UNIVERSIDADE FEDERAL DE MATO GROSSO DO SUL

CURSO DE DIREITO – CPTL

CAIO ERIK PEREIRA THOMÉ

A PROBLEMÁTICA SOBRE A APURAÇÃO DA AUTORIA NOS CRIMES CIBERNÉTICOS E A ATUAÇÃO DOS NÚCLEOS ESPECIALIZADOS DE INVESTIGAÇÃO

TRÊS LAGOAS, MS
2023

CAIO ERIK PEREIRA THOMÉ

A PROBLEMÁTICA SOBRE A APURAÇÃO DA AUTORIA NOS CRIMES CIBERNÉTICOS E A ATUAÇÃO DOS NÚCLEOS ESPECIALIZADOS DE INVESTIGAÇÃO

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Direito do Campus de Três Lagoas da Universidade Federal de Mato Grosso do Sul, como requisito parcial para obtenção do grau de Bacharel em Direito, sob a orientação do Professor Doutor Luis Renato Telles Otaviano.

TRÊS LAGOAS, MS
2023

CAIO ERIK PEREIRA THOMÉ

A PROBLEMÁTICA SOBRE A APURAÇÃO DA AUTORIA NOS CRIMES CIBERNÉTICOS E A ATUAÇÃO DOS NÚCLEOS ESPECIALIZADOS DE INVESTIGAÇÃO

Este Trabalho de Conclusão de Curso foi avaliado e julgado aprovado em sua forma final, como requisito parcial para obtenção do grau de Bacharel em Direito, perante Banca Examinadora constituída pelo Colegiado do Curso de Graduação em Direito do Campus de Três Lagoas da Universidade Federal de Mato Grosso do Sul, composta pelos seguintes membros:

Professor Doutor Luis Renato Telles Otaviano
UFMS/CPTL - Orientador

Professora Doutora Heloisa Helena de Almeida Portugal
UFMS/CPTL - Membro

Dr. Moisés Casarotto
UFMS/CPTL – Membro externo

Três Lagoas - MS, 16/11/2023.

DEDICATÓRIA

Dedico esse trabalho às pessoas mais importantes da minha vida:

Minha mãe, Ebna Dork Pereira Rosa;

Meu pai, Levair Thomé;

Meu irmão e melhor amigo, Cauan Henry Pereira Thomé;

Minha namorada e companheira de lutas, Ísis de Azevedo Ravanhani.

AGRADECIMENTOS

Gostaria de demonstrar a minha gratidão máxima à todos aqueles que de alguma forma me auxiliaram, me ouviram, me instruíram e acima de tudo: estiveram ao meu lado durante esses cinco anos de graduação.

Aos meus pais Ebna Dork Pereira Rosa Thomé e Levair Thomé que, mesmo diante da distância e das adversidades sempre estiveram ao meu lado me apoiando, me incentivando a perseguir os meus sonhos e a lutar pelos meus objetivos, bem como me deram educação e princípios que levarei pela vida toda.

À minha namorada e companheira Ísis de Azevedo Ravanhani, que desde o nosso primeiro dia de namoro sempre me incentivou a continuar estudando e me dedicando, além de me ajudar nos momentos em que mais precisei, seja como namorada, seja como amiga ou conselheira.

Ao meu irmão Cauan Henry Pereira Thomé, que é o maior presente que eu poderia ter recebido ao longo de toda a minha vida. Nenhuma das batalhas que lutei ao longo da minha trajetória teriam sentido sem a presença do Cauan.

Ao amigo e Assessor Jurídico Rafael Roble de Oliveira, que dedicou horas do seu tempo para me ensinar, me apoiar e acima de tudo me orientar desde o início da minha jornada no mundo jurídico. Ao Dr. Moisés Casarotto, Promotor de Justiça, que sempre se mostrou prestativo e me deu oportunidades de crescimento profissionais pelas quais sempre serei grato. 8ª PJ de Três Lagoas, minha gratidão a vocês.

A todos os amigos e colegas que fiz durante a graduação, em especial aos amigos Vinicius Batista da Silva, Shellton Lino e Fábio Viânez, que me acompanharam em diversos momentos nessa caminhada. Além disso, não poderia deixar de agradecer ao meu tio Lair Thomé e minha tia Cristiane Mota Thomé, que jamais mediram esforços para me ajudar no que fosse preciso.

Por fim, gratidão aos meus avós, Dona Edna e Seu Sebastião, minhas tias Cassia, Tânia e Sandrine e ao meu tio André por me instruirem no caminho dos estudos desde a minha infância. Aos demais familiares e amigos que não mencionei aqui mas que me acompanharam, também deixo meu agradecimento a vocês.

Se o conhecimento pode criar problemas, não é
através da ignorância que podemos solucioná-los.
Isaac Asimov.

