Internet: uma perspectiva histórica*, Lins, (Lins, 2013, pág. 12) descreve sobre o avanço na tecnologia contínuo e cada vez mais rápido:

Em 1989, a Internet brasileira começa a ser implantada como uma infraestrutura de comunicação para fins acadêmicos. O *backbone* da rede, que recebeu o nome de Rede Nacional de Pesquisas – RNP, foi complementado com redes estaduais, custeadas com recursos das fundações estaduais de amparo à pesquisa. A rede cresceu rapidamente. Em 1996, já contava com 7.500 domínios. Em 2000, com 170 mil. Em 2006, um milhão. Em 2014, três milhões e meio. (2013).

2.2 A IMPORTÂNCIA DA PROTEÇÃO DA INTIMIDADE NA ERA DIGITAL

Na era digital, a proteção da intimidade tornou-se ainda mais importante devido à facilidade com que dados pessoais podem ser coletados, armazenados e compartilhados. A Internet e as redes sociais permitem que informações pessoais sejam divulgadas rapidamente e para muitas pessoas, o que pode gerar riscos como exposição indevida, discriminação, fraudes e até mesmo crimes virtuais.

Além disso, empresas e governos coletam uma grande quantidade de dados para diferentes finalidades, o que exige regras claras para garantir que esses dados sejam usados de forma ética e segura. A proteção da intimidade na era digital é essencial para preservar a liberdade individual, evitar abusos e garantir que as pessoas tenham controle sobre suas informações pessoais. Leis como a Lei Geral de Proteção de Dados (LGPD) no Brasil são fundamentais para estabelecer direitos e deveres nesse sentido, promovendo um ambiente digital mais seguro e respeitoso para todos.

2.3 LEGISLAÇÃO COMPARADA SOBRE PROTEÇÃO DA INTIMIDADE

A proteção da intimidade e dos dados pessoais é um tema que tem ganhado destaque em todo o mundo, principalmente com o crescimento do uso da Internet e das tecnologias digitais. Diversos países criaram legislações específicas para garantir a privacidade dos cidadãos e regular o tratamento das informações pessoais. Um dos exemplos mais conhecidos é o Regulamento Geral sobre a Proteção de Dados (GDPR), adotado pela União Europeia em 2018. O GDPR é considerado uma das legislações mais rigorosas e abrangentes, estabelecendo regras claras sobre o consentimento do usuário, o direito ao esquecimento, a portabilidade dos dados e a obrigação das empresas em proteger as informações pessoais.

Além da União Europeia, outros países também possuem leis importantes, como a Lei de Privacidade do Consumidor da Califórnia (CCPA), nos Estados Unidos, que oferece direitos semelhantes aos consumidores em relação aos seus dados pessoais. No Brasil, a Lei Geral de Proteção de Dados (LGPD), inspirada em parte pelo GDPR, entrou em vigor em 2020 e tem como objetivo proteger os dados pessoais dos cidadãos brasileiros, estabelecendo regras para o uso, armazenamento e compartilhamento dessas informações.

Essas legislações, apesar de apresentarem diferenças em alguns pontos, compartilham o objetivo comum de garantir a privacidade e a segurança dos dados

peçoais, além de responsabilizar as organizações que não cumprirem as normas. A comparação entre essas leis permite identificar boas práticas e desafios enfrentados em diferentes contextos, contribuindo para o aprimoramento das políticas de proteção da intimidade em nível global.

3 CRIMES CONTRA A PROTEÇÃO DA INTIMIDADE

Neste capítulo, serão abordados os crimes que violam a proteção da intimidade e da privacidade das pessoas, especialmente no ambiente digital. Com o avanço da tecnologia e o uso crescente da Internet, surgiram novas formas de crimes que envolvem a exposição indevida de informações pessoais, invasão de dispositivos eletrônicos, divulgação não autorizada de dados e outras práticas que atentam contra a privacidade dos indivíduos.

É fundamental compreender esses crimes para entender como a legislação brasileira os combate, quais são as consequências para os infratores e como as vítimas podem buscar proteção e reparação. Este capítulo visa apresentar os principais tipos de crimes contra a intimidade, suas características e o impacto que causam na vida das pessoas.

3.1 TIPOS DE CRIME

A proteção da intimidade no Brasil é um direito fundamental assegurado pela Constituição Federal de 1988, em seu artigo 5º, inciso X, que estabelece que "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação".

No âmbito penal, a tutela da intimidade se materializa na tipificação de diversos crimes que visam proteger a esfera privada do indivíduo. A legislação brasileira, reconhecendo a evolução das tecnologias e o aumento das ameaças a esse direito, expandiu o rol de condutas criminosas. Assim, a invasão de privacidade não é tratada apenas como um conceito abstrato, mas como uma série de atos concretos que configuram delitos específicos, com sanções penais previstas em lei. A seguir, analisaremos a principal figura típica dessa categoria: a invasão na privacidade nos dispositivos eletrônicos.

