Tema:
Neurociência e Inteligência artificial:
As novas interfaces do conhecimento

ASCENSÃO DOS CRIMES CIBERNÉTICOS PÓS COVID-19

Matheus MESTRINELLI [1]

RESUMO: Este artigo científico se propõe a analisar os crimes cibernéticos no Brasil, uma consequência da acelerada digitalização da sociedade global. A análise desenvolvida abrange categorias variadas de crimes cibernéticos, investigação e autoria, suas implicações e as respostas legislativas e jurídicas, incluindo jurisprudência e doutrina. A pesquisa analisa também o aumento desses crimes durante a pandemia de COVID-19. Este estudo foi desenvolvido por meio de aplicação das técnicas de pesquisa bibliográfica. A conclusão da pesquisa indica que a ascensão desses crimes não se deve apenas à adaptabilidade dos criminosos, mas reflete deficiências sistêmicas nas estruturas de fiscalização, o que aponta para uma necessidade urgente de conscientização em segurança cibernética e reformas legais.

Palavras-chave: Crimes cibernéticos; COVID-19; Legislação; Internet.

1 INTRODUÇÃO

A internet foi o início de um grande avanço dentro do contexto do mundo globalizado, onde se destaca o fácil acesso e a rapidez na busca de informação, pois basta entrar em um site e escrever o que procura para obter resultados de forma imediata. Com a popularização da internet em diversos lares e locais, crimes já tipificados pelo Código Penal começaram a ser cometidos no ambiente virtual, onde o criminoso permanece "oculto na rede", dificultando a identificação do autor dos delitos. Nesse contexto, novas formas de crimes

[1] Discente do 4º ano do curso de Direito do Centro Universitário Antonio Eufrásio de Toledo de Presidente Prudente. matheusmestrinelli@toledoprudente.edu.br

emergiram, conhecidas como Crimes Cibernéticos, que, embora façam parte da realidade tanto global quanto brasileira, ainda carecem de uma legislação específica no ordenamento jurídico do Brasil.

O aumento dos crimes virtuais durante a pandemia não se trata apenas de uma questão de segurança cibernética, mas também envolve profundas implicações jurídicas. Diante da natureza em constante evolução dos crimes virtuais e da falta de uma compreensão jurídica globalmente harmonizada sobre o tema, surge a indagação: como as legislações atuais estão preparadas para enfrentar o aumento dos crimes cibernéticos? E, em um contexto mais amplo, como a sociedade pode se preparar de maneira mais eficaz para enfrentar esses desafios futuros?

Os crimes virtuais, de forma simplificada, referem-se a atividades ilícitas realizadas ou facilitadas por meios digitais. Estes englobam desde fraudes e golpes online até invasões de sistemas e sequestro de dados. Devido à natureza global e descentralizada da internet, esses delitos frequentemente transcendem as fronteiras nacionais, o que torna sua prevenção, rastreamento e punição ainda mais complexos.

O presente trabalho tem como objetivo geral analisar os aspectos que circundam crimes cibernéticos e como o direito brasileiro se porta diante desses novos delitos, também 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, busca-se compreender as categorias de crimes cibernéticos que mais se proliferaram durante este período; analisar a resposta legislativa e jurídica a esses crimes em diferentes jurisdições; propor medidas jurídicas e educacionais que possam mitigar os impactos desses crimes na sociedade.

2 CRIMES CIBERNÉTICOS

Crimes virtuais, também conhecidos como crimes cibernéticos, são infrações cometidas no ambiente digital, em particular por meio da Internet. Essa categoria abrange uma variedade de atividades ilícitas que se aproveitam das tecnologias de informação e comunicação para realizar atos criminosos. Embora a definição de crimes virtuais possa parecer simples, a natureza e o alcance desses

delitos têm se expandido rapidamente com os avanços tecnológicos, exigindo uma constante atualização dos conceitos e definições. No contexto brasileiro, crimes cibernéticos são compreendidos como aqueles que ocorrem em meio eletrônico, digital ou similar, em que tanto o ofensor quanto a vítima utilizam-se de redes de computadores, mesmo que de forma parcial.

O campo dos crimes virtuais é extenso, abrangendo desde fraudes online até espionagem cibernética, cada uma com diferentes implicações jurídicas e sociais. Vale destacar que, enquanto os crimes tradicionais exigem a presença física, os crimes virtuais podem ser cometidos de qualquer lugar do planeta, evidenciando a necessidade de uma cooperação jurídica internacional mais estreita.

