CRIMES CIBERNÉTICOS E A PROTEÇÃO DO DIREITO À INTIMIDADE NO AMBIENTE DIGITAL

Agatha Yara do Carmo Rodriguês, Frediano José Galioti Teodoro.

Universidade do Vale do Paraíba/ Faculdade de Direito, Praça Cândido Dias Castejón, 116, Centro 12245-720- São José dos Campos-SP, Brasil, agathacarmo42@gmail.com, frediano@univap.br.

Resumo
Esta pesquisa tem como objetivo analisar os meios de identificação de delitos relacionados aos crimes cibernéticos, compreender as dificuldades enfrentadas na identificação dos responsáveis, considerando o avanço tecnológico, as violações à privacidade e as lacunas ainda existentes na legislação. A metodologia adotada é qualitativa e descritiva, baseada na análise da legislação brasileira, de doutrina especializada, de artigos acadêmicos e de jurisprudência, com utilização do método hermenêutico. Os resultados demonstram que a identificação dos responsáveis por crimes cibernéticos pode ser dificultada pelo anonimato proporcionado pelas tecnologias, pela evolução das práticas criminosas, pela insuficiência de conhecimentos técnicos das autoridades e pela necessidade de maior integração entre os órgãos responsáveis pela investigação. Também se observa que a proteção do direito à intimidade permanece desafiada pelo uso e compartilhamento de dados pessoais, apesar dos mecanismos previstos na legislação brasileira, especialmente na Lei Geral de Proteção de Dados. Conclui-se que o enfrentamento dos crimes cibernéticos exige o aprimoramento dos mecanismos de investigação e proteção, a capacitação dos agentes públicos, a educação digital, a cooperação entre instituições e a atualização contínua das normas jurídicas.
Palavras-chave: Crimes Cibernéticos. Direito à Intimidade. Mecanismos de Proteção. Violações.

Área do Conhecimento: Ciências Jurídicas. Direito Público.

Introdução

A era digital tem promovido transformações profundas na sociedade, alterando não apenas a maneira como interagimos, mas também como vivenciamos e protegemos nossos direitos fundamentais. Os crimes cibernéticos, definidos como atividades ilícitas que utilizam dispositivos eletrônicos e a internet, emergem como uma preocupação crescente em todo o mundo. No Brasil, essas práticas se manifestam de diversas formas, desde fraudes financeiras e *phishing* até ataques mais sofisticados, como *ransomware* e invasões de dados. Embora o Código Penal Brasileiro e a Lei nº 12.737/2012 tenham estabelecido diretrizes para a tipificação dessas condutas (Brasil, 1940; Brasil, 2012), a eficácia dessas legislações é frequentemente comprometida por uma série de fatores.

Um dos principais obstáculos é a falta de conhecimento técnico das autoridades responsáveis pela investigação e repressão a esses crimes. Outro aspecto crucial é a vulnerabilidade das vítimas, que muitas vezes não se restringe a falhas técnicas, mas à falta de conscientização sobre segurança digital. O uso de técnicas de engenharia social por parte dos golpistas exemplifica como a confiança das pessoas pode ser manipulada, resultando em prejuízos financeiros significativos. Isso demonstra a importância de campanhas de conscientização que orientem a população sobre os riscos do ambiente digital e sobre formas de proteção.

Nesse contexto, a proteção do direito à intimidade se torna um tema central. Com a evolução das tecnologias, especialmente das redes sociais e das plataformas de compartilhamento de dados, a privacidade individual é constantemente ameaçada. A Lei Geral de Proteção de Dados (LGPD), aprovada em 2018, foi um marco importante na busca pela proteção da privacidade dos cidadãos, exigindo consentimento explícito para o tratamento de dados pessoais (Brasil, 2018). Contudo, sua implementação enfrenta desafios, como a falta de compreensão das obrigações legais por parte das empresas e a dificuldade em garantir que os dados sejam tratados de maneira ética e transparente.

