Revista Acadêmica de Iniciação Científica 2023; 01:e007
DOI 10.5281/zenodo.10253300
ISSN 2447-6056

ARTIGO DE REVISÃO

CRIMES CIBERNÉTICOS DURANTE A PANDEMIA DE COVID19

CYBER CRIMES DURING THE COVID19 PANDEMIC

Rayssa Viana Freitas[1], Edisio do Ó Loiola Junior[2]

[1]Discente do Curso de Direito da Faculdade de Imperatriz, Imperatriz, Maranhão – Brasil
[2]Docente do Curso de Direito da Faculdade de Imperatriz, Imperatriz, Maranhão – Brasil

E-mail: rayssavianafreitas@hotmail.com

Editor Responsável: Gabriel da Silva Martins

Received: 06/10/2023 **Review:** 22/10/2023 **Accepted:** 07/12/2023

Como citar esse artigo: Freitas RV, Loiola-Junior EÓ. CRIMES CIBERNÉTICOS DURANTE A PANDEMIA DE COVID19. Revista Acadêmica de Iniciação Científica. 2023; 01:e007. https://doi.org/10.5281/zenodo.10253300

Resumo

Introdução: Este artigo científico analisa a ascensão dos crimes cibernéticos durante a pandemia de COVID-19, uma consequência da acelerada digitalização da sociedade global. Abordando desde fraudes online a ataques de ransomware e invasões de privacidade, a pesquisa revela como a dependência crescente da internet criou um terreno fértil para atividades ilícitas. A falta de legislação atualizada e a complexidade da natureza global da internet tornaram a prevenção, rastreamento e punição desses crimes mais desafiantes. A análise abrange categorias variadas de crimes cibernéticos, suas implicações jurídicas, e as respostas legislativas e jurídicas, incluindo jurisprudência e doutrina. A conclusão do estudo aponta para uma necessidade urgente de reformas legais, cooperação internacional, e educação cibernética. **Objetivo**: O objetivo geral deste trabalho é analisar a ascensão dos crimes virtuais durante a pandemia de COVID-19 e avaliar a adequação das estruturas jurídicas existentes para lidar com tais desafios. **Metodologia**: Este estudo foi desenvolvido com uma ampla aplicação das técnicas de pesquisa bibliográfica online nas mais diversas bases de dados que foram compiladas e analisadas de forma científica para alcaçar o objetivo proposto. **Resultados e Discussão**: O trabalho enfatiza que enfrentar os crimes cibernéticos exige uma estratégia multifacetada e cooperativa, envolvendo o fortalecimento das leis, compromisso com a conscientização em segurança cibernética, e efetiva colaboração transnacional, garantindo que a digitalização continue a ser uma força de progresso, e não um vetor de exploração e ameaça. **Conclusão**: O estudo evidenciou que a ascensão dos crimes virtuais não é apenas uma manifestação da adaptabilidade dos criminosos, mas um reflexo de deficiências sistêmicas nas estruturas jurídicas existentes.

Descritores: Crimes Cibernéticos; Pandemia de COVID-19; Legislação e Jurisprudência.

Área de Concentração: Ciências Humanas

INTRODUÇÃO

Crimes virtuais, de forma simplificada, referem-se a atividades ilícitas que ocorrem ou são facilitadas por meios digitais. Estes podem variar desde fraudes e golpes online até invasões de sistemas e sequestro de dados. E, dada a natureza global e descentralizada da internet, esses crimes frequentemente transcenderam fronteiras nacionais, tornando sua prevenção, rastreamento e punição ainda mais complexos.

Revista Acadêmica de Iniciação Científica 2023; 01:e007
DOI 10.5281/zenodo.10253300
ISSN 2447-6056

(BRENNER, 2010) O aumento dos crimes virtuais durante a pandemia não é apenas uma questão de segurança cibernética, mas também tem implicações jurídicas profundas. Com leis e regulamentos que muitas vezes não estão atualizados para lidar com a complexidade e a evolução dos ciberataques, torna-se crucial entender essa nova onda de criminalidade no contexto da pandemia. (SILVA, 2012). Dada a natureza em constante evolução dos crimes virtuais e a falta de uma compreensão jurídica globalmente harmonizada sobre o assunto, surge a questão: como as legislações atuais estão equipadas para lidar com o aumento dos crimes cibernéticos durante a pandemia de COVID-19? E, em um contexto mais amplo, como a sociedade pode se preparar melhor para enfrentar esses desafios no futuro?

O objetivo geral deste trabalho é analisar a ascensão dos crimes virtuais durante a pandemia de COVID-19 e avaliar a adequação das estruturas jurídicas existentes para lidar com tais desafios. Especificamente, buscaremos: (1) entender as categorias de crimes cibernéticos que mais cresceram durante este período; (2) analisar a resposta legislativa e jurídica a esses crimes em diferentes jurisdições; e (3) propor medidas jurídicas e educacionais que possam ajudar a mitigar os impactos desses crimes na sociedade.

METODOLOGIA

Este estudo trata-se de uma revisão de literatura que pode ser categorizada como narrativa, pois seleciona trabalhos acadêmico específicos de uma ampla base de dados analisados, para estruturar um texto de forma a responder o problema da pesquisa e atingir os objetivos propostos. Desta forma a busca em bases de dados como Scielo, Google Scholar foram o ponto de partida para se selecionar os artigos, monografias, dissertações e teses que em embasaram a análise da problemática e foram referenciados ao longo do texto.