3.1.1 Invasão de privacidade

A invasão de privacidade, no contexto penal, é tipificada principalmente pelo artigo 154-A do Código Penal brasileiro, que trata da Invasão de Dispositivo Informático. Este delito, introduzido pela Lei nº 12.737/2012 (conhecida como Lei Carolina Dieckmann), representou um avanço significativo na proteção da intimidade e da vida privada em ambientes digitais. A criação dessa norma foi motivada pela necessidade de o ordenamento jurídico se adaptar aos desafios impostos pela cibercriminalidade, em que a invasão de sistemas e a apropriação indevida de dados pessoais se tornaram uma ameaça constante.

A invasão de dispositivo informático é definida pela legislação da seguinte forma:

Art. 154-A. Invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário, ou de instalar vulnerabilidades para obter vantagem ilícita:
Pena – detenção, de 3 (três) meses a 1 (um) ano, e multa (Brasil, 2012).

A regra geral é que o crime de invasão de dispositivo informático é de ação penal pública condicionada à representação, conforme o § 3º do artigo 154-A. Isso significa que a vítima (sujeito passivo) precisa manifestar o interesse em processar o agressor. No entanto, o § 4º estabelece uma exceção, convertendo a ação em pública incondicionada se o crime for praticado contra a Administração Pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios, ou contra empresas concessionárias de serviços públicos.

Contudo é importante diferenciar a invasão de dispositivo informático de outros delitos que podem, à primeira vista, parecer semelhantes, mas possuem elementos distintos:

Furto qualificado mediante fraude eletrônica (Art. 155, § 4º-B, CP): A invasão aqui é o meio para o fim de subtrair um bem móvel (geralmente dinheiro) da vítima, com a finalidade de obtenção de vantagem ilícita.

Estelionato (Art. 171, CP): O estelionato envolve o uso de artifício ou ardil para induzir a vítima ao erro e obter vantagem ilícita, enquanto a invasão do 154-A não exige a colaboração da vítima.

Violação de correspondência (Art. 151, CP): Este crime se aplica a correspondências físicas, enquanto o 154-A abrange a correspondência digital, como e-mails e mensagens de aplicativos.

3.1.2 Divulgação não autorizada de dados pessoais

A divulgação não autorizada de dados pessoais, embora não tenha um tipo penal genérico, pode ser criminalizada por meio de outros delitos já existentes no Código Penal e é tratada com rigor pela Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709/2018. A LGPD, embora seja uma lei de natureza cível e administrativa, estabelece os princípios e as regras para o tratamento de dados pessoais, definidos como qualquer informação relacionada a uma pessoa natural identificada ou identificável. A violação desses princípios pode ter consequências penais.

O crime de violação de segredo profissional, previsto no artigo 154 do Código Penal, é um exemplo, pois o segredo revelado muitas vezes são os dados pessoais sigilosos do cliente ou paciente. De forma similar, a divulgação de dados obtidos por meio de uma invasão, conforme o artigo 154-A, agrava o crime principal. A exposição de dados pessoais também pode ser um meio para a prática de crimes contra a honra, como difamação ou injúria, ou para a extorsão, quando a ameaça de divulgar informações íntimas é utilizada para forçar a vítima a agir contra sua vontade. Portanto, embora não haja um artigo específico para a conduta, a divulgação de dados pessoais pode ser um ato ilícito grave, com sanções penais previstas em lei.

3.1.3 *Cyberbullying* e assédio on-line

O *cyberbullying* e o assédio online são formas de violência que ocorrem por meios digitais e se caracterizam pela perseguição, intimidação, humilhação e exposição da vítima. No Brasil, essas condutas, por si só, não são tipificadas como crimes autônomos, mas podem ser enquadradas em tipos penais já existentes, a depender da natureza da ação.

As principais figuras penais que podem caracterizar o *cyberbullying* são os crimes contra a honra: calúnia (acusação falsa de um crime), difamação (imputação de um fato desonroso) e injúria (ofensa à dignidade ou ao decoro da vítima). A pena para esses crimes pode ser aumentada quando cometidos em redes sociais, devido ao seu grande alcance e à facilidade de viralização do conteúdo. Outros crimes, como a ameaça (art. 147 CP) e o constrangimento ilegal (art. 146 CP), também podem ser utilizados para enquadrar o assédio online, especialmente quando a vítima é coagida a fazer algo contra a sua vontade.

