

INTRODUÇÃO

As fraudes virtuais, segundo Freitas et al. (2020) são um conjunto de atividades criminosas realizadas no ambiente digital com o objetivo de enganar, roubar ou prejudicar indivíduos, empresas ou organizações. No contexto atual, conforme Araújo (2021), a crescente dependência da *internet* e das tecnologias digitais ampliou a superfície de ataque para os criminosos cibernéticos. Como resultado, a incidência de fraudes virtuais aumentou exponencialmente, causando prejuízos financeiros significativos e levantando preocupações sobre a segurança online. A importância desse tema reside na necessidade urgente de entender e combater essas práticas ilícitas, protegendo os cidadãos e a integridade das infraestruturas digitais.

Esta pesquisa busca responder à seguinte pergunta: quais são os principais desafios e soluções no combate às fraudes virtuais na perspectiva do direito penal? Para abordar essa questão, foram definidos como objetivo geral proporcionar uma compreensão abrangente dos obstáculos enfrentados pelas autoridades na prevenção e punição dessas atividades criminosas e como objetivos específicos: analisar as tecnologias de investigação criminal utilizadas no combate às fraudes virtuais; examinar as implicações da jurisdição penal em crimes eletrônicos que transcendem fronteiras nacionais; investigar o papel das redes sociais e da *Deep Web/Dark Web* na facilitação de fraudes virtuais.

O estado da arte desta pesquisa baseia-se em uma revisão extensa da literatura acadêmica e de relatórios de organizações especializadas em segurança cibernética e direito penal. Estudos recentes como de Martins (2024), Aragão (2015), Freitas et al. (2020) e Junior (2020), destacam a sofisticação crescente dos métodos utilizados pelos criminosos virtuais e a dificuldade das autoridades em acompanhar essas evoluções tecnológicas. Além disso, a legislação atual muitas vezes se mostra inadequada para lidar com a natureza transnacional e anônima desses crimes (BRASIL, 2012a; BRASIL, 2012b). A metodologia adotada foi uma pesquisa bibliográfica de abordagem qualitativa. Realizou-se uma análise documental das legislações relevantes e dos conteúdos disponíveis em portais acadêmicos como o Periódico CAPES, Scientific Electronic Library Online (SciELO) e Google Acadêmico.

O DIREITO PENAL E AS FRAUDES VIRTUAIS

Conforme Aragão (2015), as fraudes virtuais são uma das modalidades mais complexas e desafiadoras de crimes na era digital, envolvendo atividades criminosas que utilizam a tecnologia para enganar e roubar vítimas desavisadas. Essas fraudes podem incluir esquemas de *phishing*, roubo de identidade, e manipulação de sistemas financeiros. Para mais, conforme a legislação os cybercrimes podem ser:

Art. 154-A. Invadir disposto informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismos de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita” (BRASIL, 2012, s.p.).

A necessidade de um arcabouço legal robusto para lidar com essas questões é imperativa, dado o impacto significativo dessas atividades na sociedade. A Lei nº 12.737, de 30 de novembro de 2012, por exemplo, introduziu importantes disposições no Código Penal brasileiro para tipificar delitos informáticos, refletindo a necessidade de atualização constante das leis para acompanhar as evoluções tecnológicas (BRASIL, 2012). Ademais, Araújo (2021) enfatiza que a aplicação do Direito Penal nos crimes virtuais requer uma abordagem específica, considerando a natureza transnacional e anônima desses crimes.

Ademais, Araújo e Aragão (2015) destacam que a jurisdição penal em crimes eletrônicos apresenta desafios únicos, especialmente quando esses crimes ultrapassam fronteiras nacionais. A globalização da *internet* permite que criminosos operem em diferentes jurisdições, complicando a aplicação da lei. Para Campos (2018), a coordenação internacional e a cooperação entre diferentes países são pertinentes para enfrentar esses desafios. No entanto, a falta de harmonização entre as legislações nacionais pode dificultar a persecução penal eficiente desses crimes. Assim, para Araújo (2021), o cybercrime exige uma abordagem integrada e colaborativa entre nações, além de um aprimoramento constante das leis para garantir que estejam sempre alinhadas às novas formas de delitos cibernéticos.

Os estudos de Aragão (2015) e Campos (2018) corroboram que hackers e crackers desempenham papéis distintos, mas igualmente prejudiciais, no universo dos crimes virtuais. Hackers frequentemente são vistos como exploradores de sistemas com fins de melhoria e segurança, enquanto crackers são diretamente associados a intenções maliciosas e criminosas. Para Junior (2020), entender essa diferença é essencial para a formulação de estratégias eficazes de combate. A Lei nº 12.735, de 30 de novembro de 2012, especifica condutas criminosas realizadas com o uso de sistemas eletrônicos, mostrando a preocupação legislativa em diferenciar e tipificar corretamente essas atividades (BRASIL, 2012). A atuação dos crackers, em particular, representa uma ameaça significativa à segurança digital, exigindo respostas legais e tecnológicas cada vez mais sofisticadas.