RESUMO

A pesquisa analisa a problemática da autoria nos crimes ocorridos por meios cibernéticos, expondo a dificuldade na apuração da autoria. Por meio do método de revisão bibliográfica, foram utilizadas doutrinas jurídicas, análise de artigos científicos, notícias e dados disponibilizados por órgãos públicos (Ministério Público e Polícia Judiciária), bem como trechos da Legislação. No primeiro momento, foi feita a explicação do conceito de autoria no Direito Penal. Já no segundo tópico houve uma análise do conceito de crime cibernético e as suas classificações. Em seguida, passou-se à ideia central do trabalho, que é expor os meios pelos quais os crimes cibernéticos são praticados e como isso dificulta a apuração da autoria criminosa. Por fim, o trabalho trouxe à tona as medidas que tem sido tomadas para combater os *cybercrimes*, com foco nos núcleos especializados de investigação. Os resultados obtidos indicam que, considerando a natureza virtual e a ausência de fronteiras para o cometimento dos crimes referidos, bem como os artíficos utilizados pelos criminosos para ocultarem as suas identidades, a criação dos núcleos de investigação especializados em crimes virtuais tem demonstrado ser uma ação efetiva no combate à essa modalidade de delitos. A presente pesquisa visa fomentar o debate à respeito das medidas que devem ser tomadas para garantir a segurança no mundo virtual.

Palavras-chave: Autoria em crimes cibernéticos. Técnicas de Investigação.

ABSTRACT

This research is looking for bring an outlook about the authorship issues into the cybercrimes, revealing the difficulties in the authorship investigation. Through the literature review, were used legal doctrines, scientific articles, news and data given by public agencies (Public prosecution and judiciary police), as well as parts of law. In the first time, a explanation about the idea of "authorship in the criminal law" was made. In the second moment was realized an analisis about the concept of cybercrimes and their classifications. Right away, followed by the central theme of the research, which is exposed the resources where the cybercrimes happens and how it difficulties the authorship investigation. In the end, the research brings the means that has been used to face the cybercrimes, focusing in the specialized research centers. The results indicate that, considering the virtual nature and the borderless in the practice of the crimes, as well as the tools used by the criminals to hide their identities, the foundation of specialized research centers in virtual crimes has demonstrated to be an effective action in the combat against this crimes. The present research aims to instigate the discussion about the ways to guarantee the security in the virtual world.

Keywords: Authorship in cybercrimes. Investigation Techniques.

SUMÁRIO

1 INTRODUÇÃO

Durante toda a história da humanidade, uma determinada prática sempre se fez presente: a criminalidade. Em maior ou menor grau, toda comunidade, cidade ou vilarejo existente no planeta já registrou alguma prática delitiva, em alguns casos, delitos patrimoniais, em outros delitos contra a vida ou a liberdade sexual, mas a prática criminosa sempre existiu.

Apesar da prática de crimes ser conhecida pela sociedade há séculos, havia uma característica marcante em relação a esses delitos que facilitava a apuração da autoria criminosa, bem como a posterior investigação e exercício do *jus puniendi* estatal sobre os autores: a pessoalidade.

Não haviam dúvidas sobre quem foi o autor do delito e, se haviam, eram dúvidas pontuais e relativas ao momento em que o crime foi cometido. Dessa forma, como os delitos eram cometidos de forma direta e presencial pelo suposto autor, as ações a serem tomadas posteriormente para dispor sobre as investigações e eventuais punições contra o autor eram mais fáceis.

Todavia, com o advento da tecnologia e o avanço da *internet* na sociedade, em especial após a segunda metade do século XX, surgiu uma modalidade de crimes em que a autoria delitiva se tornou algo controverso e de difícil apuração: os crimes cibernéticos.

Portanto, é o objeto da presente pesquisa a análise acerca dos crimes cibernéticos e as razões pelas quais existe a dificuldade na apuração da autoria delitiva. Ademais, o trabalho visa demonstrar e expor as ações tomadas pelo Estado para acompanhar a evolução das ações criminosas.

Para realização da pesquisa, foram utilizadas pesquisas bibliográficas, juntada de dados estatísticos na língua portuguesa e doutrinas jurídicas para evidenciar conceitos sobre algumas nomenclaturas jurídicas. O objetivo do artigo foi trazer à tona essa dificuldade latente em apurar autores de crimes digitais e demonstrar as medidas que vêm sendo tomadas.

2 O CONCEITO DE AUTORIA NO DIREITO PENAL

Com o avanço dos estudos sobre o Direito Penal, surgiram diversas teorias para definir o conceito de autor. De acordo com Masson (2019, p. 223), destacam-se as seguintes teorias: a) teoria subjetiva ou unitária; b) teoria extensiva; c) teoria objetiva ou dualista, sendo que esta última divide-se em: 1) teoria objetivo-formal; 2) teoria objetivo-material e 3) teoria do domínio

do fato.

A teoria unitária, também denominada de teoria monista[1], não realiza distinções entre o autor do crime e o partícipe. Nesta teoria, autor é definido como o indivíduo que age de qualquer forma para que seja gerado um resultado com efeitos no âmbito penal, sendo fundamentada pela teoria da equivalência dos antecedentes, sendo que qualquer colaboração para o resultado a ele deu causa (MASSON, 2019, p. 223).

Já para Prado (2014, p. 402), a teoria monista considera como autor todo aquele que estabelece contribuição para a realização de um fato punível, não existindo qualquer diferença entre autor e partícipe, definindo-se autor como o sujeito que intervém causalmente em um fato e é condição ou a causa do seu resultado.

Em síntese, analisando o que foi exposto por Luís Regis Prado e Cléber Masson, pode-se chegar à conclusão de que a teoria unitária define como autoria a participação de qualquer forma na prática delitiva, não havendo distinção entre o grau de participação, apenas sendo relevante o fato de o sujeito ter colaborado para a ação.