Assim, o presente trabalho se propõe a analisar a intersecção entre crimes cibernéticos e a proteção do direito à intimidade, explorando as dificuldades enfrentadas na identificação de culpados e as implicações da evolução tecnológica para a privacidade dos indivíduos. A partir dessa análise, busca-se compreender os principais desafios atuais e discutir medidas que possam contribuir para o

fortalecimento da legislação e da educação digital, visando um ambiente online mais seguro e respeitoso em relação aos direitos fundamentais.

Metodologia

A pesquisa foi desenvolvida com base na análise teórica e interpretativa do tema. Foram utilizados como base de pesquisa a legislação brasileira, especialmente a Lei nº 12.737/2012 e a Lei Geral de Proteção de Dados (LGPD) (Brasil, 2012; Brasil, 2018), além de doutrina especializada, artigos acadêmicos e jurisprudência.

A análise foi realizada por meio do método hermenêutico, buscando interpretar as normas jurídicas e sua aplicação prática nos casos de crimes cibernéticos. Também foi utilizada revisão de literatura, permitindo uma compreensão mais ampla do tema a partir de diferentes autores, além de uma análise crítica sobre a eficácia dos mecanismos atuais.

Resultados

A proteção do direito à intimidade é um princípio fundamental que resguarda a privacidade dos indivíduos, garantindo que suas informações pessoais e aspectos da vida privada não sejam expostos sem consentimento. Este direito é essencial em uma sociedade democrática, onde a liberdade e a dignidade humana são valores centrais. No entanto, a rápida evolução das novas tecnologias, especialmente a internet e as redes sociais, traz desafios significativos à proteção da intimidade, exigindo uma análise crítica e uma abordagem adaptativa por parte das legislações e da sociedade.

De acordo com a Declaração Universal dos Direitos Humanos, o artigo 12 afirma que “ninguém será sujeito a interferências arbitrárias em sua vida privada, em sua família, em seu domicílio ou em sua correspondência, nem a ataques à sua honra e reputação” (ORGANIZAÇÃO DAS NAÇÕES UNIDAS, 1948). Esse reconhecimento internacional destaca a importância da intimidade como um direito humano básico. No Brasil, a Constituição Federal de 1988, em seu artigo 5º, inciso X, consagra a inviolabilidade da intimidade e da vida privada, assegurando a proteção da intimidade, da vida privada, da honra e da imagem das pessoas, bem como o direito à indenização pelo dano material ou moral decorrente de sua violação (Brasil, 1988).

Entretanto, o advento das novas tecnologias, como smartphones, redes sociais e plataformas de compartilhamento de dados, transformou profundamente a forma como os indivíduos interagem e compartilham informações pessoais. Segundo a Fundação Getulio Vargas (FGV Direito Rio), em pesquisa iniciada em 2020 sobre a regulação de conteúdo online, as plataformas privadas de mídias sociais podem envolver questões relacionadas à privacidade e a outros direitos fundamentais, evidenciando os desafios decorrentes da utilização dessas tecnologias (FUNDAÇÃO GETULIO VARGAS, 2020). Isso é especialmente evidente nas redes sociais, onde os usuários, muitas vezes sem perceber, compartilham detalhes pessoais que podem ser acessados e explorados por terceiros.

A cultura do compartilhamento e a busca por validação social contribuem para que indivíduos revelem aspectos íntimos de suas vidas, colocando em risco a proteção de sua privacidade. Conforme apontado por Costa e Oliveira (2019), as redes sociais podem afetar os direitos da personalidade, especialmente a privacidade e a proteção de dados pessoais, sendo necessário que os usuários tenham conhecimento sobre a forma como suas informações são tratadas. Essa realidade reforça a importância da educação digital, para que os cidadãos compreendam os riscos envolvidos no compartilhamento de informações e saibam como proteger sua privacidade.

Ademais, a coleta e o uso de dados pessoais por empresas de tecnologia levantam questões sérias sobre a proteção da intimidade. A Lei Geral de Proteção de Dados Pessoais (LGPD), aprovada em 2018, estabelece diretrizes rigorosas para o tratamento de dados pessoais, buscando garantir a privacidade dos indivíduos (Brasil, 2018). No entanto, a implementação da LGPD enfrenta desafios, como a falta de entendimento por parte das empresas sobre suas obrigações legais e a dificuldade em assegurar que os dados sejam tratados de maneira ética e transparente.