A classificação dos crimes cibernéticos é complexa e diversificada. Uma das principais categorias envolve crimes contra a propriedade, como fraudes financeiras, *phishing* e roubo de identidade. Outra categoria importante são os crimes contra a pessoa, como cyberbullying, difamação online e até mesmo crimes mais graves, como assédio e ameaças. Existem também os crimes que comprometem a integridade, disponibilidade e confidencialidade das redes e sistemas de computadores, como ataques de negação de serviço e disseminação de malware.

Além disso, há uma categoria relacionada ao conteúdo, incluindo a disseminação de pornografia infantil, discursos de ódio e atividades associadas ao terrorismo digital (MCGUIRE & HOLT, 2017). No entanto, essa classificação não é definitiva e é frequentemente revisada para incluir novos tipos de delitos que surgem com o avanço contínuo da tecnologia.

A autora contemporânea Patrícia Peck Pinheiro em seu livro Direito Digital (2007), define com exemplos duas modalidades de crimes virtuais, que segue abaixo:

> Os crimes virtuais têm modalidades distintas, dependendo do bem jurídico tutelado. Nesse sentido, podemos dar como exemplo o crime de interceptação de dados, que tem como bem jurídico tutelado os dados, ou seja, o que se quer é proteger a transmissão de dados e coibir o uso dessas informações para fins delituosos, como, por exemplo, captura de informações para envio de “e-mail bombing[2]”, e o “e-mail com vírus[3]”, o

[2] **E-mail Bombing** – é o envio de e-mails imensos ou vários e-mails, por isso Bombing, que se refere como “explosão, ou bomba” em inglês. De qualquer forma pode vir a causar atraso na recepção e

> "spam[4]". Esse tipo penal protege também a questão da inviolabilidade das correspondências eletrônicas. (PINHEIRO, 2007)

Existe uma classificação que divide os crimes cibernéticos em dois tipos: os Crimes Cibernéticos Próprios e os Crimes Cibernéticos Impróprios. Os quais serão abordados a seguir.

2.1 Crimes Cibernéticos Próprios

São crimes que podem ser cometidos unicamente no ambiente digital, onde tanto a execução quanto a consumação ocorrem nesse meio. Consistem em novos tipos de delitos em que o bem jurídico protegido é a informática, sendo direcionados contra os dados da vítima que utiliza um computador ou celular. Os agentes causadores são denominados *hackers*, e atuam por meio da invasão de sistemas, modificação, alteração, inserção de dados ou informações falsas. Essas condutas atingem diretamente os softwares dos computadores, que geralmente são invadidos através de Pen drives, e-mails ou por arquivos que que contém algum vírus, que quando ativado se espalha cada vez mais, danificando diversos arquivos e programas.

2.2. Crimes Cibernéticos Impróprios

Os crimes cibernéticos impróprios são aqueles tipificados no Código Penal, pois violam bens jurídicos comuns e ferem à dignidade da pessoa humana. Com relação ao patrimônio, tem-se uma certa dificuldade em reconhecer os crimes

---

gasto adicional com conta de internet, por exemplo. Nesses casos seria aplicável o art. 163 do Código Penal (crime de dano).

[3] **E-mail com vírus** – é quando a pessoa recebe um e-mail, e vem anexado um vírus, é muito comum nos dias de hoje, e-mails com tentativas de vírus através de propostas bancárias, ou solicitação de dados por e-mail. Nesse sentido a legislação prevê os artigos 151, § 1º, II e III, e 163 do Código Penal, com aplicação do artigo 65 da LCP, com pena de prisão simples de 15 dias a 2 meses, ou multa por perturbação da tranquilidade.

[4] **Spam** – Propaganda maciça na Internet, feita em geral com software especialmente projetado para enviar solicitações aos usuários por meio de e-mail

cibernéticos impróprios, pois não se consegue tipificar a informação armazenada como um bem material, mas sim um bem imaterial, insuscetível de apreensão como objeto, por exemplo, os crimes de transferência de valores em contas bancárias, no qual os criminosos utilizam-se dos sistemas informáticos apenas como *animus operandi*, ou seja, furtando dinheiro da conta da vítima através de um sistema interligado à internet.