Já a teoria extensiva segue uma linha semelhante à teoria unitária, visto que no âmbito da corrente extensiva também não há distinção entre autor e partícipe. Todavia, no que tange à teoria extensiva, autor é aquele que coopera com a prática delitiva impondo uma condição para tal, considerando-se o autor aquele que colabore causalmente com a prática do delito, realizando alguma ação não prevista como forma de participação (PRADO, 2014, p. 403).

Masson (2019, p. 223) pontua que se trata de uma teoria mais suave, visto que admite algumas causas de diminuição de pena para que sejam determinados os diversos graus de autoria. No âmbito da teoria extensiva é que surge a figura do cúmplice, também chamado de comparsa, tratando-se do autor que concorre de modo menos relevante para o resultado da conduta.

Por fim, tratando sobre a teoria objetiva ou dualista sobre a autoria, esta realiza uma notória distinção entre o autor e o partícipe. É a teoria que foi adotada pelo Código Penal em sua importante reforma realizada pela Lei 7.209/1984 e se divide em outras três teorias (MASSON, 2019, p. 223).

A saber, a teoria objetivo-formal define autor como aquele que pratica o núcleo do tipo, aquela conduta definida como central, ou seja, o verbo do tipo penal (MASSON, 2019, p. 223).

---

[1] Conforme se vê no sítio do Tribunal de Justiça do Distrito Federal e dos Territórios, no seguinte endereço: https://www.tjdft.jus.br/consultas/jurisprudencia/jurisprudencia-em-temas/a-doutrina-na-pratica/concurso-de-pessoas/introducao#:~:text=De%20acordo%20com%20a%20teoria,e%20o%20outro%2C%20pelos%20part%C3%ADcipes. Acesso em: 29 out. 2023.

Para exemplificar: no crime de homicídio, a conduta tipificada é a de matar alguém. Neste caso, autor é aquele que realiza a conduta de matar, ou seja, o verbo nuclear do tipo penal previsto no art. 121 do Código Penal.

No âmbito da corrente objetivo-formal, faz-se menção à figura do partícipe, sendo este o indivíduo que de qualquer forma contribui para a conduta delitiva, mas que não realiza o verbo nuclear do tipo. Luís Regis Prado define a teoria objetivo-formal de uma forma mais expansiva em relação à figura do partícipe, conforme exposto:

> Teoria objetivo-formal - autor é aquele que realiza a ação típica, quer dizer, executa a ação determinada pelo núcleo do tipo (verbo reitor do tipo). Define-se o autor como sendo aquele cujo comportamento se encontra no círculo abarcante do tipo; sendo partícipe aquele que presta ajuda causalmente para o fato. Conforme essa orientação, os autores e os coautores tomam parte na execução do fato e os partícipes (que também tomam parte) colaboram na execução do delito. Então, caracteriza-se por definir autor como aquele que executa, parcial ou totalmente, a ação descrita no tipo legal de delito. Autor é aquele que realiza o tipo legal (PRADO, 2014, p. 405-406).

Em que pese a posição de Prado sobre a teoria objetivo-formal, extraí-se que, nessa corrente, a figura do autor se pauta naquele que realizou a conduta nuclear, ou seja, o verbo do tipo. Já partícipe (ou coautor) é aquele que auxilia, participa na consecução criminal de qualquer forma.

Relativamente à teoria objetivo-material sobre autoria, a figura do autor é conceituada como o agente que colabora de maneira mais significativa para que seja alcançado o objetivo da prática delitiva, não necessariamente praticando o verbo nuclear do tipo. Partícipe é definido como aquele que concorre de forma mais trivial, mesmo que pratique o núcleo do tipo (MASSON, 2019, p. 223 e 224).

Por fim, Prado (2014, p. 406), tendo por base Hans Welzel e Reinhart Maurach, cita que a teoria do domínio do fato (também denominada de teoria objetiva final ou objetiva-subjetiva de base finalista) "[...] conceitua autor como aquele que tem o domínio final do fato (conceito regulativo), enquanto o partícipe carece desse domínio".

A teoria do domínio do fato estabelece um papel de importância para o partícipe, dispondo que o coautor presta uma função independente e clara para a prática delituosa, sendo que a figura do coautor (ou partícipe) deve possuir o "codomínio" do fato, dividindo tarefas com o autor principal. Além disso, essa teoria também faz distinção entre autor imediato (ou direto) e autor mediato (indireto), sendo que esta última figura utiliza-se de terceiros como um instrumento para a prática delitiva (PRADO, 2014, p. 406).

No Brasil, a teoria adotada pelo Código Penal para definir o autor é a teoria objetiva, em seu caráter objetivo-formal. Aplica-se distinção entre a figura de autor e coautor, sendo

autor quem pratica o verbo nuclear do tipo e coautor quem concorre de qualquer modo para o crime, conforme expresso no art. 29 do Código Penal[2] (MASSON, 2019, p. 224).

Destaca-se ainda que, caso a participação seja de menor importância, a pena poderá ser diminuída (na terceira fase de dosimetria da pena, segundo o critério trifásico) de um sexto a um terço (vide art. 29, §1º do Código Penal), evidenciando a notória distinção entre autor e coautor, na medida de sua culpabilidade, conforme determina a teoria objetivo-formal adotada em solo pátrio.