A Lei nº 14.132/2021 trouxe um importante avanço ao tipificar o crime de perseguição, ou *stalking*, no artigo 147-A do Código Penal. Embora não mencione o termo *cyberbullying*, a perseguição online se encaixa perfeitamente na descrição do crime: "perseguir alguém, reiteradamente e por qualquer meio, ameaçando-lhe a integridade física ou psicológica" (1940). Este tipo penal abarca a conduta de assédio continuado, que é uma das principais características do *cyberbullying*. Além disso, a divulgação de cena de sexo ou nudez sem consentimento, popularmente conhecida como *revenge porn*, é um crime específico e grave, previsto no artigo 218-C do Código Penal, e é uma das formas mais comuns de assédio on-line.

3.2 CONSEQUÊNCIAS JURÍDICAS

A violação da intimidade e da vida privada, além de configurar um ilícito penal, pode desencadear uma série de consequências jurídicas em outras esferas do direito, como a cível e a administrativa. É crucial compreender a distinção e a complementaridade entre a responsabilidade civil, a responsabilidade penal e a responsabilidade administrativa, pois todas visam tutelar o direito violado, mas com finalidades e sanções distintas. Enquanto a responsabilidade penal busca a punição do ofensor pelo Estado, a responsabilidade civil tem como objetivo principal a reparação do dano sofrido pela vítima, e a responsabilidade administrativa, a sanção por descumprimento de normas regulamentares. Essa pluralidade de ações judiciais permite que uma única conduta ilícita resulte em um conjunto de penalidades aplicadas por diferentes esferas do poder público, reforçando a proteção do bem jurídico da intimidade.

3.2.1 Responsabilidade civil

A responsabilidade civil surge da obrigação de reparar o dano causado a outrem, conforme estabelecem os artigos 186 e 927 do Código Civil. Para sua configuração, são necessários quatro elementos: a conduta do agente, o dano, o nexo de causalidade e a culpa ou dolo.

Neste sentido, observa-se o disposto nos artigos 186 e 187, do Código Civil (2012), brasileiro:

Art. 186. Aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente,

comete ato ilícito. Art. 187. Também comete ato ilícito o titular de um direito que, ao exercê-lo, excede manifestamente os limites impostos pelo seu fim econômico ou social, pela boa-fé ou pelos bons costumes.

No contexto dos crimes contra a intimidade, o dano é o elemento central, podendo ser de natureza material ou moral. O dano material refere-se a prejuízos patrimoniais, como custos com a restauração de um sistema invadido ou a perda de renda decorrente da violação da privacidade. Já o dano moral, o mais comum nestes casos, atinge a esfera não-econômica da vítima, como sua dignidade, honra, imagem e a própria intimidade. A indenização por dano moral tem uma dupla finalidade: compensar o sofrimento da vítima e servir como uma sanção pedagógica para o agressor, desestimulando a repetição da conduta. O valor da compensação é arbitrado pelo juiz, que pondera a gravidade do ato, a extensão do dano e a capacidade financeira das partes.

3.2.2 Responsabilidade penal

A responsabilidade penal surge da prática de uma conduta que a lei define como crime e é exercida exclusivamente pelo Estado, que tem o poder de punir o infrator. O objetivo da sanção penal não é a reparação do dano à vítima, mas sim a aplicação de uma pena, que pode ser privativa de liberdade (detenção ou reclusão), restritiva de direitos ou de multa.

Nos crimes contra a intimidade, as condutas são tipificadas no Código Penal. A invasão de dispositivo informático (Art. 154-A), por exemplo, é punida com detenção. As condutas de *cyberbullying* e assédio online podem ser enquadradas em crimes como injúria (Art. 140), difamação (Art. 139) e, mais recentemente, perseguição (*stalking*, Art. 147-A). Cada um desses tipos penais prevê uma pena específica, que pode ser aumentada dependendo das circunstâncias, como a divulgação em redes sociais, que potencializa o dano.

É importante ressaltar a independência entre as responsabilidades civil e penal. Uma vítima pode ajuizar uma ação cível para buscar indenização, independentemente de o criminoso ser condenado ou não na esfera penal. No entanto, o Princípio da Adesão estabelece que uma sentença penal condenatória definitiva tem impacto na esfera cível, tornando o fato e a autoria incontestáveis. Por outro lado, a absolvição criminal que se baseia na inexistência do fato ou na negativa de autoria impede que a

vítima busque reparação na esfera cível pelo mesmo motivo, pois a matéria já foi definitivamente julgada. A coexistência e a independência dessas esferas reforçam a eficácia da proteção jurídica à intimidade.

4 ANÁLISE DO PAPEL DO MARCO CIVIL DA INTERNET NA PROTEÇÃO DA INTIMIDADE

O presente capítulo tem como objetivo central examinar como o Marco Civil da Internet contribui para a proteção da intimidade, o Marco Civil da Internet (MCI), Lei nº 12.965/2014, emerge como um instrumento jurídico fundamental. Considerado a “Constituição da Internet brasileira”, o MCI não se limita a punir crimes, mas estabelece os princípios, garantias, direitos e deveres para o uso da rede no Brasil.