Um exemplo emblemático do impacto das novas tecnologias sobre a intimidade é o caso dos vazamentos de dados. Em 2021, informações de mais de 530 milhões de usuários do Facebook foram divulgadas publicamente, conforme informações divulgadas pela Meta (2021). Os dados não foram obtidos por meio de invasão aos seus sistemas, mas por meio da técnica conhecida como *scraping*, utilizada para coletar informações de perfis da plataforma. O caso demonstra como a falta de proteção

adequada pode resultar na violação da intimidade e na exploração indevida de informações pessoais. Este incidente ilustra a vulnerabilidade dos indivíduos em um ambiente digital, onde seus dados podem ser acessados, utilizados e divulgados sem seu consentimento. Como resultado, a proteção da intimidade se torna uma prioridade não apenas para os indivíduos, mas também para os legisladores e as organizações que buscam garantir um ambiente digital seguro.

A proteção dos direitos à intimidade enfrenta desafios complexos diante da influência das novas tecnologias. A rápida evolução das plataformas digitais e a cultura do compartilhamento exigem uma abordagem adaptativa por parte das legislações e da sociedade. É crucial que haja um esforço coordenado entre o governo, o setor privado e a população para promover a educação sobre segurança digital e a proteção da intimidade. A LGPD é um passo importante, mas sua eficácia depende da conscientização e do engajamento de todos os envolvidos. A defesa da intimidade não é apenas uma questão individual, mas uma responsabilidade coletiva que deve ser reforçada em um mundo digital cada vez mais complexo e dinâmico.

Discussão

Os crimes cibernéticos podem ser definidos como atos ilícitos cometidos por meio de dispositivos eletrônicos e da internet. Segundo a Secretaria Nacional de Segurança Pública (SENASP), o enfrentamento dos crimes cibernéticos envolve ações de investigação, prevenção e repressão, além da capacitação dos profissionais responsáveis por essas atividades (Brasil, 2025). O Código Penal Brasileiro (CP) e a Lei nº 12.737/2012 estabelecem diretrizes para a tipificação de diversas condutas ilícitas. O Código Penal, em seu artigo 154-A, tipifica a conduta de invasão de dispositivo informático no Brasil (Brasil, 1940), enquanto a Lei nº 12.737/2012 foi responsável por introduzir essa tipificação no ordenamento jurídico brasileiro (Brasil, 2012). Contudo, a eficácia dessas leis depende da capacidade das autoridades de identificar e processar os infratores.

A falta de conhecimento técnico das autoridades sobre crimes cibernéticos limita a eficácia das investigações e a aplicação da legislação. De acordo com o Ministério Público Federal (Brasil, 2021), a investigação de crimes cibernéticos exige conhecimentos técnicos e jurídicos específicos para a obtenção e análise das provas digitais. Além disso, o acesso à informação e à tecnologia por parte dos criminosos tem aumentado, tornando a identificação de culpados ainda mais complicada. Um dos principais obstáculos à identificação de culpados é o anonimato que permeia o ambiente digital. Criminosos cibernéticos frequentemente utilizam ferramentas como redes privadas virtuais (VPNs), servidores proxy e criptografia para ocultar suas identidades. Segundo Queiroz (2024), mecanismos de anonimização de dados e o compartilhamento de endereços IP dificultam a identificação dos autores e podem comprometer o prosseguimento das investigações criminais. Assim, a ausência de um rastro claro de atividades ilícitas exige investigações tecnicamente sofisticadas e adaptáveis às constantes mudanças nas estratégias dos criminosos.

É importante que o Brasil desenvolva uma atuação integrada no enfrentamento dos crimes cibernéticos, envolvendo não apenas a aplicação de leis, mas também a promoção da educação, conscientização e cooperação internacional. Segundo o Ministério da Justiça e Segurança Pública, a capacitação dos profissionais de segurança pública é fundamental para o desenvolvimento de conhecimentos e habilidades voltados à investigação de crimes cibernéticos, incluindo a preservação, a coleta e a análise de vestígios digitais (Brasil, 2026).