Ante o exposto, considerando as diversas teorias relativas à autoria, verifica-se que o Direito Penal Brasileiro acolheu uma das correntes mais abrangentes no que tange à culpabilidade nos crimes, restando margem para a aplicação de pena contra aquele que concorre de qualquer forma para a prática criminosa, mas diferenciando de forma clara as figuras do autor e partícipe.

3 CRIMES CIBERNÉTICOS: CONCEITO E CLASSIFICAÇÕES

A chamada "Era da informação" trouxe consigo uma infinidade de recursos que facilitam o cotidiano das bilhões de pessoas que vivem no século XXI. A *internet* proporcionou uma quantidade de opções imensa em se tratando de bens de consumo, entretenimento, formas de trabalho e estilo de vida, além de ter facilitado a comunicação entre usuários sem que haja a necessidade de um contato físico.

Os recursos amplos e democráticos que a modernidade proporcionou serviram para uma quantidade ampla de práticas que ajudam a humanidade no seu cotidiano e desenvolvimento. Todavia, um dos aspectos sociais mais antigos do planeta também encontrou novas possibilidades com o acesso amplo à *internet*: o crime, mas desta vez em sua modalidade cibernética.

Crimes cibernéticos, também chamados de crimes informáticos ou crimes digitais, são os delitos cometidos por meio ou em contrariedade à tecnologia da informação. É um fato típico e ilícito que ocorre por meio da informática em geral ou contra um sistema de computadores ou uma rede (JESUS; MILAGRE, 2016, p. 49 e 50).

Verifica-se, no conceito exposto, que os crimes informáticos são tanto aqueles que possuem como bem jurídico tutelado o sistema de computadores ou a rede eletrônica, bem como aqueles fatos típicos que ocorrem por este meio, mas que possuem vítimas definidas.

[2] Art. 29. Quem, de qualquer modo, concorre para o crime incide nas penas a este cominadas, na medida de sua culpabilidade (BRASIL, 1940).

Para elucidar, Damásio de Jesus faz uma exemplificação sobre os crimes eletrônicos, em que pese a sua prática se dar por meio virtual mas objetivar atingir um sujeito passivo de fato (vítima):

> Fato é que a maior parte dos crimes eletrônicos está relacionada a delitos em que o meio para a realização da conduta é virtual, mas o crime em si não. A exemplo, tem-se como crimes mais comuns praticados na rede o estelionato e a pornografia infantil e os ataques mais comuns os praticados por meio de vírus de computador ou *malware*, seguido de invasão de perfis nas redes sociais e por ataques de *phishing*. Já os crimes cibernéticos mais raros (porém crescentes) continuam sendo aqueles causados por códigos maliciosos, negação de serviço, dispositivos roubados, sequestrados e roubo de informações privilegiadas. Quando combinados, esses fatores são responsáveis por mais de 78% dos custos anuais com crimes cibernéticos para as organizações (JESUS; MILAGRE; 2016, p. 50-51).

Neste sentido, os crimes cibernéticos são divididos em quatro classificações, em atenção ao crime em que a informática é meio e fim. Crimes cibernéticos são classificados em: a) crimes informáticos próprios; b) crimes informáticos impróprios; c) crimes informáticos mistos e d) crime informático mediato ou indireto.

Damásio de Jesus e José Antonio Milagre (2016, p. 54) compreendem que o crime informático próprio é aquele que a vítima é a tecnologia da informação (*internet*), sendo que estes delitos ainda carecem de tipificação penal, e portanto são considerados atípicos em sua maioria.

Já os impróprios são aqueles em que o uso da *internet* serve como meio para atingir um bem jurídico já tutelado pelo Direito Penal (patrimônio, liberdade sexual, etc.), sendo que, para estes delitos, já há tipos penais suficientes. Os crimes informáticos mistos são complexos, funcionam como a soma de dois tipos penais diferentes e unidos em uma única conduta.

Em outra vista, o crime informático mediato ou indireto é aquele que se dá com a ocorrência de um crime cibernético em si mas que prescinde de outra conduta não cibernética (ou física) para que se chegue a sua consumação (JESUS; MILAGRE, 2016, p. 54 e 55).

Na modalidade mediata dos crimes cibernéticos, verifica-se que se trata de uma circunstância de atuação criminosa em que há o uso (meio) da *internet* para se alcançar a possibilidade para a consecução típica. Realizando uma analogia, o crime cibernético funciona como uma chave para abrir a porta (praticar o delito físico), funcionando como meio e sendo absorvido pelo crime-fim, em respeito ao princípio da consunção.

Neste sentido, é possível exemplificar: o roubo de uma conta pessoal no *Instagram*, por exemplo, é um crime cibernético, visto que ocorre através do meio virtual. Todavia, após passar

a ter acesso à conta roubada, o autor do fato se passa pelo proprietário da conta para pedir dinheiro.

Verifica-se que, a princípio, trata-se de um crime puramente cibernético. Entretanto o autor do fato criminoso utilizou-se de meio fraudulento para induzir a rede de conexões da vítima à erro, obtendo vantagem ilícita, neste caso a vantagem pecuniária, incorrendo nas formas do delito de estelionato (art. 171 do Código Penal).

Portanto, em análise sobre as classificações mais comuns dos *cybercrimes*, crime cibernético nada mais é que um fato típico, ilícito e culpável praticado por intermédio da rede mundial de computadores contra alguém ou contra a própria rede, sendo um conceito amplo e abarcando todos aqueles fatos típicos que ocorrem através do uso da tecnologia informacional.