Fulano (2018) corrobora com isso ao mencionar que a *Deep Web* e a *Dark Web* são frequentemente utilizadas para a realização de atividades ilícitas, incluindo fraudes virtuais. Essas camadas ocultas da *internet* proporcionam anonimato aos criminosos, tornando difícil sua identificação e captura. Martins (2024) argumenta que a natureza anônima e descentralizada desses ambientes digitais apresenta desafios únicos para a aplicação do Direito Penal. Para Aragão (2015), a presença de mercados negros online, onde dados roubados e ferramentas de hacking são comercializados, exemplifica a necessidade de estratégias inovadoras de investigação e persecução penal. A cooperação internacional e o desenvolvimento de tecnologias avançadas são fundamentais para enfrentar esses desafios e garantir a segurança no ciberespaço.

Os crimes cometidos nas redes sociais representam outra dimensão crítica das fraudes virtuais. Freitas et al. (2020) destacam que as plataformas de redes sociais são frequentemente exploradas para disseminar informações falsas, aplicar golpes financeiros e realizar outras atividades fraudulentas. Para Campos (2018), a legislação precisa evoluir para abordar as peculiaridades desses crimes e assegurar a responsabilização adequada dos criminosos. Além disso, o uso de tecnologias como o reconhecimento facial na persecução penal pode oferecer novas ferramentas para identificar e capturar criminosos online (MARTINS, 2024). No entanto, Freitas et al. (2020) também alertam sobre as implicações éticas e de privacidade associadas a essas tecnologias, ressaltando a necessidade de um equilíbrio entre segurança e direitos fundamentais.

Desta maneira, conforme Aragão (2015) e Araújo (2021), a evolução do Direito Penal em resposta às fraudes virtuais e outros crimes cibernéticos é essencial para garantir a justiça e a segurança na era digital. As leis devem ser continuamente atualizadas para enfrentar as novas ameaças apresentadas pela tecnologia, e a cooperação internacional deve ser fortalecida para efetivamente combater crimes que transcendem fronteiras. Estudos como os de Freitas et al. (2020) e Martins (2024) mostram que, além de legislações robustas, a implementação de tecnologias avançadas e o respeito aos direitos fundamentais são relevantes para uma abordagem equilibrada e eficaz no combate às fraudes virtuais e outros crimes cibernéticos. (FREITAS et al., 2020; MARTINS, 2024).

CONCLUSÃO

A análise das fraudes virtuais sob a perspectiva do direito penal revela um cenário complexo e dinâmico, onde a evolução tecnológica traz tanto oportunidades quanto desafios significativos. A compreensão dos mecanismos e estratégias empregadas pelos criminosos virtuais, assim como a eficácia das ferramentas de investigação disponíveis, demonstra que a

legislação atual ainda enfrenta limitações consideráveis. A crescente sofisticação dos métodos utilizados por fraudadores exige uma constante atualização das leis e um aprimoramento das práticas investigativas. O enfrentamento desses crimes demanda uma abordagem integrada que envolva tanto a modernização das normas jurídicas quanto a adoção de tecnologias avançadas para a detecção e prevenção de fraudes virtuais.

Além disso, a jurisdição penal em crimes eletrônicos, especialmente quando estes transcendem fronteiras nacionais, revela a necessidade de uma colaboração mais efetiva entre países e organizações internacionais. A dificuldade de coordenar esforços em um ambiente globalizado e a falta de harmonização entre as legislações nacionais são obstáculos que devem ser superados para que a justiça possa ser efetivamente alcançada.

REFERÊNCIAS

ARAGÃO, David Farias de. **Crimes cibernéticos na pós-modernidade: direitos fundamentais e a efetividade da investigação criminal de fraudes bancárias eletrônicas no Brasil**. 2015. 125 f. Dissertação (Mestrado em Direito e Instituições do Sistema de Justiça) - Universidade Federal do Maranhão, São Luís, 2015.

ARAÚJO, Cláudio Rodrigues. **Análise da aplicação do Direito Penal nos crimes virtuais**. Pensar Acadêmico, Manhuaçu, v.19, n.2, p.494-511, mai./set., 2021.

BRASIL. **Lei n. 12.735, de 30 de novembro de 2012**. Altera o Decreto-Lei 2.848, de 7 de dezembro de 1940 – Código Penal, o Decreto-Lei nº 1.001, de 21 de outubro de 1969 – Código Penal Militar, e a Lei n. 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistemas eletrônicos, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências. Acesso em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/112735.htm

_____. **Lei n. 12.737, de 30 de novembro de 2012**. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei n. 2.848, de 7 de dezembro de 1940 – Código Penal; e dá outras providências. Acesso em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/112737.htm

CAMPOS, Yonara de Vasconcelos. **A evolução do Direito Penal frente às novastecnologias: um estudo sobre os crimes virtuais de natureza sexual**. 21f. Artigo (Graduação em Direito) – Centro de Ciências Humanas e Sociais Aplicadas do Centro Universitário de Maringá, Maringá, 2018.

FREITAS, Victor Valério Medeiros Siqueira; SANTOS, Waldiney Batista; CURY, Leticia Vivianne Miranda. **Crimes virtuais: um olhar sob a ótica do direito penal**. Revista Iberoamericana De Humanidades, Ciências E Educação, 9(5), 1285–1304.

JUNIOR, Júlio César Alexandre. **Cibercrime: um estudo acerca do conceito de crimes informáticos**. Revista Eletrônica da Faculdade de Direito de Franca,

MARTINS, Geovanna Santos. **A atuação do direito penal no combate aos cibercrimes:** perspectivas para a efetividade da justiça digital. Pontifícia Universidade Católica de Goiás, Goiânia-Go, 2024.