A identificação dos responsáveis por crimes cibernéticos no Brasil envolve diferentes dificuldades, incluindo o anonimato proporcionado pela tecnologia, a evolução constante das táticas criminosas, a aplicação deficiente da legislação e a falta de integração entre as autoridades. Segundo a Secretaria Nacional de Segurança Pública (SENASP), a integração, coordenação e articulação entre as unidades especializadas são fundamentais para fortalecer a prevenção, investigação e repressão aos crimes cibernéticos (Brasil, 2025).

Conclusão

A análise realizada demonstra que o enfrentamento dos crimes cibernéticos e a proteção do direito à intimidade no Brasil ainda apresentam desafios, demandando uma abordagem integrada e colaborativa. A identificação de culpados em delitos cibernéticos é dificultada não apenas pela sofisticação das técnicas utilizadas pelos criminosos, mas também pela ausência de uma formação técnica adequada entre as autoridades responsáveis. Essa deficiência no conhecimento limita a

eficácia das investigações, perpetuando um ciclo de impunidade que só reforça a confiança dos infratores na continuidade de suas atividades ilícitas. Além disso, a fragmentação das informações entre diferentes esferas de governo e instituições de segurança pública prejudica a articulação necessária para um combate eficaz aos crimes cibernéticos. A criação de um sistema de informação integrado que promova o compartilhamento de dados e experiências pode contribuir significativamente para a agilidade e eficiência das investigações, permitindo a identificação de padrões e a atuação coordenada entre diferentes agências. É imperativo que o Ministério da Justiça, a Polícia Federal e outros órgãos desenvolvam protocolos robustos de cooperação, para que a resposta ao crime cibernético seja mais eficaz e abrangente.

Outro aspecto crucial é a educação digital e a conscientização da população. O fortalecimento de iniciativas educativas nas escolas e nas empresas é fundamental para reduzir a vulnerabilidade dos cidadãos, preparando-os para navegar de forma segura no ambiente digital. Campanhas de conscientização, como as promovidas pela FEBRABAN, devem ser ampliadas, enfatizando a importância de reconhecer tentativas de fraudes e a necessidade de proteger informações pessoais (FEBRABAN, 2024). Ao capacitar a população, cria-se um círculo virtuoso que não apenas protege os indivíduos, mas também fortalece a segurança coletiva.

A LGPD representa um avanço significativo na proteção da privacidade dos cidadãos, mas sua eficácia depende de um entendimento claro por parte das empresas sobre suas obrigações legais. A promoção de uma cultura de proteção de dados, juntamente com a fiscalização efetiva, é essencial para garantir que a legislação alcance seu objetivo de proteger os direitos à intimidade. A colaboração entre o governo e o setor privado deve ser intensificada, assegurando que a implementação da LGPD seja uma prioridade.

Além disso, a participação do Brasil em tratados internacionais sobre crimes cibernéticos, como a Convenção de Budapeste (Brasil, 2023), é fundamental para fortalecer a cooperação internacional. A adesão a esses acordos não apenas amplia a capacidade das autoridades brasileiras de combater crimes cibernéticos, mas também promove um padrão global de respostas a esses desafios. A proteção da intimidade, portanto, deve ser encarada como um elemento essencial para a manutenção da confiança social e das instituições democráticas.

Nesse contexto, o enfrentamento dos crimes cibernéticos depende da atuação conjunta do poder público, das instituições responsáveis pela segurança e investigação, das empresas de tecnologia e da própria sociedade. Além do aprimoramento dos mecanismos de investigação e da legislação, é necessário ampliar a conscientização da população sobre os riscos existentes no ambiente digital. Essas medidas podem contribuir para a redução das violações de privacidade e para uma proteção mais efetiva dos direitos fundamentais no meio digital.

Referências

BRASIL. Constituição (1988). Constituição da República Federativa do Brasil de 1988. Brasília, DF: Presidência da República, 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 28 mar. 2026.