2.3. Investigação e autoria dos crimes cibernéticos

No tocante à investigação dos crimes cibernéticos, temos como plano normativo o artigo 1º da Lei de Organização da Investigação Criminal, (Lei nº 49/2008) com a ressalva de que sua última versão tem como parâmetro a Lei nº 57/2015; no que tange as seguintes informações:

> A investigação criminal compreende o conjunto de diligências que, nos termos da lei processual penal, se destinam a averiguar a existência de um crime, determinar os seus agentes e a sua responsabilidade e descobrir e recolher as provas, no âmbito do processo. (BRASIL, 2015)

A investigação fica a cargo do Ministério Público e das Policias Judiciárias dependendo do crime. Nos crimes cibernéticos, a perícia é um dos melhores métodos para se identificar a materialidade e a autoria delitiva. Geralmente a perícia é realizada na fase policial em virtude da urgência e da necessidade de ser feita de imediato ou o mais rápido possível após o acontecimento do crime. Salienta-se que o perito deve ser especializado, pois à medida que os meios de consumação dos crimes cibernéticos se atualizam, os fiscais devem acompanhar tais mudanças.

Quanto à autoria dos crimes cibernéticos, um dos grandes problemas a ser enfrentado é a dificuldade de localizar o autor do fato, pois os criminosos muitas vezes se escondem atrás de um dispositivo, sendo computador, tablet, ou celulares por exemplo, outro fator que aumenta a dificuldade é a utilização de perfis falsos para cometer os crimes, dificilmente o autor vai utilizar dados verdadeiros. Deste modo, já que os usuários dificilmente são identificados através de fotos ou documentos, a autoria fica vinculada através de um IP do dispositivo utilizado para o crime.

O Superior Tribunal de Justiça (STJ) tem interpretado normas infraconstitucionais em relação aos ilícitos praticados pela rede. O tribunal, por exemplo, decidiu manter preso preventivamente um rapaz de 19 anos que, por meio das mídias sociais, compelia jovens (algumas menores de idade) a enviar fotos e vídeos íntimos e depois exigia que elas lhe entregassem dinheiro e outros bens para não divulgar o material na internet. Ele também estendia as ameaças às famílias das vítimas.

Para o ministro Rogerio Schietti Cruz, relator do caso, ficou nítido que o acusado se aproveitou da vulnerabilidade das vítimas no ambiente virtual para exigir os valores, que eram cada vez mais altos a cada ato de extorsão. Ao negar pedido de Habeas Corpus, Schietti destacou que os crimes sexuais virtuais são impulsionados pela oportunidade do anonimato e, independentemente dos aspectos que permeiam a vida pessoal e socioeconômica do criminoso, estariam “diretamente relacionados ao comportamento sexista, comumente do gênero masculino” (processo em segredo de justiça).

3 LEGISLAÇÕES COMPETENTES PARA OS CRIMES CIBERNÉTICOS

Considerando a facilidade de acesso à internet nos dias atuais, é notório que a legislação ainda está em processo de formação e adaptações. Dessa forma, até um passado recente os crimes praticados em ambientes virtuais eram tipificados analogicamente em tipos penais comuns (TAVARES, 2012).

3.1 Lei Carolina Dieckmann

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. Ressalta-se que a referida lei transitava na câmara desde 1999, mas só foi sancionada após a comoção do caso da atriz, introduzindo então no Código Penal brasileiro o tipo nominado “Invasão de dispositivo informático”, sobre isso dispõe Masson:

> Como de praxe, os debates sobre uma legislação específica para os crimes ligados à internet (crimes cibernéticos) se arrastavam há anos, em velocidade de conexão discada. Mas a atividade dos congressistas, impulsionada pela opinião pública, recebeu imenso upload depois da invasão do computador pessoal de Carolina Dieckmann. (Masson, 2017)

Inicialmente a pena era de detenção de três meses a um ano para esses crimes, entretanto em 2021 foi aprovada a lei nº 14.155/21 que aumentou a pena para um a quatro anos de reclusão.

O artigo 154-A, trata de quando o criminoso invade um dispositivo utilizando-se de um meio fraudulento para romper os mecanismos de segurança e praticar os delitos. Trazendo nos parágrafos 1º, 2º e 3º, que atenua a pena quando a invasão resulta prejuízo econômico, ou que contenha informações sigilosas, ou comunicações eletrônicas privadas. Outrossim a pena é aumentada em 2 terços se o conteúdo for comercializado ou transmitido a terceiros.

Já o artigo 266 estabelece regulamentação sobre quem pratica o crime impedindo ou dificultando informações de utilidade pública, e de quem usa dos dados para falsificação de documentos. Outro artigo que foi contemplado no Código Penal, através da Lei Carolina Dieckmann, é o artigo 298 que trata da falsificação de cartões, que é um crime recorrente na atualidade.