De acordo com Gil (2010), a revisão de literatura tem o objetivo de permitir ao pesquisador o contato com o que já foi escrito sobre determinado tema, de modo a assegurar que não esteja redescobrindo o que já é conhecido, mas sim aprofundando ou descobrindo novas perspectivas e abordagens. Além disso, a revisão narrativa, especificamente, não requer uma estrutura pré-definida, o que permite ao pesquisador ter mais liberdade na seleção e interpretação dos estudos.

Lakatos e Marconi (1991) também destacam que a revisão de literatura é um passo fundamental na pesquisa científica. Ela permite identificar as lacunas existentes no conhecimento, o que pode direcionar o pesquisador para áreas ainda pouco exploradas. Através dela, é possível compreender o estado da arte sobre o tema e estabelecer um marco teórico sólido para o estudo.

RESULTADOS E DISCUSSÕES

Crimes virtuais, também referidos como crimes cibernéticos, são delitos que ocorrem no ambiente digital, especificamente através da Internet. Esta classificação engloba uma série de atividades ilícitas que exploram tecnologias de informação e comunicação para perpetrar infrações. Embora a definição de crimes virtuais possa parecer direta, a natureza e o escopo desses crimes têm evoluído rapidamente com os avanços tecnológicos, tornando essencial a atualização constante dos conceitos e definições (BRENNER, 2010). No contexto brasileiro, crimes cibernéticos são entendidos como aqueles que ocorrem em meio eletrônico, digital ou similar, em que o ofendido ou o agente praticante utiliza-se de redes de computadores, ainda que parcialmente (SILVA, 2012).

Revista Acadêmica de Iniciação Científica 2023; 01:e007
DOI 10.5281/zenodo.10253300
ISSN 2447-6056

O universo dos crimes virtuais é vasto e inclui desde fraudes online até espionagem cibernética, cada qual com implicações jurídicas e sociais distintas (GOODMAN, 2011). Importante notar que, enquanto os crimes tradicionais requerem presença física, os crimes virtuais podem ser perpetrados de qualquer lugar do mundo, demonstrando a necessidade de uma cooperação jurídica internacional mais integrada (DEBARDELEBEN & PAVLAKOVICH-KOCHI, 2007).

A taxonomia dos crimes cibernéticos é complexa e diversificada. Uma das principais categorias envolve crimes de propriedade, que incluem fraudes financeiras, phishing e roubos de identidade (WALL, 2008). Outra categoria relevante são os crimes contra a pessoa, como cyberbullying, difamação online e até mesmo crimes mais graves como assédio e ameaças (JEWKES & YAR, 2013). Há ainda os crimes que comprometem a integridade, disponibilidade e confidencialidade das redes e sistemas de computadores, como os ataques de negação de serviço e a disseminação de malware (CLARKE & KNAAKE, 2010).

Além destas, há uma categoria de crimes relacionados ao conteúdo, como a disseminação de pornografia infantil, discursos de ódio e atividades relacionadas ao terrorismo digital (MCGUIRE & HOLT, 2017). Esta classificação, porém, não é exaustiva e é frequentemente atualizada para abordar novos tipos de delitos que surgem com os contínuos avanços tecnológicos.

De acordo com Alves (2020 apud SANTOS e NUNES, 2023) temos que:

> a internet propiciou a geração de um novo perfil de criminoso que com conhecimentos técnicos em informática consideráveis, conduziram a maneira de execução dos delitos convencionais para moldes mais tecnológicos. Os hackers são exemplos de praticantes deste tipo de delito, mas não é algo que se deva generalizar, pois é um termo genérico e pejorativo, haja visto que existem hackers que utilizam do seu conhecimento para praticar boas ações, sendo contratados pelas próprias organizações para melhorem os seus sistemas de segurança, encontrando seus pontos de vulnerabilidade para que possam impedir roubos de identidade e informações sigilosas, ou outros tipos de crimes cibernéticos, antes que outros criminosos percebam as falhas em seu sistema. (ALVES, 2020 apud SANTOS e NUNES, 2023, p.2)

O excerto apresentado de Alves (2020 apud SANTOS e NUNES, 2023) traça uma importante distinção entre o perfil convencional do criminoso e o criminoso cibernético emergente. Este novo perfil ressalta a adaptabilidade e o avanço técnico associado à era digital. Central a essa discussão está o termo "hacker", frequentemente mal interpretado ou usado de forma indistinta pela mídia e pelo público em geral.

O termo "hacker" originalmente se refere a indivíduos com habilidades técnicas avançadas em computadores e redes, que têm paixão por entender e modificar sistemas. Muitos hackers são motivados pela curiosidade e pelo desejo de aprender e compartilhar conhecimento. Em sua essência, um hacker é alguém que explora e inova, geralmente de maneira lúdica, para superar um problema ou limitação técnica. Em contraste, o termo "cracker" é frequentemente usado para descrever indivíduos que usam habilidades semelhantes especificamente para fins maliciosos, como quebrar a segurança de sistemas, cometer fraudes ou disseminar malwares.