Esta seção analisará os principais pilares do MCI que dialogam diretamente com a proteção da intimidade, incluindo a garantia da inviolabilidade e do sigilo do fluxo de comunicações e do armazenamento de dados, as regras sobre a guarda e a disponibilização de registros de acesso e a responsabilidade dos provedores de aplicação. A compreensão do papel do MCI é crucial para demonstrar que a proteção da intimidade na era digital exige uma abordagem jurídica multifacetada, que combina a repressão penal com a regulação e a garantia de direitos fundamentais.

4.1 MECANISMOS DE PROTEÇÃO PREVISTOS NA LEGISLAÇÃO

O Marco Civil da Internet (MCI), Lei nº 12.965/2014, vai muito além de um simples estatuto regulatório e se estabelece como uma verdadeira Carta Magna do ciberespaço brasileiro, instituindo mecanismos concretos para a proteção da intimidade. Seus dispositivos atuam como uma barreira legal contra o uso abusivo da Internet, traduzindo o direito fundamental à privacidade em garantias práticas.

O principal alicerce dessa proteção está no Artigo 7º, que consagra expressamente o direito à inviolabilidade e ao sigilo das comunicações privadas e dos registros de conexão e de acesso. O inciso II desse artigo assegura a inviolabilidade e o sigilo do fluxo de comunicações, e o inciso III garante a inviolabilidade e o sigilo das comunicações privadas armazenadas. Ambas as garantias são condicionadas a uma ordem judicial, o que impede que provedores e terceiros acessem essas informações sem uma autorização expressa da justiça, fortalecendo o controle do

indivíduo sobre seus dados.

Outro ponto crucial é a regulamentação sobre a guarda de dados, que é um dos maiores desafios da privacidade digital. O MCI estabelece que os provedores de conexão devem manter os registros de conexão dos usuários por um período de um ano (Art. 13), enquanto os provedores de aplicação devem manter os registros de acesso por seis meses (Art. 15). Essa exigência visa a permitir que, em caso de violação de direitos, a vítima tenha uma forma de identificar o agressor. No entanto, a lei é clara ao proibir que esses dados sejam utilizados para outros fins, a não ser mediante ordem judicial, o que evita a comercialização ou o uso indevido das informações pessoais.

Por fim, o Artigo 11º do Marco Civil da Internet aborda a questão da extraterritorialidade, um tema de suma importância em um mundo globalizado. Ele determina que o tratamento de dados pessoais coletados no Brasil deve seguir a legislação brasileira, mesmo que a sede da empresa ou o servidor esteja localizado no exterior. Esse dispositivo garante que plataformas e empresas internacionais que atuam no Brasil não possam se eximir de suas responsabilidades, protegendo os dados dos cidadãos brasileiros independentemente da localização dos centros de dados.

4.2 LIMITAÇÕES E DESAFIOS NA APLICAÇÃO

Apesar de ser um marco na legislação, a aplicação do Marco Civil da Internet não está isenta de limitações e desafios. O modelo adotado pela lei, que busca o equilíbrio entre a liberdade de expressão e a privacidade, muitas vezes gera impasses práticos que dificultam a efetiva proteção da intimidade.

Uma das principais limitações reside no sistema de responsabilidade civil dos provedores. O Artigo 19º do MCI estabelece que os provedores de aplicação só podem ser responsabilizados por conteúdo gerado por terceiros após o descumprimento de uma ordem judicial de remoção. Esse modelo, conhecido como *notice and takedown* mediado, visa a proteger a liberdade de expressão ao evitar que provedores removam conteúdo de forma arbitrária. Contudo, em casos de grave violação da intimidade, como a divulgação de fotos íntimas ou a disseminação de informações falsas, a exigência de uma ordem judicial pode gerar um atraso significativo. Durante o tempo que o processo judicial leva para ser concluído, o

conteúdo ilícito pode viralizar, causando danos irreparáveis à honra e à imagem da vítima.

Outro desafio relevante é a questão da identificação do agressor. Mesmo que o provedor seja obrigado por ordem judicial a fornecer os registros de acesso, muitas vezes esses dados se resumem a um endereço de IP, que nem sempre é suficiente para a identificação da pessoa física que cometeu o ilícito. A utilização de redes privadas virtuais (VPNs) ou a simples troca de redes de Wi-Fi abertas dificulta o rastreamento, tornando o trabalho de investigação complexo e, em alguns casos, inviável.