4 A PROBLEMÁTICA SOBRE A AUTORIA NOS CRIMES CIBERNÉTICOS: OS MEIOS EMPREGADOS QUE DIFICULTAM A IDENTIFICAÇÃO DOS PRATICANTES

A disseminação dos meios cibernéticos (celulares, computadores e dispositivos eletrônicos) ao público em geral demonstrou-se como uma forma efetiva e rápida de cometer crimes com a identidade camuflada. Atrás de uma tela de computador, criminosos se escondem e praticam estelionatos, furtos, estupros e uma série de delitos que ocorrem de maneira ardilosa e sutil.

Neste sentido, considerando que a modalidade de crimes cibernéticos ocorre por meios não convencionais (por meio da rede mundial de computadores), é possível afirmar que a investigação sobre esses delitos também deve seguir um padrão não convencional, em especial quando se refere à apuração do autor do crime ocorrido por meio digital.

A identificação do autor em um crime informático geralmente se inicia com a apuração do número de endereço do IP (*internet protocol)* do aparelho, sendo que cada computador e dispositivo com conexão à rede de *internet* possui um número de IP, traduzindo-se numa peça chave para a identificação do criminoso (BRAGA, 2019).

Todavia, apesar da apuração do endereço de IP dos aparelhos ser um caminho importante para a investigação criminal, a complexidade dos *cybercrimes* permite que os autores burlem esse lastro e dificultem ainda mais a descoberta de suas identidades, sendo comum que os autores utilizem de serviços que ocultem os seus endereços de IP, como os *proxies* e os VPNs (*virtual private network*).

Segundo Tunholi (2023), os *proxies* e os VPNs são ferramentas que possibilitam utilizar

a *internet* de uma forma mais segura e privada. Os *proxies* agem como um meio entre o aparelho com acesso à rede e o site utilizado, sendo que o *proxy* trata de ocultar o endereço de IP original daquele aparelho e gerar um novo endereço, possibilitando que o usuário burle as restrições de localidade.

Por sua vez, o VPN age de modo a criar uma nova conexão entre o aparelho e um servidor remoto, criando também um novo endereço de IP ao usuário e lhe garantindo privacidade, bem como evitando que outros usuários tenham acesso à sua atividade na *internet* (TUNHOLI, 2019).

As ferramentas dos VPNs e os *proxies* foram criadas com o intuito de proteger os usuários da rede mundial de computadores, transmitindo privacidade aos internautas que desejam manter os seus dados restritos, visto que as ferramentas criptografam[3] as informações enviadas e recebidas e assim evitam que possíveis *crackers* ou criminosos virtuais roubem os dados do usuário.

Entretanto, como se pode perceber, da mesma forma que a *internet* foi criada para fins benéficos e comunicacionais mas corrompeu-se com alguns criminosos ao longo dos anos, o mesmo se verificou com os *proxies* e os VPNs. Segundo Demartini (2023), os *proxies* funcionam em duplo sentido: enquanto os usuários podem ocultar a própria conexão ou até burlar alguns bloqueios, os fornecedores ganham dinheiro com a sua disponibilização.

Deste modo, o uso de *proxies* é comum para a criação de contas falsas, compras de seguidores em redes sociais e o seu uso para golpes, bem como expõe vulnerabilidades do usuário para ataques e roubos de dados, ou seja: o usuário paga o preço por utilizar o serviço para as atividades negativas, se expondo aos riscos também (DEMARTINI, 2023).

Além dos VPNs e *proxies,* que têm a capacidade de criptografar as informações daquele usuário e podem ser utilizados para o cometimento de atividades ilícitas (além de exporem o usuário a roubos de dados e outros crimes cibernéticos), existe uma outra ferramente utilizada por *cybercriminosos* para praticarem crimes: trata-se do *phishing.*

O *phishing,* traduzido da língua inglesa como “pescaria”, é uma modalidade em que o criminoso metaforicamente “pesca” dados pessoais do usuário, para, posteriormente, cometer crimes. Segundo Campelo (2023), “*phishing* é uma técnica utilizada por cibercriminosos para obter informações sensíveis de usuários, tais como senhas, números de cartões de crédito e

[3] Criptografar significa converter um texto, dado ou informação legível para um código secreto, sendo que apenas aqueles que detenham o código podem acessar o conteúdo criptografado. É um recurso utilizado para proteger os dados do usuário durante uma troca de mensagens ou informações, como é utilizado pelo aplicativo *WhatsApp,* por exemplo.

informações bancárias".

Através da técnica referida, os criminosos conseguem obter aqueles dados úteis e essenciais para a vida pessoal do usuário, como números de CPF e cartões bancários. Após colocarem em prática a técnica e obterem êxito, os autores utilizam os dados para comprarem produtos on-line, criarem contas bancárias e para realizarem uma série de outros crimes.