Apesar dessas distinções, o termo "hacker" tornou-se popularmente associado a atividades cibernéticas mal-intencionadas, em grande parte devido à representação da mídia. Esta representação, muitas vezes sensacionalista, tem o efeito colateral de obscurecer o papel valioso que muitos hackers desempenham no avanço da tecnologia e na proteção de sistemas. Como Alves aponta, há hackers que são contratados especificamente para identificar e corrigir vulnerabilidades, sendo conhecidos no mundo da cibersegurança como "hackers éticos". Estes profissionais desempenham um papel crucial na defesa contra ameaças cibernéticas, muitas vezes antecipando-se aos crackers para proteger dados e infraestruturas críticas.

Revista Acadêmica de Iniciação Científica 2023; 01:e007
DOI 10.5281/zenodo.10253300
ISSN 2447-6056

Historicamente, o enquadramento jurídico relativo aos crimes cibernéticos foi desafiador devido à sua natureza inovadora e transfronteiriça (GRABOSKY, 2007). Muitos países, inicialmente, tentaram aplicar legislações tradicionais para lidar com delitos virtuais, mas logo perceberam a necessidade de leis específicas (BRENNER, 2007). No Brasil, por exemplo, a Lei Carolina Dieckmann (Lei nº 12.737/2012) foi um dos primeiros instrumentos legislativos que tratou especificamente sobre delitos informáticos, tipificando condutas relacionadas a invasões de dispositivos eletrônicos.

A Lei nº 12.737/2012, conhecida como Lei Carolina Dieckmann, recebeu tal denominação devido a um famoso caso envolvendo a atriz brasileira Carolina Dieckmann, na qual fotos pessoais foram ilegalmente acessadas e divulgadas sem seu consentimento. A lei alterou o Código Penal Brasileiro e tipificou condutas relacionadas a invasões de dispositivos informáticos, estabelecendo penalidades para essas ações. Mais especificamente, tornou crime a invasão de sistemas ou dispositivos eletrônicos com o objetivo de obter, adulterar ou destruir dados sem autorização do titular do dispositivo. (MORAES, 2014). Quer vejamos o que aponta o Art. 154-A

> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:
> Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.
> § 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput.
> § 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.
> § 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:
> Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.

Esta lei aponta alguns detalhes importantes que vêm ser levados em consideração :A Natureza do Crime: O caput do artigo 154-A estabelece claramente o que constitui o crime: a invasão de qualquer dispositivo informático, independentemente de estar ou não conectado à rede de computadores. Isso significa que tanto computadores pessoais quanto sistemas isolados são protegidos por essa lei. A invasão deve ser realizada através da violação indevida de um mecanismo de segurança, indicando que qualquer acesso não autorizado a sistemas protegidos é considerado crime.

Intenção e Resultado da Invasão: O artigo também detalha os propósitos que tornam a invasão um delito, incluindo a obtenção, adulteração ou destruição de dados ou informações sem o consentimento do proprietário do dispositivo. Adicionalmente, a instalação de vulnerabilidades para obter uma vantagem ilícita também é criminalizada, destacando a amplitude da proteção legal contra diferentes tipos de ameaças cibernéticas.

Produção e Distribuição de Ferramentas Maliciosas: O § 1º amplia a abrangência da lei para abordar não apenas aqueles que invadem, mas também os que facilitam a invasão. Aqueles que criam, distribuem ou vendem ferramentas que podem permitir invasões são igualmente responsabilizados, visando frear a proliferação de softwares e dispositivos maliciosos.

Consequências Econômicas: O § 2º aborda situações em que a invasão resulta em prejuízo econômico. Quando há perdas financeiras devido ao crime, a pena é

Revista Acadêmica de Iniciação Científica 2023; 01:e007
DOI 10.5281/zenodo.10253300
ISSN 2447-6056

aumentada, ressaltando a gravidade do impacto econômico causado por crimes cibernéticos.

Violação de Privacidade e Controle Remoto: O § 3º dá ênfase especial às situações em que os conteúdos das comunicações privadas são obtidos, ou quando há a aquisição de segredos comerciais, industriais e outras informações consideradas sigilosas. Também é considerada a situação em que o criminoso obtém controle remoto do dispositivo invadido. Estes são considerados delitos mais sérios, com penas mais rigorosas, evidenciando a alta prioridade dada à privacidade e à segurança da informação.

Esta questão relacionada aos crimes cibernéticos, foi posteriormente incorporada e ampliada pelo Marco Civil da Internet (Lei nº 12.965/2014), que estabeleceu princípios, garantias, direitos e deveres para o uso da Internet no país (MORAES, 2014). Em âmbito internacional, a Convenção de Budapeste sobre Cibercrime, elaborada pelo Conselho da Europa em 2001, é considerada uma das principais referências legislativas, pois busca harmonizar as leis nacionais e melhorar a cooperação jurídica internacional em relação aos crimes cibernéticos (SIEBER, 2002).

O advento da pandemia de COVID-19 forneceu um terreno fértil para a proliferação de fraudes e golpes online, aproveitando o clima de medo e incerteza prevalente na população mundial. Phishing, golpes de caridade falsa e vendas fraudulentas de suprimentos médicos são apenas alguns dos métodos utilizados por cibercriminosos para explorar a situação. Estas ações não só causam prejuízo financeiro, mas também podem ter implicações para a saúde pública ao propagar informações erradas ou falsas esperanças (MCAFEE, 2020).