Por fim, a ausência de um órgão regulador específico para o MCI, ao contrário da Lei Geral de Proteção de Dados (LGPD) que criou a ANPD, representa uma limitação institucional. A fiscalização e a aplicação das normas do Marco Civil dependem, em grande parte, do Poder Judiciário, que nem sempre possui a agilidade e o conhecimento técnico necessários para lidar com as especificidades do ambiente digital. Essa dependência exclusiva do judiciário pode retardar a resolução de conflitos e enfraquecer a eficácia da proteção da intimidade online.

4.2.1 Ambiguidade de termos

Apesar de ser uma lei moderna, o Marco Civil da Internet (MCI) não está imune a certas imprecisões que dificultam sua aplicação prática, gerando insegurança jurídica. A redação de alguns de seus artigos utiliza termos que não possuem uma definição clara e consensual na doutrina e jurisprudência, o que abre margem para diferentes interpretações e, conseqüentemente, retarda a efetiva proteção da intimidade.

Um exemplo notável é a ambiguidade do termo "registros de acesso a aplicações", previsto no Artigo 15 do MCI. Embora o dispositivo determine que os provedores de aplicação devem manter esses registros por seis meses, a lei não define o que exatamente a expressão abrange. A falta de clareza gera questionamentos sobre a legalidade da coleta de dados de navegação, de mensagens ou de interações em redes sociais. A indefinição do que constitui um "registro" de acesso pode levar a disputas judiciais, nas quais a coleta de dados é contestada, prolongando o processo de identificação do ofensor e a responsabilização pela violação da intimidade. Outra questão é a ausência de uma métrica clara para o que

configura um "grave dano", que poderia justificar uma ordem judicial para a remoção imediata de conteúdo ilícito, sem a necessidade de um processo demorado, conforme previsto no Artigo 21. A interpretação do que é "grave" fica a critério do juiz, o que pode levar a decisões heterogêneas e a uma tutela da intimidade menos célere.

4.3 CASOS EMBLÉMATICOS E JURISPRUDÊNCIA

A jurisprudência brasileira, especialmente a do Superior Tribunal de Justiça (STJ), tem desempenhado um papel crucial na interpretação da lei e na sua adaptação aos desafios da era digital. A análise de casos emblemáticos é fundamental para entender como os mecanismos de proteção da intimidade são postos à prova, e quais limitações persistem na prática.

Caso Facebook e vazamento de dados do Cambridge *Analytica* (2018): o escândalo envolvendo a Cambridge *Analytica* em 2018 representa um marco na discussão sobre a proteção de dados pessoais por entidades privadas. A consultoria política britânica foi acusada de coletar indevidamente informações de milhões de usuários do Facebook, mesmo com a plataforma garantindo que esses dados não seriam compartilhados com terceiros.

A utilização dessas informações, que incluíam resultados de testes de entretenimento e "curtidas", foi notadamente observada na campanha presidencial de Donald Trump em 2016. A Cambridge *Analytica*, ao analisar esse material, construiu perfis psicográficos dos usuários, o que permitiu o envio de publicidade eleitoral segmentada e personalizada. Essa prática, ao que tudo indica, conferiu uma vantagem injusta à campanha de Trump sobre os demais candidatos.

Inicialmente, a Federal *Trade Commission* (FTC) estimou que entre 50 e 65 milhões de perfis foram afetados, número que posteriormente foi revisado para 85 milhões de usuários. A gravidade da violação da privacidade dos consumidores levou a FTC a impor uma multa de 5 bilhões de dólares, a maior já aplicada pela comissão em casos dessa natureza.

Caso pornografia de vingança Rose Leonel: o caso de Rose Leonel, residente em Maringá (PR), à época com 41 anos, apresentadora de televisão, colunista e fundadora da ONG Marias da Internet, ilustra de forma contundente a brutalidade do revenge porn e suas devastadoras consequências. As informações deste relato são extraídas, principalmente, das entrevistas concedidas pela própria vítima a programas

televisivos.

Rose narra que a tormentosa situação teve início em outubro de 2005, após o término de seu relacionamento de quatro anos com Eduardo Gonçalves Dias. Segundo seu testemunho em entrevista ao programa Jogo Aberto (2014), Eduardo não aceitou a separação, manifestando inconformismo e proferindo ameaças como: "se você não ficar comigo, eu vou acabar com a sua vida".

A vítima, contudo, jamais imaginou a proporção que as palavras de seu ex-companheiro tomariam, afirmando não ter concebido que ele seria capaz de expô-la da forma como o fez, "nunca imaginei que a gente pudesse dormir com o inimigo", desabafou Rose na mesma entrevista. Em janeiro de 2006, Eduardo enviou um e-mail contendo material íntimo da vítima para mais de 15 mil destinatários, incluindo colegas de trabalho, familiares, conhecidos da cidade e até mesmo pessoas desconhecidas.

