OS DESAFIOS DO ORDENAMENTO JURÍDICO BRASILEIRO DIANTE DA CRIMINALIDADE DIGITAL

THE CHALLENGES FACING THE BRAZILIAN LEGAL SYSTEM IN THE FACE OF DIGITAL CRIME

https://doi.org/10.63330/aurumpub.066-014

Gabriel Silva Ribeiro
Graduando em Direito do 10º período. Faculdade de Educação Santa Terezinha.
E-mail: tankergabriel50@gmail.com

Maíla Rocha Feitosa Herênio
Advogada Criminalista. Professora. Bacharel em Direito pela Universidade Federal do Maranhão (UFMA). Licenciada em Filosofia (UniBF). Especialista em Direito Tributário (UniBF). Pós-graduanda em Direito Penal.
E-mail: mailarochaadv@gmail.com

Resumo

O avanço das tecnologias da informação e da comunicação, sobretudo com a expansão da internet, transformou as formas de interação social, econômica e jurídica e também ampliou as possibilidades de práticas ilícitas no ambiente virtual. Nesse contexto, os crimes cibernéticos representam um desafio significativo para o Direito Penal e para as autoridades responsáveis pela repressão dessas condutas. O presente artigo analisa os crimes cibernéticos no Brasil, destacando os principais desafios do ordenamento jurídico no combate e na responsabilização dos autores desses delitos no ambiente digital. A pesquisa é qualitativa, exploratória e descritiva, com método dedutivo e procedimentos bibliográfico e documental, fundamentada em legislação, doutrina, jurisprudência e relatórios institucionais. O estudo aborda o conceito e a evolução dos crimes cibernéticos, sua classificação, a legislação brasileira aplicável, as principais modalidades de delitos digitais e os desafios relacionados à identificação da autoria, à produção de provas, à cooperação internacional e à capacitação técnica. A análise evidencia que, embora tenham ocorrido avanços legislativos, como a Lei nº 12.737/2012 e a Lei nº 14.155/2021, a rápida evolução tecnológica ainda exige aprimoramento contínuo das normas e dos mecanismos de investigação. Conclui-se que o enfrentamento da criminalidade digital demanda legislação adequada, investimentos em tecnologia, capacitação profissional, cooperação internacional e medidas de prevenção e educação digital.

Palavras-chave: Crimes cibernéticos; Criminalidade digital; Direito penal; Legislação brasileira; Prova digital.

Abstract

The advancement of information and communication technologies, especially with the expansion of the internet, has transformed social, economic and legal interactions and has also increased the possibilities for illicit practices in the virtual environment. In this context, cybercrimes represent a significant challenge for Criminal Law and for the authorities responsible for repressing such conduct. This article analyzes cybercrimes in Brazil, highlighting the main challenges faced by the legal system in combating and holding perpetrators accountable in the digital environment. The research is qualitative, exploratory and descriptive, using a deductive method and bibliographic and documentary procedures, based on legislation, legal scholarship, case law and institutional reports. The study addresses the concept and evolution of cybercrimes, their classification, applicable Brazilian legislation, the main forms of digital offenses, and challenges related to identifying perpetrators, producing evidence, international cooperation and technical training. The analysis shows that, although legislative advances have occurred, such as Law No. 12,737/2012 and Law No. 14,155/2021, rapid technological development still requires continuous improvement of legislation and investigative mechanisms. It concludes that addressing digital criminality requires adequate legislation, technological investment, professional training, international cooperation, and prevention and digital education measures.

Keywords: Brazilian legislation; Cybercrimes; Criminal law; Digital criminality; Digital evidence.

1 INTRODUÇÃO

A expansão da internet e das tecnologias da informação modificou profundamente a forma como as pessoas se comunicam, realizam atividades econômicas e desenvolvem suas relações sociais. Paralelamente aos benefícios proporcionados pelo ambiente digital, surgiram novas possibilidades para a prática de condutas ilícitas, dando origem e ampliando o campo dos chamados crimes cibernéticos.

Os crimes cibernéticos podem ocorrer em ambientes digitais ou utilizar recursos tecnológicos como instrumento para a prática delitiva. Segundo Bitencourt (2021), os crimes cibernéticos podem ser compreendidos como condutas ilícitas praticadas por meio de sistemas informáticos, com o objetivo de obter vantagem indevida, causar danos ou violar direitos. De forma semelhante, Capez (2022) entende que esses crimes abrangem tanto aqueles que têm o computador como alvo quanto aqueles em que ele é utilizado como instrumento.