O Relatório de Ameaças da McAfee Labs, referente a abril de 2021, trouxe novos insights e atualizações sobre o cenário de ciberameaças. De forma notável, o aumento de ataques cibernéticos com temáticas relacionadas à COVID-19 chama a atenção para a adaptabilidade dos cibercriminosos em relação a eventos globais atuais. Com um aumento expressivo de 114%, fica evidente a necessidade de constante vigilância e atualização em mecanismos de defesa cibernética. Outra preocupação se dá com o aumento de malwares para celulares, que cresceram 118%, indicando uma mudança no foco de ataques, possivelmente devido ao uso ampliado de dispositivos móveis no ambiente de trabalho e pessoal (MCAFEE, 2020).

Além disso, com o aumento da demanda por informação confiável sobre o vírus da COVID19, muitos cibercriminosos passaram a utilizar sites falsos ou e-mails de phishing que imitavam organizações de saúde reconhecidas, como a Organização Mundial de Saúde (OMS), para coletar informações pessoais ou disseminar malwares (KASPERSKY, 2020). Esse panorama reforça a necessidade de os usuários serem cautelosos e verificarem as fontes de informações, especialmente em tempos de crise (NORTON, 2021).

Os ataques de ransomware tornaram-se um dos crimes cibernéticos mais temidos, onde os criminosos sequestram dados valiosos das vítimas e exigem um resgate para seu retorno. Durante a pandemia, houve um aumento acentuado desses ataques, visando principalmente instituições de saúde, pesquisa e infraestrutura crítica, aproveitando-se da urgência do contexto da COVID-19 para forçar pagamentos rápidos (SYMANTEC, 2020).

Em particular, hospitais foram alvos significativos de tais ataques, com os criminosos apostando que a necessidade crítica de acessar prontuários de pacientes e sistemas hospitalares levaria a uma maior disposição para pagar resgates. Este cenário não só coloca em risco a segurança da informação, mas também vidas humanas, demonstrando a gravidade ética e moral dos ataques de ransomware em contextos de pandemia (FIREYE, 2020).

Revista Acadêmica de Iniciação Científica 2023; 01:e007
DOI 10.5281/zenodo.10253300
ISSN 2447-6056

Além dos setores de saúde, indústrias e instituições de pesquisa focadas no desenvolvimento de vacinas também se tornaram alvos primários. O roubo de pesquisas relacionadas à COVID-19 representa não apenas um risco econômico, mas também uma ameaça à resposta global à pandemia (CISCO, 2021).

pandemia viu uma explosão no uso das redes sociais como principal meio de comunicação e interação social. Entretanto, essa tendência também levou a um aumento nos casos de cyberbullying e desinformação. Fake news sobre tratamentos, origens do vírus e teorias da conspiração proliferaram, levando a consequências reais, como estigmatização de grupos e comportamentos prejudiciais à saúde (ZHANG & LUO, 2020).

O cyberbullying, em particular, encontrou um novo impulso em meio ao isolamento social, com indivíduos sendo alvo de hostilidade devido à sua origem étnica, condição de saúde ou simplesmente por expressar opiniões divergentes. A circulação de informações errôneas ou mal-intencionadas em plataformas digitais não apenas perpetua o medo e a discriminação, mas também representa um obstáculo significativo para os esforços de contenção da pandemia (SMITH & GALBRAITH, 2021).

Tendo em vista esse panorama, torna-se crucial que as plataformas de mídia social intensifiquem seus esforços para monitorar e combater tanto o cyberbullying quanto a desinformação. O papel das redes sociais como disseminadoras de informação durante a pandemia reforça a importância de garantir a integridade e a veracidade do conteúdo que circula nessas plataformas (MILLER & BARNES, 2020).

Com a rápida digitalização da sociedade e a consequente migração de dados pessoais e financeiros para plataformas online, invasões de privacidade e roubos de identidade tornaram-se preocupações primordiais para indivíduos e organizações. O roubo de identidade ocorre quando criminosos obtêm e utilizam informações pessoais de um indivíduo, sem sua permissão, com o objetivo de cometer fraudes e outros crimes. Eles podem se apropriar de dados como nome, CPF, endereço e informações bancárias para realizar transações ilícitas, abrir contas fraudulentas ou até mesmo solicitar empréstimos em nome da vítima (SANTOS, 2023).

O roubo de identidade não é apenas uma violação da privacidade, mas também uma séria ameaça financeira e, muitas vezes, emocional para as vítimas. Além do impacto econômico direto, a recuperação de uma identidade comprometida pode ser um processo longo e extenuante, exigindo que a vítima entre em contato com diversas instituições para provar sua identidade e corrigir registros falsos (SANTOS, 2023).

Durante a pandemia de COVID-19, a pressa em oferecer assistência financeira à população resultou em oportunidades para criminosos explorarem vulnerabilidades em sistemas bancários digitais. No Brasil, o aplicativo CAIXA TEM, desenvolvido para facilitar o acesso ao auxílio emergencial e outros benefícios, foi um alvo notório. De acordo com reportagens, quadrilhas especializadas conseguiram ativar contas no CAIXA TEM indevidamente, desviando valores destinados aos verdadeiros beneficiários. Estas fraudes causaram não apenas prejuízos financeiros, mas também ampliaram a desconfiança na segurança das transações digitais em um momento crítico (FOLHA PE, 2023).