BRASIL. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. Código Penal. Brasília, DF: Presidência da República, 1940. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 30 mar. 2026.

BRASIL. Decreto nº 11.491, de 12 de abril de 2023. Promulga a Convenção sobre o Crime Cibernético, celebrada em Budapeste, em 23 de novembro de 2001. Brasília, DF: Presidência da República, 2023. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/d11491.htm. Acesso em: 2 abr. 2026.

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. Brasília, DF: Presidência da República, 2012. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 2 abr. 2026.

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:

https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709compilado.htm. Acesso em: 5 abr. 2026.

BRASIL. Ministério da Justiça e Segurança Pública. Curso sobre crimes cibernéticos está disponível na Rede EaD Senasp. Brasília, DF, 10 set. 2026. Disponível em: https://www.gov.br/mj/pt-br/assuntos/noticias-1/curso-sobre-crimes-ciberneticos-esta-disponivel-na-rede-ead-senasp. Acesso em: 28 set. 2026.

BRASIL. Ministério da Justiça e Segurança Pública. Secretaria Nacional de Segurança Pública**.** Portaria SENASP/MJSP nº 624, de 23 de junho de 2025. Institui a Rede Nacional de Enfrentamento aos Crimes Cibernéticos – Rede Ciber. Brasília, DF, 2025. Disponível em: http://dspace.mj.gov.br/handle/1/15331. Acesso em: 6 ago. 2026.

BRASIL. Ministério Público Federal. Câmara de Coordenação e Revisão, 2. Roteiro de atuação: crimes cibernéticos e provas eletrônicas. 4. ed. atual. e ampl. Brasília, DF: MPF, 2021. Disponível em: https://www.mpf.mp.br/atuacao/ccr2/publicacoes/roteiro-atuacoes. Acesso em: 6 ago. 2026.

COSTA, Ramon Silva; OLIVEIRA, Samuel Rodrigues de. Os direitos da personalidade frente à sociedade de vigilância: privacidade, proteção de dados pessoais e consentimento nas redes sociais. *Revista Brasileira de Direito Civil em Perspectiva*, v. 5, n. 2, p. 22-41, 2019. Disponível em: https://indexlaw.org/index.php/direitocivil/article/view/5778. Acesso em: 8 abr. 2026.

FEBRABAN. Febraban lança hoje campanha antifraudes com Fabio Porchat. 14 out. 2024. Disponível em: https://portal.febraban.org.br/noticia/4196/pt-br/. Acesso em: 8 abr. 2026.

FUNDAÇÃO GETULIO VARGAS. FGV Direito Rio. Regulação de conteúdo online. Rio de Janeiro, 2020. Disponível em: https://direitorio.fgv.br/pesquisa/regulacao-de-conteudo-online. Acesso em: 3 ago. 2026.

META. Entenda os fatos por trás da notícia sobre dados do Facebook. 6 abr. 2021. Disponível em: https://about.fb.com/br/news/2021/04/entenda-os-fatos-por-tras-da-noticia-sobre-dados-do-facebook/. Acesso em: 9 abr. 2026.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS (ONU). Declaração Universal dos Direitos Humanos. Artigo 12. Disponível em: https://brasil.un.org/pt-br/81736-artigo-12-direito-à-privacidade. Acesso em: 9 abr. 2026.

QUEIROZ, Liv Ferreira Augusto Severo. Os crimes cibernéticos no ordenamento jurídico brasileiro: investigação criminal e desafios. *Revista do CNMP*, Brasília, DF, n. 12, 2024. Publicado em: 18 fev. 2025. Disponível em: https://ojs.cnmp.mp.br/index.php/revistacnmp/article/view/707. Acesso em: 6 ago. 2026.

Agradecimentos

Agradeço a Deus, por me conceder força e sabedoria ao longo desta jornada.
À minha família, pelo apoio e incentivo em todos os momentos.
Ao meu orientador, Prof. Dr. Frediano José Galioti Teodoro, pela orientação, disponibilidade e valiosas contribuições para o desenvolvimento deste trabalho.