De acordo com Pinheiro (2021, p. 45), "os crimes digitais representam uma nova categoria de ilícitos penais que acompanham a evolução tecnológica da sociedade contemporânea". Tal compreensão evidencia que o Direito Penal precisou se adaptar às novas realidades impostas pelo ambiente virtual.

A evolução desses crimes está diretamente ligada ao crescimento da internet. Inicialmente, as

infrações eram simples, como invasões de sistemas e disseminação de vírus. Contudo, atualmente, observa-se a prática de delitos complexos, como fraudes financeiras, estelionato digital, vazamento de dados e ataques cibernéticos em larga escala (Greco, 2021).

Nesse sentido, pode-se afirmar que os crimes cibernéticos evoluíram paralelamente ao desenvolvimento tecnológico, tornando-se mais sofisticados e difíceis de combater, o que exige constante atualização das normas jurídicas e dos mecanismos de investigação.

A presente pesquisa analisa de que maneira o ordenamento jurídico brasileiro tem enfrentado a evolução dos crimes cibernéticos e quais são os principais obstáculos para a efetiva punição dos infratores no ambiente digital.

Para tanto, o artigo examina a eficácia do aparato legal brasileiro no combate aos crimes cibernéticos, identificando os limites da atuação jurídica e as dificuldades processuais no cenário digital contemporâneo.

Além disso, esta pesquisa identifica os tipos de crimes cibernéticos de acordo com a legislação vigente no Brasil; examina as dificuldades técnicas relativas à identificação da autoria e materialidade dos delitos virtuais; e avalia a evolução legislativa brasileira, destacando os avanços e as omissões das leis específicas sobre o tema.

A pesquisa caracteriza-se como qualitativa, de caráter exploratório e descritivo, adotando o método dedutivo e procedimentos de pesquisa bibliográfica e documental. A fundamentação parte das normas constitucionais e dos princípios gerais do Direito Penal brasileiro para chegar às questões específicas relacionadas aos crimes cibernéticos.

2 CONCEITO E EVOLUÇÃO DOS CRIMES CIBERNÉTICOS

Com o avanço das tecnologias da informação e da comunicação, sobretudo com a expansão da internet, surgiram novas formas de interação social, econômica e jurídica. Nesse contexto, também emergiram novas modalidades de delitos, conhecidos como crimes cibernéticos. Tais infrações ocorrem em ambientes digitais ou utilizam recursos tecnológicos como meio para sua prática.

Segundo Bitencourt (2021), os crimes cibernéticos podem ser compreendidos como condutas ilícitas praticadas por meio de sistemas informáticos, com o objetivo de obter vantagem indevida, causar danos ou violar direitos. De forma semelhante, Capez (2022) entende que esses crimes abrangem tanto aqueles que têm o computador como alvo quanto aqueles em que ele é utilizado como instrumento.

De acordo com Pinheiro (2021, p. 45), “os crimes digitais representam uma nova categoria de ilícitos penais que acompanham a evolução tecnológica da sociedade contemporânea”. Tal afirmação demonstra a relação direta entre o desenvolvimento tecnológico e a transformação das formas de criminalidade.

A evolução desses crimes está diretamente ligada ao crescimento da internet. Inicialmente, as infrações eram simples, como invasões de sistemas e disseminação de vírus. Contudo, atualmente, observa-se a prática de delitos complexos, como fraudes financeiras, estelionato digital, vazamento de dados e ataques cibernéticos em larga escala (Greco, 2021).

Nesse sentido, pode-se afirmar que os crimes cibernéticos evoluíram paralelamente ao desenvolvimento tecnológico, tornando-se mais sofisticados e difíceis de combater, o que exige constante atualização das normas jurídicas e dos mecanismos de investigação.

Os crimes cibernéticos podem ser classificados de diversas formas, sendo a mais comum aquela que os divide em crimes próprios e impróprios. Os crimes cibernéticos próprios são aqueles que só podem ser cometidos por meio da tecnologia, como a invasão de dispositivos informáticos. Já os crimes impróprios são aqueles que já existiam no mundo físico, mas passaram a ser praticados também no ambiente virtual, como o estelionato e a difamação (Capez, 2022).

De acordo com Greco (2022), essa distinção é fundamental para a aplicação correta da legislação penal, uma vez que nem todos os crimes digitais possuem tipificação específica. Em muitos casos, utiliza-se a analogia com crimes já previstos no Código Penal. Pinheiro (2020) destaca ainda que outra forma de classificação considera o bem jurídico tutelado, como crimes contra a honra, contra o patrimônio, contra a privacidade e contra a segurança da informação.