O excerto de texto aponta informações contra esta prática no Pernambuco:

> A Operação Apate, deflagrada nesta terça-feira (10) pela Polícia Federal (PF), cumpriu nove mandados de busca e apreensão em Alagoas e um na cidade de Águas Belas, no Agreste de Pernambuco, para desarticular uma quadrilha que praticava fraudes no auxílio emergencial. De acordo com a corporação, o esquema criminoso consistia em ativar de forma indevida o Caixa Tem, aplicativo usado pela Caixa Econômica para efetuar os pagamentos do benefício social. Inúmeros CPFs foram usados na fraude. Os números eram cadastrados e validados inapropriadamente, o que levou a vários pagamentos

Revista Acadêmica de Iniciação Científica 2023; 01:e007
DOI 10.5281/zenodo.10253300
ISSN 2447-6056

> fraudulentos dos auxílios emergenciais segundo a polícia. (FOLHA PE, 2023, p.1)

Esta conduta pode ser enquadrada em diversos crimes, entre eles a falsidade ideológica, uma vez que dados falsos ou de terceiros foram utilizados para obtenção de vantagem ilícita; estelionato, devido à apropriação de valores financeiros mediante fraude; e, possivelmente, associação criminosa, considerando a organização e atuação conjunta dos envolvidos na prática das fraudes

A Lei nº 14.155, de 27 de maio de 2021, introduziu importantes modificações no Código Penal Brasileiro no que concerne a crimes praticados no ambiente digital, especialmente fraudes eletrônicas. As alterações foram propostas em um contexto de avanço significativo das atividades criminosas digitais, que passaram a se sofisticar e impactar ainda mais os cidadãos e as instituições financeiras (BRASIL, 2021).

A primeira grande alteração foi no Art. 155, que trata do furto. Com a nova lei, foi inserido o §4º-A, estabelecendo que, quando o crime de furto qualificado for praticado mediante fraude eletrônica ou com o emprego de informações fornecidas pela vítima ou por terceiro induzido a erro por meio de manipulação, artifício, truque ou montagem, a pena será de reclusão de 4 a 8 anos e multa. Esta disposição vem para se adequar ao contexto atual, em que crimes de engenharia social, phishing e outros tipos de fraudes eletrônicas se tornaram comuns (BRASIL, 2021). Quer vejamos a letra de lei:

> Art. 155 [...] § 4º-B. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se o furto mediante fraude é cometido por meio de dispositivo eletrônico ou informático, conectado ou não à rede de computadores, com ou sem a violação de mecanismo de segurança ou a utilização de programa malicioso, ou por qualquer outro meio fraudulento análogo.
> § 4º-C. A pena prevista no § 4º-B deste artigo, considerada a relevância do resultado gravoso:
> I - Aumenta-se de 1/3 (um terço) a 2/3 (dois terços), se o crime é praticado mediante a utilização de servidor mantido fora do território nacional;
> II - Aumenta-se de 1/3 (um terço) ao dobro, se o crime é praticado contra idoso ou vulnerável. (BRASIL, 2021, p.1)

Outra modificação relevante está no Art. 157, que trata do roubo. Foi inserido o §2º-A, que prevê uma pena de reclusão de 4 a 8 anos e multa para casos em que o roubo é cometido com o uso de violência ou grave ameaça exercida por meio de comunicação eletrônica ou outro meio de comunicação à distância. Esta inserção reconhece a evolução da natureza do roubo, adaptando-se às situações em que os criminosos, mesmo à distância, utilizam meios eletrônicos para coagir suas vítimas (BRASIL, 2021).

Ambas as alterações promovidas pela Lei nº 14.155 refletem a necessidade do Direito Penal de se adaptar ao atual cenário de crescente digitalização da sociedade e à sofisticação das práticas criminosas no ambiente digital. Elas representam um esforço do legislador em proteger os cidadãos e, ao mesmo tempo, sinalizam para a sociedade a gravidade destes atos, equiparando-os, em termos de pena, a outros crimes severos previstos no código. Estas modificações legislativas evidenciam uma tendência mundial de endurecimento das penas relacionadas a crimes cibernéticos, dada a amplitude de seu impacto e potencial dano às vítimas (BRASIL, 2021).

Em meio ao cenário da pandemia, a Terceira Seção do STJ consolidou a perspectiva de que a retirada ilícita de fundos de uma conta bancária por meio de transação eletrônica enganosa constitui delito de furto, conforme o artigo 155, parágrafo 4º, inciso II, do Código Penal (STJ, 2023).

Em um cenário onde transações digitais se tornaram mais frequentes devido ao isolamento social, surgiu uma controvérsia relativa à jurisdição adequada para tratar

Revista Acadêmica de Iniciação Científica 2023; 01:e007
DOI 10.5281/zenodo.10253300
ISSN 2447-6056

de furtos executados através da internet. Segundo o STJ, a jurisdição é estabelecida pelo local de onde o recurso foi efetivamente retirado da vítima (STJ, 2023).

Ao deliberar sobre um conflito de competência (CC 145.576) que tratava de um furto via transferência eletrônica oriundo de contas situadas em uma agência em Barueri (SP) - com os fundos sendo direcionados a Imperatriz (MA) -, o tribunal decidiu que o juiz de Barueri seria o competente para a causa, dado que foi nesse município que os fundos foram inicialmente subtraídos (STJ, 2023).