Desse modo, explica Marcelo Campelo sobre algumas das técnicas de *phishing* aplicadas pelos *cybercriminosos*:

> Os criminosos utilizam diversas estratégias para atrair a vítima e fazer como que ela forneça informações confidenciais. Eles podem se passar por empresas conhecidas, como bancos, lojas online e redes sociais, e enviar mensagens falsas com links maliciosos que levam o usuário a um site falso. Nesse site, o usuário é induzido a fornecer informações confidenciais, que são então utilizadas pelos criminosos para cometer fraudes e crimes financeiros. Neste caso incidiria o art. 155 – furto – e o art. 171 – estelionato – ambos do Código Penal. Outra técnica comum de *Phishing* é o *spear phising,* que é uma abordagem mais direcionada e personalizada. Nesse caso, os criminosos pesquisam informações sobre a vítima e utilizam essas informações para criar mensagens falsas que parecem mais legítimas e convincentes (CAMPELO, 2023).

Como se pode verificar, o uso de instrumentos como os VPNs e os *proxies* por si só tornam dificultosa a apuração da autoria do delito. Além delas, o uso de técnicas como o *phishing* possibilita aos criminosos a obtenção de dados pessoais de usuários na *internet*, sendo que esses dados podem ser facilmente empregados na prática de novos crimes virtuais.

De acordo com o Ministério Público de Minas Gerais, a invasão de perfis na rede social *Instagram* teve a sua maior incidência entre os crimes cibernéticos no início do ano de 2022, conforme os dados da Coordenadoria de Combate aos Crimes Cibernéticos do MP/MG. Apenas em janeiro de 2022, registrou-se o total de 388 ocorrências de golpes para obtenção de valores no estado mineiro (MINAS GERAIS, 2022).

Em se tratando de golpes envolvendo o *hackeio* de redes sociais, o Ministério Público de Minas Gerais ainda ressalta que a técnica do *phishing* é uma das mais comuns no cometimento de crimes, sendo que após assumirem o controle do perfil, os criminosos se passam pelo proprietário da conta e passam a vender objetos ou exigir dinheiro do dono daquela conta.

Em síntese, conforme disposto pelo próprio MP/MG, a prática do "roubo*"* de contas em redes sociais fornece ao criminoso um meio de praticar golpes e outros crimes (estelionatos, furtos, extorsões) sem que a sua imagem seja descoberta, visto que o autor do delito utiliza da imagem e confiança que as pessoas depositam em outrem (o proprietário original da conta).

Em que pese o roubo de dados e uso de dispositivos que dificultam a apuração imediata

dos autores, o rastreio do protocolo IP (*internet protocol*) é um grande desafio aos órgãos de investigação no que tange à descoberta de elementos sobre autoria delitiva, conforme ressaltado pela Procuradora do Ministério Público Federal Neide Cardoso:

> Um dos maiores desafios das autoridades brasileiras, ao investigar crimes digitais, é hoje rastrear o protocolo IP, uma espécie de assinatura individual de cada usuário da internet; Antes, o IP era individualizado, identificando hora, minutos e segundos e o usuário daquele endereço eletrônico. Hoje pode haver mais de 100 usuários usando o mesmo IP. Para produzir provas digitais, além dos IP´s, os investigadores também usam dezenas de outras ferramentas, como a geolocalização do celular ou imagens de câmera de segurança para comprovação válida (BRASIL, 2022b).

Considerando-se os pontos expostos, verifica-se que os meios empregados para a consumação de crimes na esfera cibernética (*phishing,* uso de *proxies* e VPNs, roubo de dados) por si só torna dificultosa a investigação acerca da autoria. Há materialidade (elementos que o crime ocorreu), mas a indicação de suspeitos resta prejudicada em razão do meio empregado.

A dificuldade na investigação dos delitos cibernéticos é evidente, pois os autores geralmente utilizam-se de meios para burlar a identificação dos seus computadores e, além disso, a Polícia Judiciária ainda não conta com aparato material e humano suficiente para empregar na identificação desses autores.

Takahashi (2022) aponta que a apuração de crimes cibernéticos possui algumas características que tornam evidente a necessidade de recursos adequados para apuração do delito, sendo que o Ministério Público pode atuar solicitando dados de empresas provedoras de *internet* e empresas de tecnologia, atuando de forma conjunta com a Polícia Judiciária na investigação.

Todavia, ainda em relação à dificuldade em apurar autores dos crimes na modalidade on-line, a investigação tende à ser dificultosa, visto que criminosos utilizam-se de servidores no exterior (o que dependerá de cooperação internacional para obtenção de dados) ou de diferentes endereços de IP, tornando a identificação da autoria delitiva ainda mais nebulosa (TAKAHASHI, 2022).

Há de se questionar: o Brasil tem os meios necessários para lidar com uma modalidade de delitos que evolui velozmente? Quais as ações que os órgãos de Segurança Pública tem tomado para acompanhar a evolução da criminalidade e qual a efetividade dessas ações?

Portanto, é necessário realizar tais questionamentos acerca da problemática sobre a apuração da autoria em crimes cibernéticos. A democratização da *internet* é uma realidade, e a tendência é que os crimes cibernéticos se tornem uma modalidade cada vez mais comum, sendo iminente o debate acerca das formas de prevenção e combate aos *cybercrimes.*

5 AS MEDIDAS QUE TÊM SIDO TOMADAS PARA COMBATER OS CRIMES CIBERNÉTICOS: OS NÚCLEOS ESPECIALIZADOS DE INVESTIGAÇÃO

O aumento no número de delitos praticados por meios digitais é notório e percebe-se pela quantidade de notícias e situações envolvendo golpes por meio de aplicativos, ligações e redes sociais. Diante do aumento da criminalidade nas plataformas digitais, os órgãos de segurança pública no Brasil tem traçado algumas estratégias para o combate ao crime cibernético.