3.2 Marco Civil da Internet

O Marco Civil da Internet, lei nº 12.965/14, criado pelo Poder Executivo em 23 de abril de 2014, tem como objetivo garantir a defesa dos consumidores que utilizam a internet para realizar comércio, seja adquirindo produtos e serviços ou oferecendo aos consumidores, assegurando a livre iniciativa, bem como a livre concorrência. Regulamentando também os serviços prestados por multinacionais provedoras de internet.

> Sobre a intenção do marco civil da internet Siqueira leciona: A lei do Marco Civil foi criada para suprir as lacunas no sistema jurídico em relação aos crimes virtuais, num primeiro momento tratando dos 17 fundamentos, conceitos para sua interpretação e objetivos que o norteiam, além de

> enumerar os direitos dos usuários, tratar de assunto polêmicos como por exemplo a solicitação de histórico de registros, a atuação do poder público perante os crimes virtuais e por último garante o exercício do direito do cidadão de usufruir da internet de modo individual e coletivo estando devidamente protegido. (Siqueira 2017, p. 126).

Essa lei estabeleceu princípios, garantias, direitos e deveres para o uso da internet, bem como determinou as diretrizes para atuação da União, Estados e municípios, tendo como fundamentos o respeito à liberdade de expressão, reconhecimento da escala mundial de rede, exercício da cidadania em meios digitais, pluralidade e diversidade, proteção da privacidade e dados pessoais, na forma da lei. O art. 3º traz outros princípios, como o estímulo a boas práticas, responsabilização dos agentes em conformidade com a lei.

O artigo quarto teve como assunto central a promoção do direito ao acesso à internet para todos, prezando também o acesso à informação ampliando e fomentando novas tecnologias e pesquisa. Desta forma, o Marco Civil da Internet surgiu para regular as ações tomadas na internet estipulando os direitos e deveres de quem à utiliza. Tendo em vista que a internet é a maior fonte de informações de hoje em dia, buscou-se regulamentar os tráfegos de dados e minimizar os problemas que ocorrem na rede.

3.3 Lei Geral de Proteção de Dados

A regulamentação da proteção de dados pessoais no âmbito da persecução penal se revelou urgente por ordem constitucional direta. Com a promulgação da Emenda Constitucional nº 115/2022, que acrescentou o inciso LXXIX ao artigo 5º da Constituição Federal, nesse cenário a Lei Geral de Proteção de Dados (Lei n.º 13.709/2018), foi sancionada em 2018, mas entrou em vigor somente no ano de 2020. Ela veio com o objetivo de estabelecer uma segurança jurídica e proteger os dados pessoais de todos os cidadãos presentes no território brasileiro.

No entanto, no contexto da LGPD, a proteção de dados pessoais carece de previsão legal quanto às investigações criminais e ações penais, seara em que os direitos e garantias fundamentais dos indivíduos são mais relativizados. No

Legislativo, o caminho para suprir o atual vácuo normativo e contemplar o tratamento de dados pessoais no âmbito criminal já teve início com a apresentação à Câmara dos Deputados, em novembro de 2020, do Anteprojeto de Lei de Proteção de Dados para Segurança Pública e Persecução Penal, realizado por comissão de juristas liderada pelo então ministro do STJ, Nefi Cordeiro.

A análise do anteprojeto revela que, se aprovado no parlamento, o projeto de lei desempenhará um papel crucial na proteção dos direitos e garantias fundamentais dos titulares de dados, ao mesmo tempo em que proporcionará segurança jurídica aos meios de investigação legítimos e adequados às inovações tecnológicas. Baseada em importantes estatutos jurídicos do direito comparado, como a Diretiva 680/2016 da União Europeia e legislações dos Estados Unidos, a chamada LGPD-Penal elevará o ordenamento jurídico brasileiro, nesta área, aos padrões internacionais.

4 CRIMES CIBERNÉTICOS NO CONTEXTO DA PANDEMIA DE COVID-19

O advento da pandemia de COVID-19 criou um ambiente propício para a proliferação de fraudes e golpes online, como *cibercriminosos* valendo-se da atmosfera de medo e insegurança que permeava a população global. Entre os métodos mais comuns utilizados por esses criminosos estão as práticas de golpes envolvendo falsas instituições de caridade e a venda fraudulenta de suprimentos médicos. Essas ações não apenas resultam em prejuízos financeiros significativos para as vítimas, mas também podem ter sérias implicações para a saúde pública, ao disseminar desinformação e criar falsas esperanças em um momento de crise global.