Em alguns crimes cibernéticos ambas as partes, vítima e acusado podem colidir para a consumação de um crime de fraude, Oliveira (2022), relata questões relacionadas a doutrina:

> E quando há uma tentativa de cometer o crime por ambas as partes, qual é o posicionamento jurídico que a legislação brasileira adota? Não há um entendimento pacífico, nesse viés é necessário analisar os entendimentos doutrinários. Para Nélson Hungria, não há crime nenhum, pois a proteção legal só serve para um fim legítimo, tendo como base jurídica o artigo 883, caput do Código Civil, in verbis: "Art. 883. Não terá direito à repetição aquele que deu alguma coisa para obter fim ilícito, imoral, ou proibido por lei" . O posicionamento majoritário é que existe o crime, não importando a má fé do ofendido, entendimento esse adotado por Fernando Capez, que afirma: O autor revela maior temibilidade, pois ilude a vítima e lhe causa prejuízo; (ii) não existe compensação de condutas no Direito Penal, devendo punir-se o sujeito ativo e, se for o caso, também a vítima; (iii) a boa-fé do lesado não constitui elemento do tipo do crime de estelionato; (iv) o dolo do agente não pode ser eliminado apenas porque houve má-fé, pois, a consciência e a vontade finalística de quem realiza a conduta independem da intenção da vítima." Dessa forma, nota-se que mesmo quando a tentativa de fraude é bilateral o posicionamento majoritário é que há crime, pois, a má fé do ofendido não constitui como elemento do tipo do crime. (OLIVEIRA, 2022, p.1)

No contexto da pandemia de COVID-19, crimes cibernéticos, como golpes de phishing relacionados a vacinas ou tratamentos, tornaram-se comuns. Em um cenário hipotético em que tanto o agente quanto a vítima tentam enganar um ao outro, seria possível aplicar as doutrinas de Nélson Hungria e Fernando Capez para interpretar o enquadramento jurídico.

Se considerarmos a perspectiva de Nélson Hungria, de que a má-fé bilateral anula o cometimento do delito, então neste cenário nenhum crime teria ocorrido. Hungria justificaria isso com base no Art. 883 do Código Civil, argumentando que ambas as partes agiram com fins ilícitos, e portanto, a lei não deveria oferecer proteção a nenhum dos lados.

Em contraste, de acordo com o entendimento de Fernando Capez, o crime de phishing seria considerado consumado, independentemente da má-fé da vítima. Capez argumenta que o foco deve estar na ação do sujeito ativo que, neste caso, seria o autor do golpe de phishing. O autor induziria a vítima a erro para obter vantagem ilícita, cumprindo assim os elementos do tipo penal para estelionato eletrônico, conforme o Art. 171 do Código Penal Brasileiro.

Nesse sentido, o consenso majoritário, apoiado pela visão de Capez, defende a ideia de que o crime foi cometido, uma vez que a tipicidade, a ilicitude e a culpabilidade estariam presentes na ação do agente ativo. Esta visão é consistente com os princípios objetivos do Direito Penal Brasileiro, que visam mais à proteção do ordenamento jurídico do que à avaliação da moralidade das partes envolvidas.

A comodidade de comprar online ganhou ainda mais adeptos durante a pandemia, tornando-se essencial para muitos consumidores. Entretanto, essa migração intensificou a exposição a práticas fraudulentas, como plataformas que ofertam mercadorias que jamais chegam ao consumidor (STJ, 2023).

Revista Acadêmica de Iniciação Científica 2023; 01:e007
DOI 10.5281/zenodo.10253300
ISSN 2447-6056

De acordo com uma decisão do STJ (CC 133.534), estabelecer páginas online com a finalidade de comercializar produtos fictícios, sem a intenção de efetivar a entrega, enquadra-se no delito contra a economia popular, de acordo com o artigo 2º, inciso IX, da Lei 1.521/51 (STJ, 2023).

A Corte esclareceu que, ao montar um website para a venda de itens inexistentes, a intenção não é direcionada a enganar vítimas específicas, mas enganar um universo amplo e indeterminado de consumidores que podem se deparar com a oferta enganosa (STJ, 2023).

O caso de um comerciante que atraía consumidores para adquirir produtos virtualmente, os quais não eram entregues, ganhou destaque. A Quinta Turma do STJ, ao analisar um recurso de habeas corpus (RHC 65.056), manteve a ordem de detenção, sustentada, entre outros fatores, na necessidade de preservar a ordem pública e evitar reiterações da prática delitiva. Segundo consta nos autos, o réu mantinha vários domínios online, ofertando eletrônicos, como computadores portáteis e dispositivos fotográficos, com preços abaixo do mercado (STJ, 2023).