Uma das medidas tomadas para intensificar a investigação e apuração dos crimes cibernéticos é a criação de núcleos e coordenadorias especializados em *cybercrimes*, em especial por parte do Ministério Público.

A Constituição Federal estabelece que "o Ministério Público é instituição permanente, essencial à função jurisdicional do Estado, incumbindo-lhe a defesa da ordem jurídica, do regime democrático e dos interesses sociais e individuais indisponíveis" (BRASIL, 1988).

Deste modo, considerando a atribuição do órgão ministerial no sentido da defesa da ordem jurídica e dos interesses sociais e individuais, o Ministério Público tem desempenhado um papel de destaque na prevenção e investigação dos crimes ocorridos pela plataforma virtual em diversos estados da federação.

O Ministério Público da Bahia criou, por meio do Ato 418/2011-PGJ (reformulado pelo Ato 428/2014), o Núcleo de Combate aos Crimes Cibernéticos (NUCCIBER), possuindo como objetivo auxiliar e fornecer suporte técnico às Promotorias de Justiça do Estado da Bahia em casos que envolvam crimes cibernéticos, possuindo diversas atribuições em sua instituição (BAHIA, 2023).

Entre as competências do Núcleo, estão: o auxílio ao Promotor de Justiça em medidas legais, o auxílio na instrução de inquéritos civis e acompanhamento de inquéritos policiais, a coleta de dados, informações e provas necessárias no combate aos crimes cibernéticos, a celebração de convênios com provedores de serviços de *internet*, entre outras possibilidades de atuação (BAHIA, 2023).

Por sua vez, o Ministério Público do Estado de Mato Grosso do Sul criou, no ato de 2021, o Núcleo de Crimes Cibernéticos (Nucib), formalizado através da Resolução 35/2021-PGJ, focando na coordenação de ações que orientassem os meios mais adequados para o combate aos delitos digitais (MATO GROSSO DO SUL, 2021).

A criação desses núcleos não se restringe aos Estados da Bahia e de Mato Grosso do

Sul. Atualmente, existem diversos estados com núcleos especializados no combate aos crimes ocorridos em ambiente virtual, como o Estado de São Paulo, Rio Grande do Sul, Espírito Santo, etc.

Os núcleos especializados, além de prestarem apoio às atuações do próprio Ministério Público também servem como auxiliares de ações em fase de inquérito policial, os quais são conduzidos pela Polícia Civil, responsável pela apuração de indícios sobre autoria e materialidade na fase pré-processual (investigativa).

Neste sentido, não foi apenas o Ministério Público que inovou no combate aos crimes virtuais. A Lei 12.735/2012, conhecida como "Lei Azeredo", estabeleceu, em seu art. 4º, sobre a criação de equipes especializadas em crimes cibernéticos nos órgãos da Polícia Judiciária (Polícia Civil e Polícia Federal): "Os órgãos da polícia judiciária estruturarão, nos termos do regulamento, setores e equipes especializados no combate à ação delituosa em rede de computadores, dispositivo de comunicação do sistema informatizado" (BRASIL, 2012).

A partir da promulgação da Lei 12.737/2012, foram criados diversos setores e equipes com especialidade em crimes cibernéticos em toda a extensão do território nacional, atuando de maneira estratégica e com foco no combate à modalidade de crimes ocorridas em meios virtuais, considerando a maior complexidade na investigação desses delitos.

Através do Decreto 65.241/2020, foi criada, no Estado de São Paulo, a Divisão de Crimes Cibernéticos (DCCIBER), sendo dividida inicialmente em quatro delegacias especializadas em fraudes contra instituições financeiras praticadas por meios eletrônicos, fraudes contra instituições de comércio eletrônico, violação de dispositivos eletrônicos e redes de dados e lavagem e ocultação de ativos ilícitos por meios eletrônicos, além de um Centro de Inteligência Cibernética e um Laboratório Técnico (SÃO PAULO, 2020).

No Estado de Goiás, no ano de 2017, foi publicada a Lei 19.907, sendo criada a Delegacia de Repressão aos Crimes Cibernéticos (DERCC). Possuindo circunscrição estadual, a Delegacia Especializada atua na apuração de infrações penais cometidas por meio da *internet*, apurando crimes como favorecimento à prostituição, calúnia, difamação, etc. (GOIÁS, 2017).

Já na esfera federal, no ano de 2022, foi criada, pela Polícia Federal, a Unidade Especial de Investigação de Crimes Cibernéticos (UEICC), voltada para "intensificar a repressão a diversos outros crimes praticados no ambiente virtual, como a pornografia infantil, contra instituições públicas, setor varejusta, operadoras de telefonia" (BRASIL, 2022a).

A criação de unidades especializadas em crimes ocorridos on-line pelos órgãos do Ministério Público e das Polícias Judiciárias no Brasil é uma ação que tem aumentado nos últimos anos. Todavia, apenas a criação desses núcleos especializados sem uma ação efetiva no

combate à criminalidade não possui efeito prático, por essa razão é importante questionar: a implantação de núcleos especializados tem sido efetiva?