A respeito da gravidade desses delitos, Bitencourt (2021, p. 112) afirma: “a internet potencializa o alcance do dano, tornando os crimes cibernéticos mais lesivos do que seus equivalentes tradicionais”. Isso ocorre porque a disseminação de informações na rede é rápida e muitas vezes irreversível.

Assim, a classificação dos crimes cibernéticos é essencial para compreender sua natureza e para possibilitar a aplicação adequada das normas jurídicas.

2.1 LEGISLAÇÃO APLICÁVEL AOS CRIMES CIBERNÉTICOS NO BRASIL

No Brasil, a legislação referente aos crimes cibernéticos tem evoluído nos últimos anos, acompanhando o crescimento dessas práticas ilícitas. Um marco importante foi a Lei nº 12.737/2012, conhecida como Lei Carolina Dieckmann, que tipificou o crime de invasão de dispositivo informático (Brasil, 2012). Posteriormente, o Marco Civil da Internet (Lei nº 12.965/2014) estabeleceu princípios, garantias, direitos e deveres para o uso da internet no país (Brasil, 2014).

Segundo Greco (2022), essas legislações representam avanços significativos, mas ainda são insuficientes diante da complexidade dos crimes digitais. A esse respeito, destaca-se a seguinte citação direta longa de Pinheiro (2021, p. 78):

> A legislação brasileira ainda se encontra em processo de adaptação às novas realidades tecnológicas, sendo necessário o constante aprimoramento das normas para garantir a efetiva proteção dos usuários e a punição dos infratores no ambiente digital.

Além disso, a Lei Geral de Proteção de Dados (Lei nº 13.709/2018) também desempenha papel fundamental na prevenção de crimes cibernéticos, ao estabelecer regras para o tratamento de dados pessoais.

De forma indireta, Capez (2022) ressalta que o ordenamento jurídico brasileiro ainda enfrenta desafios para acompanhar a velocidade das transformações tecnológicas, o que pode gerar lacunas na proteção jurídica. Dessa forma, embora existam avanços legislativos, ainda há necessidade de aprimoramento contínuo para combater de forma eficaz os crimes cibernéticos.

Entre as principais modalidades de crimes cibernéticos, destacam-se o estelionato digital, o phishing, a invasão de sistemas, o furto de dados e os ataques de ransomware. O estelionato digital consiste na obtenção de vantagem ilícita por meio de fraudes realizadas na internet, como a criação de sites falsos ou perfis fraudulentos. Segundo Capez (2022), essa modalidade tem crescido significativamente nos últimos anos, especialmente com o aumento do comércio eletrônico.

O phishing, por sua vez, é uma técnica utilizada para enganar usuários e obter informações confidenciais, como senhas e dados bancários. De acordo com Pinheiro (2021), esse tipo de golpe é um dos mais comuns no ambiente digital. Greco (2022, p. 134) especifica que "o phishing se caracteriza pela manipulação psicológica da vítima, explorando sua confiança para obter dados sensíveis".

Outra modalidade relevante é o ransomware, que consiste no sequestro de dados mediante pagamento de resgate. Trata-se de um crime altamente sofisticado, que pode causar grandes prejuízos a empresas e instituições.

Além disso, há também os crimes contra a honra praticados na internet, como a difamação e a injúria, que ganham maior proporção devido à ampla disseminação de conteúdo nas redes sociais (Capez, 2022). Portanto, os crimes cibernéticos apresentam diversas formas, todas com elevado potencial de dano, o que reforça a necessidade de medidas preventivas e repressivas.

2.2 DESAFIOS NO COMBATE AOS CRIMES CIBERNÉTICOS

O combate aos crimes cibernéticos enfrenta diversos desafios, especialmente em razão das características dessas infrações. Segundo Capez (2022), a identificação dos autores é uma das principais dificuldades, uma vez que os criminosos utilizam técnicas para ocultar sua identidade, como redes privadas virtuais (VPNs) e criptografia.

Além disso, a cooperação internacional é essencial para a investigação desses crimes, já que muitas vezes os servidores e os criminosos estão localizados em diferentes países. Outro desafio importante é a

falta de capacitação técnica das autoridades responsáveis pela investigação, o que pode comprometer a eficácia das ações (Pinheiro, 2020). A esse respeito, Capez (2022, p. 201) destaca que "a ausência de estrutura adequada e de profissionais especializados dificulta significativamente a apuração dos crimes cibernéticos, exigindo investimentos em tecnologia e capacitação para enfrentar essa nova realidade criminal." (Crespo, 2021).