O Relatório de Ameaças da McAfee Labs, referente a abril de 2021, trouxe novos *insights* e atualizações sobre o cenário de “ciberameaças”. Com um aumento expressivo de 114% é notável a adaptabilidade de criminosos em face dos cenários em que se encontram, evidenciando 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.

Com a rápida digitalização da sociedade e a consequente transferência de dados pessoais e financeiros para plataformas online, as invasões de privacidade e o roubo de identidade se tornaram questões de grande preocupação para indivíduos e organizações. O roubo de identidade ocorre quando criminosos obtêm e utilizam informações pessoais de uma pessoa, sem sua autorização, com o propósito de cometer fraudes e outros delitos. Esses criminosos podem se apropriar de dados como nome, CPF, endereço e informações bancárias para realizar transações ilegais, abrir contas fraudulentas ou até mesmo solicitar empréstimos em nome da vítima (SANTOS, 2023).

Ademais, com o crescimento da busca por informações confiáveis sobre o vírus da COVID-19, diversos “cibercriminosos” começaram a empregar sites falsos ou e-mails de *phishing* (tipo de ciberataque que persuade as pessoas a tomar uma ação que dá a um golpista acesso ao seu dispositivo, contas ou informações pessoais) que simulavam ser de organizações de saúde renomadas, como a Organização Mundial da Saúde (OMS), com o intuito de coletar dados pessoais ou espalhar *malwares* (software malicioso, escrito intencionalmente para prejudicar os sistemas de computador ou seus usuários).

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).

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. 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.

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.

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).

5 CONCLUSÃO

Ao final da pesquisa, conclui-se que o tema abordado é de extrema relevância nos dias atuais, especialmente porque representa uma prática em ascensão, 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, revelando uma lacuna crítica na capacidade da sociedade de enfrentar o crescente problema dos crimes cibernéticos. O uso massivo da internet e de tecnologias digitais transformou os padrões de criminalidade, permitindo que novas modalidades de delitos, como os crimes cibernéticos, proliferem com maior intensidade e sofisticação.

No Brasil, crimes como os contra a honra, a divulgação não autorizada de fotos, e a pedofilia e pornografia infantil têm ocorrido com preocupante frequência, especialmente no ambiente virtual. Os responsáveis por esses atos ilícitos frequentemente não enfrentam punições proporcionais às suas condutas, o que gera uma sensação de impunidade. As vítimas, por sua vez, sofrem

consequências que transcendem o espaço digital, impactando profundamente sua vida íntima e causando danos psicológicos e sociais que podem perdurar por longos períodos.

O Código Penal brasileiro tipifica diversas condutas que ocorrem na internet, mas as penas previstas ainda são consideradas brandas e insuficientes para dissuadir a prática desses crimes. A introdução da Lei nº 12.737/2012, conhecida como Lei Carolina Dieckmann, que alterou o Código Penal para incluir crimes cibernéticos, foi um passo importante. O Marco Civil da Internet também promoveu através de princípios e fundamentos maior garantia à proteção do usuário. No entanto, a legislação ainda apresenta lacunas, resultando em interpretações ambíguas e punições leves, o que enfraquece sua eficácia.

Para enfrentar esses desafios, é fundamental promover uma revisão legislativa que endureça as penas para crimes cibernéticos, assegurando que as punições sejam adequadas à gravidade dos atos cometidos. Além disso, é necessária a criação de uma legislação específica e abrangente para crimes cibernéticos, que contemple as particularidades do ambiente virtual e ofereça clareza jurídica.

Outra solução envolve a capacitação das autoridades policiais e judiciárias para lidar com crimes digitais, garantindo que tenham os recursos técnicos e conhecimento necessários para investigar e processar esses casos de forma eficaz. A cooperação internacional também deve ser fortalecida, dada a natureza transnacional dos crimes cibernéticos.

Por fim, campanhas de conscientização pública sobre os riscos e responsabilidades no uso da internet são essenciais para prevenir a ocorrência desses crimes e incentivar as vítimas a buscarem proteção e justiça. A combinação de medidas legislativas, educativas pode contribuir para a criação de um ambiente digital mais seguro e justo, onde os direitos e a dignidade das pessoas sejam efetivamente protegidos.

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 1 998, e do financiamento do terrorismo. Diário Oficial da União, Brasília, DF, 2 out. 2019. Seção 1.

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: 25 agosto 2024

MASSON, Cleber. Código Penal comentado. 5ª ed. São Paulo: Método, 2017.
MEDEIROS, Claudia Lucio de. **Deficiências da legislação penal brasileira frente aos crimes cibernéticos**. 2010.

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

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

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

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: 26 agosto 2024