Além disso, de acordo com o STJ (2022) uma resposta proativa do sistema judiciário, conforme enfatizado pelo corregedor nacional, foi a promulgação da Lei 13.964/2019 (Lei Anticrime), a qual permitiu a infiltração digital de agentes investigativos com o objetivo de adquirir informações de conexão e cadastro de indivíduos associados a delitos cibernéticos. (STJ, 2022)

Em adição às estratégias legislativas, houve a implementação do Provimento 88/2019 pela Corregedoria Nacional de Justiça. Esta medida incorpora os cartórios extrajudiciais no combate mais assertivo contra práticas de lavagem de dinheiro. (STJ, 2022)

O Provimento N.º 88, de 1º de outubro de 2019, marca uma significativa ampliação dos esforços do Judiciário brasileiro no combate aos crimes de lavagem de dinheiro e ao financiamento do terrorismo. Ele traz diretrizes claras e objetivas sobre as práticas e protocolos que devem ser adotados por notários e registradores, inserindo esses profissionais na linha de frente da luta contra atividades criminosas que têm, na movimentação financeira obscura, sua principal característica. (BRASIL, 2019)

O documento é notável por reconhecer que as práticas de cartório, tradicionalmente vistas como atividades meramente burocráticas, desempenham um papel crucial na identificação e prevenção de operações suspeitas. Ao lidarem com uma ampla gama de transações que envolvem a transferência de propriedade e outros direitos, os notários e registradores estão em uma posição única para detectar anomalias ou inconsistências que podem indicar práticas ilícitas.(BRASIL, 2019)

Ao estabelecer procedimentos e controles específicos, o provimento busca garantir que esses profissionais não apenas reconheçam, mas também relatem qualquer atividade suspeita às autoridades competentes. Isso é feito de forma a proteger o sistema financeiro brasileiro, prevenindo que ele seja utilizado como meio para lavar dinheiro ou financiar atos de terrorismo.

Outra característica notável do Provimento N.º 88/2019 é a ênfase na capacitação e treinamento. É essencial que notários e registradores, bem como seus auxiliares, estejam adequadamente informados sobre as técnicas e métodos mais recentes utilizados por criminosos para lavar dinheiro ou financiar o terrorismo. Dessa forma, eles estarão mais preparados para identificar e, consequentemente, impedir tais práticas. (BRASIL, 2019)

O provimento também destaca a importância da cooperação interinstitucional. É crucial que haja uma comunicação fluida e eficiente entre cartórios e outras entidades, como o COAF (Conselho de Controle de Atividades Financeiras), que desempenha um papel central na detecção e prevenção de operações financeiras ilícitas no Brasil. (BRASIL, 2019)

Revista Acadêmica de Iniciação Científica 2023; 01:e007
DOI 10.5281/zenodo.10253300
ISSN 2447-6056

CONSIDERAÇÕES FINAIS

O cenário imprevisto da pandemia de COVID-19 provocou uma transformação digital sem precedentes, marcada tanto por avanços como por desafios. A emergência sanitária que forçou a sociedade a migrar para o ambiente virtual também revelou uma face sombria: o aumento acentuado dos crimes cibernéticos. Esta pesquisa forneceu uma análise abrangente e crítica dos crimes virtuais durante a pandemia, contemplando desde fraudes e golpes online até ataques de ransomware, cyberbullying e invasões de privacidade.

O estudo evidenciou que a ascensão dos crimes virtuais não é apenas uma manifestação da adaptabilidade dos criminosos, mas um reflexo de deficiências sistêmicas nas estruturas jurídicas existentes. A falta de legislação atualizada e a complexidade inerente à natureza global da internet complicaram os esforços para prevenir, rastrear e punir esses crimes. As diferentes categorias de crimes cibernéticos exploradas no artigo ilustram a amplitude e profundidade dos desafios enfrentados.

A resposta legislativa e jurídica durante a pandemia, apesar de notável, foi, em muitos casos, insuficiente ou inadequada. A análise das jurisprudências e doutrinas, incluindo o comércio virtual e a lavagem de dinheiro, apontou para uma necessidade urgente de reformas legais, cooperação internacional e educação cibernética.

Em conclusão, a pandemia de COVID-19, ao acelerar a transformação digital, revelou uma lacuna crítica na capacidade da sociedade de enfrentar o crescente problema dos crimes cibernéticos. O trabalho demonstrou que essa não é apenas uma questão tecnológica, mas um desafio jurídico e social complexo que requer uma abordagem holística. O futuro deve ver não apenas o fortalecimento das leis e regulamentos, mas também um compromisso com a educação e conscientização sobre segurança cibernética, bem como uma cooperação transnacional efetiva. Somente uma estratégia multifacetada e cooperativa poderá mitigar os impactos dos crimes cibernéticos e garantir que a digitalização continue a ser uma força de progresso e não um vetor de exploração e ameaça.

SUPORTE FINANCEIRO

Não foi necessário nenhum suporte financeiro por se tratar de uma pesquisa de revisão de literatura com fontes de dados online.

CONFLITOS DE INTERESSE

Nenhum conflito de interesse a declarar.

ABSTRACT

Introduction: This scientific article analyzes the rise of cybercrimes during the COVID-19 pandemic, a consequence of the accelerated digitalization of global society. Covering everything from online fraud to ransomware attacks and invasions of privacy, the research reveals how growing dependence on the internet has created fertile ground for illicit activity. The lack of updated legislation and the complexity of the global nature of the internet have made preventing, tracking and punishing these crimes more challenging. The analysis covers varied categories of cybercrimes, their legal implications, and legislative and legal responses, including case law and doctrine. The study's conclusion points to an urgent need for legal reforms, international cooperation, and cyber education. Objective: The general objective of this work is to analyze the rise of cybercrimes during the COVID-19 pandemic and assess the adequacy of existing legal frameworks to deal with such challenges. **Methodology**: This study was developed with a wide application of online bibliographic research

Revista Acadêmica de Iniciação Científica 2023; 01:e007
DOI 10.5281/zenodo.10253300
ISSN 2447-6056

techniques in the most diverse databases that were compiled and analyzed in a scientific way to achieve the proposed objective. **Results and Discussion:** The work emphasizes that tackling cybercrime requires a multifaceted and cooperative strategy, involving the strengthening of laws, a commitment to cybersecurity awareness, and effective transnational collaboration, ensuring that digitalization continues to be a force for progress, and not a vector of exploitation and threat. **Conclusion**: The study showed that the rise of virtual crimes is not just a manifestation of the adaptability of criminals, but a reflection of systemic deficiencies in existing legal structures.