Em um ato de extrema crueldade e sarcasmo, Eduardo elaborou uma apresentação de slides, anexada às mensagens enviadas, intitulada "Apresentando a colunista social Rose Leonel – Capítulo I". O agressor detalhou e qualificou cada uma das fotos com legendas que simulavam um portfólio de uma garota de programa (Buzzi, 2015, p. 46). A partir de então, encarregou-se de distribuir as fotos de Rose em milhões de sites com conteúdo pornográfico.

A exposição, entretanto, não cessou. O agressor continuou a divulgar materiais íntimos de Rose por um período de aproximadamente três anos e meio, enviando e-mails com "capítulos" sucessivos (capítulo 2, 3, 4). Além de utilizar imagens autênticas da vítima, seu ex-companheiro passou a manipular montagens, combinando o rosto de Rose com corpos de outras mulheres nuas. Toda essa exposição foi acompanhada pela divulgação de telefones pessoais da vítima, de seu local de trabalho e, inclusive, do telefone de seu filho, que era adolescente na época, conforme relatado por Rose no programa Jogo Aberto:

"Eu perdi meu emprego, perdi os meus amigos, perdi minha vida social, sofri um assassinato psicológico, moral, profissional, você sofre uma crise de identidade, porque o que as pessoas veem ali é uma ideia que foi jogada na Internet. Além do meu ex me expor na Internet, ele me humilhava e escrevia coisas horríveis a meu respeito. Então, ele me vendia como se eu fosse uma garota de programa, a partir de fotos e textos, além de fornecer os números de telefone da minha casa, meu celular e inclusive o celular do meu filho." (Leonel, 2014, 4:24).

Hoje, 13 anos após sua exposição, Rose tornou-se um ícone no combate à Pornografia de Revanche. Foi um marco no âmbito jurídico brasileiro, haja vista ser uma das primeiras brasileiras a conseguir reparação contra um ex companheiro que compartilhou suas imagens sem qualquer consentimento. A saber, no ano de 2012, Eduardo foi condenado ao pagamento de R\$30.000,00 a título de danos morais, bem como reclusão de um ano e onze meses. Logo após o caso se deu origem a lei Rose Leonel, oficialmente conhecida como Lei nº 14.132/2021.

5 PROPOSTAS DE APRIMORAMENTO

As propostas aqui discutidas buscam não apenas corrigir lacunas identificadas na legislação atual, mas também antecipar desafios futuros, promovendo uma adaptação contínua às transformações tecnológicas e sociais. Entre os aspectos abordados, destacam-se a necessidade de maior clareza nas responsabilidades dos provedores, o aprimoramento dos mecanismos de fiscalização e punição, e a ampliação da educação digital para usuários e agentes do setor. A análise dessas sugestões é fundamental para contribuir com o debate jurídico e social, visando a construção de uma Internet que respeite e proteja efetivamente a intimidade e a privacidade de todos.

5.1 SUGESTÕES LEGISLATIVAS

Apesar dos avanços proporcionados pelo Marco Civil da Internet e pela Lei Geral de Proteção de Dados (LGPD), ainda existem lacunas e desafios que demandam aprimoramentos legislativos para garantir uma proteção mais eficaz da intimidade no ambiente digital. Primeiramente, é necessário estabelecer com maior clareza as responsabilidades dos provedores de Internet e plataformas digitais, especialmente no que tange à obrigação de remoção de conteúdos ilícitos e à proteção contra vazamentos de dados. A legislação poderia prever prazos mais definidos para atendimento de ordens judiciais, bem como sanções mais rigorosas para o descumprimento dessas determinações.

Além disso, a incorporação de dispositivos específicos para lidar com novas formas de violação da privacidade, como *deepfakes*, inteligência artificial e monitoramento automatizado, é fundamental para acompanhar a evolução

tecnológica. A criação de mecanismos legais que incentivem a transparência no uso de algoritmos e no tratamento de dados pessoais também contribuiria para a proteção dos usuários. Outro ponto importante é o fortalecimento dos órgãos reguladores e fiscalizadores, como a Autoridade Nacional de Proteção de Dados (ANPD), garantindo-lhes maior autonomia, recursos e poder de atuação para investigar e punir infrações.

A legislação poderia ainda prever a obrigatoriedade de relatórios periódicos de transparência por parte das empresas, detalhando as medidas adotadas para proteger a privacidade dos usuários. Por fim, a harmonização das normas brasileiras com padrões internacionais de proteção de dados e privacidade, como o Regulamento Geral sobre a Proteção de Dados (GDPR) da União Europeia, pode facilitar a cooperação internacional e elevar o nível de proteção oferecido aos cidadãos.