De forma indireta, Greco (2022) também aponta que a rápida evolução tecnológica exige constante atualização dos métodos de investigação e das normas jurídicas. Assim, o enfrentamento dos crimes cibernéticos demanda não apenas legislação adequada, mas também investimentos em tecnologia, cooperação internacional e capacitação profissional.

Diante do exposto, verifica-se que os crimes cibernéticos representam um dos principais desafios do Direito Penal contemporâneo. Sua evolução acompanha o avanço tecnológico, tornando-se cada vez mais complexos e sofisticados. (Crespo, 2021; Nucci, 2022).

A doutrina aponta que, embora haja avanços legislativos, ainda existem lacunas que precisam ser preenchidas para garantir maior efetividade no combate a esses delitos. Além disso, é fundamental investir em prevenção, educação digital e cooperação internacional.

Portanto, a compreensão teórica dos crimes cibernéticos é essencial para o desenvolvimento de estratégias eficazes de enfrentamento, contribuindo para a proteção dos direitos fundamentais no ambiente digital. (Nucci, 2022).

3 CONSIDERAÇÕES E RESULTADOS

A análise dos crimes cibernéticos demonstra que o avanço tecnológico modificou as formas de prática delitiva e trouxe novos desafios para o ordenamento jurídico brasileiro. Condutas que inicialmente estavam relacionadas a invasões de sistemas e disseminação de vírus passaram a abranger fraudes financeiras, estelionato digital, phishing, furto de dados, ransomware e crimes contra a honra praticados na internet.

O estudo identificou que a legislação brasileira apresentou avanços importantes, especialmente com a Lei nº 12.737/2012, o Marco Civil da Internet (Lei nº 12.965/2014), a Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e a Lei nº 14.155/2021. Esses instrumentos compõem a resposta jurídica às transformações do ambiente digital, mas não eliminam todasas dificuldades relacionadasà criminalidade cibernética.

Entre os principais obstáculos estão a identificação da autoria, a produção de provas, a utilização de mecanismos de ocultação de identidade, a falta de capacitação técnica e a transnacionalidade da internet. Tais fatores podem dificultar a investigação e a responsabilização dos infratores.

A pesquisa também evidencia a importância da capacitação técnica das autoridades e dos

investimentos em tecnologia. A existência de normas jurídicas, isoladamente, não garante uma resposta adequada se os órgãos responsáveis pela investigação não dispuserem de estrutura e profissionais preparados para lidar com os recursos utilizados na prática dos delitos.

A cooperação internacional constitui outro elemento fundamental. Como servidores e criminosos podem estar em diferentes países, a investigação frequentemente ultrapassa as fronteiras nacionais. A articulação entre autoridades é necessária para facilitar a obtenção de informações e a responsabilização dos envolvidos.

Conclui-se que o enfrentamento dos crimes cibernéticos exige uma atuação integrada entre legislação adequada, investigação especializada, proteção de dados, capacitação profissional, investimentos tecnológicos, cooperação internacional e prevenção. A constante evolução da tecnologia torna necessária a atualização contínua do ordenamento jurídico e dos mecanismos de investigação.

Assim, a compreensão da criminalidade digital é essencial para o desenvolvimento de respostas jurídicas compatíveis com a realidade contemporânea, contribuindo para a proteção dos direitos fundamentais no ambiente digital.

REFERÊNCIAS

BITENCOURT, Cezar Roberto. **Tratado de direito penal**: parte geral. 27. ed. São Paulo: Saraiva Educação, 2021.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Diário Oficial da União: seção 1, Brasília, DF, 24 abr. 2014.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União: seção 1, Brasília, DF, 15 ago. 2018.

BRASIL. **Lei nº 12.737, de 30 de novembro de 2012**. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Diário Oficial da União: seção 1, Brasília, DF, ano 149, n. 232, p. 1-2, 3 dez. 2012.

BRASIL. **Lei nº 14.155, de 27 de maio de 2021**. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet. Diário Oficial da União: seção 1, Brasília, DF, ano 158, n. 100, p. 1, 28 maio 2021.

CAPEZ, Fernando. **Curso de direito penal**: parte especial. 22. ed. São Paulo: Saraiva, 2022. v. 2.

CRESPO, Marcelo Xavier de Freitas. **Crimes digitais**. 2. ed. São Paulo: Saraiva, 2021.

GRECO, Rogério. **Curso de direito penal**. 19. ed. Rio de Janeiro: Impetus, 2022.

NUCCI, Guilherme de Souza. **Código penal comentado**. 22. ed. Rio de Janeiro: Forense, 2022.

PINHEIRO, **Patricia Peck. Direito digital**. 7. ed. São Paulo: Saraiva, 2021.