Keywords: Cyber Crimes; COVID-19 pandemic; Legislation and Jurisprudence.

REFERÊNCIAS

BRASIL. **Corregedoria Nacional de Justiça. Provimento N.º 88, de 1º de outubro de 2019**. Dispõe sobre a política, os procedimentos e os controles a serem adotados pelos notários e registradores visando à prevenção dos crimes de lavagem de dinheiro, previstos na Lei n. 9.613, de 3 de março de 1998, e do financiamento do terrorismo. Diário Oficial da União, Brasília, DF, 2 out. 2019. Seção 1.

BRENNER, Susan W. Cybercrime: criminal threats from cyberspace. ABC-CLIO, 2010.

BRENNER, Susan**. Cybercrime and the law**: Challenges, issues, and outcomes. Northeastern University Press, 2007.

CLARKE, Richard A; KNAAKE, Robert K. **Cyber War**: The Next Threat to National Security and What to Do About It. HarperCollins, 2010.

DEBARDELEBEN, Joan; PAVLAKOVICH-KOCHI, Vera. **The security challenges for Canada and Europe in the 21st century**. Canada: Canada-Europe Transatlantic Dialogue, 2007.

FOLHAPE. **Quadrilha usava Caixa Tem para fraudar auxílio emergencial**; há mandado para Agreste. 2023. Disponível em: https://www.folhape.com.br/noticias/quadrilha-ativava-caixa-tem-indevidamente-para-fraudar-auxilio/226293/. Acesso em: [data de acesso, por exemplo, 15 ago. 2023].

GOODMAN, Marc. **Future Crimes**: Everything Is Connected, Everyone Is Vulnerable and What We Can Do About It. Doubleday, 2011.

GRABOSKY, Peter N. **Electronic crime**. Upper Saddle River, NJ: Pearson Prentice Hall, 2007.

GIL, A. C. **Como elaborar projetos de pesquisa**. São Paulo: Atlas. 2010.

JEWKES, Yvonne; YAR, Majid. **Handbook of Internet crime**. Routledge, 2013.

LAKATOS, E. M.; MARCONI, M. de A. **Metodologia do trabalho científico**. São Paulo: Atlas. 1991.

MCGUIRE, Michael; HOLT, Thomas J. **The Routledge Handbook of Technology**, Crime and Justice. Routledge, 2017.

Revista Acadêmica de Iniciação Científica 2023; 01:e007
DOI 10.5281/zenodo.10253300
ISSN 2447-6056

MORAES, Guilherme Peña de. **Marco civil da internet comentado**. Rio de Janeiro: Alta Books, 2014.

OLIVEIRA, Pedro Luis Freitas de. **Crime Cibernéticos**: estelionato virtual na pandemia aos olhos do ordenamento jurídico brasileiro. DIREITO PENAL, 18 out. 2022.

PEREIRA, Tacieli; PITON, Vinícius; ALBRECHT, Evandro Carlos. **Qual a influência da pandemia do covid-19 aos crimes cibernéticos**?. Anuário Pesquisa e Extensão Unoesc São Miguel do Oeste, v. 6, p. e27783-e27783, 2021.

STJ (Superior Tribunal de Justiça). **Crimes pela internet, novos desafios para a jurisprudência.** 2023. Disponível em: https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias-antigas/2018/2018-06-17_06-57_Crimes-pela-internet-novos-desafios-para-a-jurisprudencia.aspx. Acesso em: 16 Ago 2023

SANTOS, Orismar Teixeira dos; NUNES, Nathalia Pereira. **Evolução dos crimes cibernéticos na pandemia**. 2023.

SIEBER, Ulrich. **International review of criminal policy** - Nos. 43 and 44. United Nations, 2002.

SILVA, De Plácido e. **Vocabulário jurídico**. Rio de Janeiro: Forense, 2012.

STJ. **Crime cibernético tomou lugar de roubos e furtos na pandemia, diz ministro Humberto Martins**. 2022. Disponível em: https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/Crime-cibernetico-tomou-lugar-de-roubos-e-furtos-na-pandemia--diz-o-ministro-Humberto-Martins.aspx. Acesso em:

VELOSO, Bárbara Ohanna dos Santos. **Aplicabilidade da lei geral de proteção de dados no contexto da pandemia do COVID-19**: auxílio emergencial–estudo de caso. 2021.

WALL, David S. **Cybercrime: the transformation of crime in the information age**. Polity, 2008.

WANDERLEY, Carlos Alberto Cardoso; DA COSTA, Rodrigo Silva; DE PAULA RIBEIRO, Lara**. Crimes Cibernéticos Em Tempos De Pandemia**: O Isolamento Social Como Propulsor Da Vulnerabilidade Da População E Do Aumento Dos Casos. Facit Business and Technology Journal, v. 1, n. 37, 2022.