5.2 O PAPEL DA EDUCAÇÃO DIGITAL NA PROTEÇÃO DA INTIMIDADE

A educação digital é um componente essencial para a proteção da intimidade no ambiente online, capacitando os usuários a compreenderem os riscos e adotarem práticas seguras no uso da Internet. No Brasil, dados do Comitê Gestor da Internet (CGI.br) indicam que, em 2022, cerca de 81% da população brasileira acessava a Internet, sendo que muitos usuários ainda apresentam baixo nível de conhecimento sobre segurança digital e privacidade. Segundo a pesquisa TIC Domicílios 2022, apenas 38% dos internautas brasileiros afirmaram saber como proteger seus dados pessoais na Internet, evidenciando a necessidade urgente de programas educativos.

Além disso, a pesquisa “Vulnerabilidades Digitais no Brasil”, realizada pelo Instituto Locomotiva em 2023, revelou que 45% dos brasileiros já foram vítimas de algum tipo de golpe ou invasão digital, o que reforça a importância da educação digital para a prevenção desses incidentes. A educação deve abordar temas como configuração de privacidade em redes sociais, reconhecimento de golpes, uso seguro de senhas e a importância do consentimento informado. Capacitar profissionais do setor tecnológico, educadores, jornalistas e agentes públicos também é fundamental para que possam atuar como multiplicadores dessas informações, promovendo uma cultura digital pautada no respeito à intimidade e à privacidade.

5.3 FORTALECIMENTO DAS INSTITUIÇÕES DE FISCALIZAÇÃO

Campanhas públicas, como a iniciativa “Internet Segura” do CGI.br, e parcerias com organizações da sociedade civil, como o *SaferNet* Brasil, ampliam o alcance da educação digital, tornando-a acessível a diferentes faixas etárias e contextos sociais. Dessa forma, a educação digital atua como uma ferramenta preventiva, reduzindo a vulnerabilidade dos usuários e fortalecendo a proteção da privacidade de forma complementar às medidas legislativas e regulatórias.

O fortalecimento das instituições responsáveis pela fiscalização e proteção da privacidade na Internet é fundamental para garantir a efetividade das normas legais e a segurança dos usuários. No Brasil, a Autoridade Nacional de Proteção de Dados (ANPD) desempenha papel central na implementação e fiscalização da Lei Geral de Proteção de Dados (LGPD). Contudo, para que a ANPD possa cumprir plenamente sua missão, é necessário ampliar sua autonomia, recursos financeiros e humanos, bem como garantir maior independência técnica e política.

Segundo o Relatório Anual da ANPD de 2022, a autoridade ainda enfrenta desafios relacionados à estruturação interna e à capacidade de fiscalização além dos avanços, o documento destaca que “Nesse cenário de fortalecimento jurídico, a designação dos membros e a estruturação do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade também representou um avanço relevante, na medida em que concretizou uma instância colegiada consultiva para a ANPD, com participação de profissionais altamente qualificados.” (ANPD, 2022, p. 5). Além da ANPD, outros órgãos como o Ministério Público, a Polícia Federal e os Tribunais de Justiça também têm papel relevante na fiscalização e repressão de crimes contra a intimidade e privacidade na Internet. A integração e cooperação entre essas instituições devem ser aprimoradas para otimizar a investigação e punição de infrações.

A legislação poderia prever mecanismos que garantam maior independência orçamentária e administrativa para a ANPD, além de ampliar suas competências para atuar de forma preventiva, por meio de auditorias e orientações técnicas. Também é recomendável a criação de canais acessíveis e eficientes para denúncias e reclamações, facilitando o acesso dos cidadãos à proteção de seus direitos. No entanto a capacitação contínua dos agentes públicos envolvidos na fiscalização é essencial para acompanhar as constantes inovações tecnológicas e as novas modalidades de violação da privacidade, garantindo respostas rápidas e eficazes.

CONSIDERAÇÕES FINAIS

O presente Trabalho de Conclusão de Curso possibilitou a análise do papel do Marco Civil da Internet na proteção da intimidade e da privacidade dos usuários no ambiente digital. Ao longo da pesquisa, foi possível perceber que o avanço da tecnologia e o uso constante da Internet trouxeram benefícios significativos para a sociedade, mas também ampliaram os riscos relacionados à violação de direitos fundamentais, especialmente no que se refere à vida privada das pessoas.

A análise do Marco Civil da Internet demonstrou que a referida legislação representa um importante avanço no ordenamento jurídico brasileiro, ao estabelecer princípios e garantias voltados à proteção da privacidade, da liberdade de expressão e da responsabilidade dos provedores de serviços digitais. Essa norma contribuiu para a criação de regras mais claras sobre o uso da Internet, buscando equilibrar os direitos dos usuários com o desenvolvimento tecnológico.

No decorrer do trabalho, observou-se que os crimes contra a intimidade, como a invasão de dispositivos eletrônicos, a divulgação não autorizada de dados pessoais e o assédio online, têm se tornado cada vez mais comuns. Essas condutas causam danos significativos às vítimas, afetando não apenas sua honra e imagem, mas também sua saúde emocional e sua vida social, o que reforça a necessidade de uma proteção jurídica mais efetiva.

Verificou-se, ainda, que embora existam mecanismos legais para responsabilizar os infratores nas esferas civil e penal, a aplicação prática dessas normas enfrenta desafios. A rapidez com que as informações se espalham na Internet e as dificuldades na identificação dos responsáveis muitas vezes impedem que a reparação ocorra de forma imediata e eficaz, fazendo com que o dano causado seja, em muitos casos, irreversível.

Diante desse cenário, o estudo evidenciou a importância do aprimoramento da legislação e do fortalecimento das instituições responsáveis pela fiscalização e aplicação das normas. Além disso, destacou-se o papel da educação digital como medida preventiva, permitindo que os usuários tenham maior consciência sobre os riscos do ambiente virtual e adotem práticas mais seguras no uso da Internet.

Por fim, conclui-se que o Marco Civil da Internet exerce um papel relevante na proteção da intimidade no ambiente digital, porém, diante das constantes transformações tecnológicas, torna-se necessária sua constante atualização.

Somente por meio da combinação entre legislação eficaz, fiscalização adequada e conscientização dos usuários será possível garantir um ambiente digital mais seguro, que respeite a dignidade e os direitos fundamentais dos indivíduos.

REFERÊNCIAS

ANPD. **Relatório de Atividades 2022**. Brasília: Agência Nacional de Proteção de Dados, 2022. Disponível em: <https://www.gov.br/anpd/pt-br/cnpd-2/cnpd-rel-atividades-2022.pdf>

BBC. Como os dados de milhões de usuários do Facebook foram usados na campanha de Trump. **BBC News Brasil**, abril de 2018. Disponível em: <https://www.bbc.com/portuguese/geral-43705839>.

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm

BRASIL. Lei nº 12.965, de 23 de abril de 2014. **Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil (Marco Civil da Internet)**. Brasília, DF: Presidência da República, 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Brasília, DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

BRASIL. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. **Código Penal**. Rio de Janeiro: Presidência da República, 1940. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm

BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. Institui o **Código Civil**. Brasília, DF: Presidência da República, 2002. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406.htm

BRASIL. Lei nº 12.737, de 30 de novembro de 2012. **Dispõe sobre a tipificação criminal de delitos informáticos (Lei Carolina Dieckmann)**. Brasília, DF: Presidência da República, 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm

BRASIL. Lei nº 14.132, de 31 de março de 2021. **Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para incluir o crime de perseguição (stalking)**. Brasília, DF: Presidência da República, 2021. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14132.htm

BUZZI, V. D. M. **Pornografia de vingança: contexto histórico-social e abordagem no direito brasileiro**. 2015. Disponível em: <https://repositorio.ufsc.br/handle/123456789/133841>.

CONJUR. **Marco Civil da Internet**: regulação precisa ser mais equilibrada. Disponível em: <https://www.conjur.com.br/2025-jun-18/por-que-a-decisao-do-stf-merece-ser-compreendida/>

FEDERAL TRADE COMMISSION. **FTC Imposes \$5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook**. July 24, 2019. Disponível em: <https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-pr>.

INSTITUTO LOCOMOTIVA. **Vulnerabilidades digitais no Brasil**. São Paulo: Instituto Locomotiva, 2023. Disponível em: <https://ilocomotiva.com.br>. Acesso em: 19 fev. 2026.

LEONEL, Rose. **Jogo Aberto – Rose Leonel (30/08) Bloco 01**. Youtube, 30 ago. 2014. Disponível em: <https://youtu.be/MLubGW2ePco>. Acesso em: 12 de fev. 2026

LINS, B. F. E. **A evolução da Internet**: uma perspectiva histórica. Cadernos Aslegis, 2013. Disponível em: https://belins.eng.br/ac01/papers/aslegis48_art01_hist_internet.pdf

POLÍCIA FEDERAL. **Combate a crimes cibernéticos**. Dados Estatísticos de Combate a Crimes Cibernéticos — Polícia Federal. Disponível em: <https://www.gov.br/pf/pt-br/aceso-a-informacao/estatisticas/diretoria-de-combate-a-crimes-ciberneticos-dciber>. Acesso em jan de 2026.

SAFERNET BRASIL. **Campanhas e Projetos**. Disponível em: <https://internetsegura.br/outras-iniciativas/>.

A R T I G O 07

DELEGAÇÃO DA REDAÇÃO JURÍDICA DE DECISÕES À INTELIGÊNCIA ARTIFICIAL: ANÁLISE DOS LIMITES E POSSIBILIDADES

Samuel Costa Silva

Leonardo Silva de Oliveira Bandeira