De acordo com a Polícia Civil do Rio Grande do Sul, as Polícias Civis dos Estados do Rio Grande do Sul e do Estado de Goiás desarticularam uma associação criminosa especializada em crimes cibernéticos, deflagrando a Operação Sem Fronteiras, coordenada por duas delegacias especializadas: a Delegacia de Repressão a Crimes Cibernéticos e a Delegacia de Repressão aos Crimes Informáticos e Defraudadores, dos Estados de Goiás e Rio Grande do Sul, respectivamente (RIO GRANDE DO SUL, 2022).

A atuação em conjunto das Polícias Civis de diversos estados brasileiros não é caso isolado, se tornando cada vez mais comum quando se trata de crimes cibernéticos. Segundo dados do Ministério Público de Santa Catarina, a Operação *Pessinus* contou com o trabalho do CyberGAECO (órgão do Ministério Público Catarinense), do Ministério da Justiça e da Polícia Civil do Piauí.

Durante a Operação Pessinus, foram cumpridos mandados de busca e apreensão nos Estados de Santa Catarina, Mato Grosso, Piauí e Rio de Janeiro, sendo que o objetivo da operação foi o combate a diversos crimes como: contrangimento ilegal, estupro de vulnerável, apologia ao crime, incitação ao preconceito de raça, entre outros, todos os delitos cometidos por meio virtual (RIO GRANDE DO SUL, 2022).

Em 2023, outro caso importante de atuação em conjunto das Polícias Civis foi deflagrado: A Divisão de Combate a Crimes Econômicos e Patrimoniais Praticados por Meios Cibernéticos (DCCEP) da Polícia Civil do Pará, com o apoio da Delegacia Especializada de Roubos e Furtos da Polícia Civil do Mato Grosso realizou a Operação Rondon, realizando a prisão de seis pessoas no município de Rondonópolis (MT), de acordo com a Polícia Civil do Estado do Pará (PARÁ, 2023).

De acordo com o delegado-geral da Polícia Civil, Walter Resende: “Esse trabalho integrado é importante para dar celeridade às investigações e localização dos indiciados. A PCPA seguirá vigilante para enfrentar crimes virtuais”, destacando o papel fundamental do trabalho conjunto entre as Políciais Judiciárias dos Estados da Federação (PARÁ, 2023).

Conforme se verificou, as ações para combate aos *cybercrimes* podem ocorrer em conjunto. A participação dos órgãos especializados do Ministério Público em apoio às divisões de crimes cibernéticos das Políciais Civis em diversos estados age de uma forma inteligente: ao passo que o crime cibernético não possui barreiras de divisas estaduais ou fronteiras, os órgãos tem seguido o mesmo *modus operandi.*

Já no ano de 2022, foi deflagrada, no Distrito Federal, uma operação nomeada *Payback.*

A ação foi realizada em conjunto pelo Núcleo Especializado do Ministério Público do Distrito Federal e Territórios, o Núcleo de Combate a Crimes Cibernéticos (Ncyber) e a Polícia Civil do Distrito Federal (PCDF) para a investigação sobre uma associação criminosa responsável por fraudes bancárias, de acordo com o Ministério Público do Distrito Federal e Territórios (BRASÍLIA, 2022).

As operações desencadeadas a partir do apoio entre os núcleos especializados do Ministério Público, divisões especializadas da Polícia Civil e da Polícia Federal são exemplos de como a cooperação entre os órgãos (mesmo que de estados diferentes) pode gerar bons frutos no combate aos delitos virtuais.

Por fim, é preciso destacar a importância do Poder Judiciário na autorização de pedidos de quebra de sigilo telefônico, acesso à informações em dispositivos de computação, bem como das empresas provedoras de *internet* para que a atuação dos núcleos especializados seja potencializada e ocorra de forma célere.

Em resumo, foram criados, ao longo dos últimos anos, diversos núcleos de atuação com atribuição especializada para investigação de delitos cibernéticos. A criação desses núcleos tem se demonstrado efetiva, visto que, além de prestarem apoio mútuo entre si, contam com profissionais que possuem o conhecimento necessário para ingressarem em sites, servidores e endereços virtuais a fim de colher elementos de autoria.

6. CONSIDERAÇÕES FINAIS

As inovações trazidas pelo mundo virtual são inegáveis: diversos meios facilitadores foram criados, aplicativos de *delivery,* redes sociais que integram as mais distantes partes do mundo, acesso aos sistemas bancários através dos *smartphones* e a possibilidade de trabalhar e praticar atos da vida civil por meio da *internet* transformaram o século XXI.

Entretanto, essas facilidades criadas pelo avanço tecnológico trouxeram um efeito colateral inesperado: o avanço da criminalidade através dos meios digitais. Os crimes, que até cerca de 40 anos atrás somente eram praticados de maneira personalíssima, passaram a ocorrer na plataforma virtual, e com um detalhe: sem a possibilidade de se enxergar o autor.

Em razão da maior dificuldade em se apurar quem são os verdadeiros praticantes dos delitos, a modalidade avança cada dia mais, principalmente com o acesso à redes sociais, dados bancários e contas em corretoras de valores, o que torna a modalidade de crimes cibernéticos cada vez mais atraente aos criminosos.

Outro fator que potencializa a prática é a possibilidade de se manter impune. Enquanto

nos delitos convencionais, aqueles que são praticados de maneira pessoal, o autor precisa se expor ao risco de ser identificado, nos crimes cibernéticos existem diversos meios de ocultar a sua identidade: o uso de *proxies* e VPNs, diferentes endereços de IP e o roubo de contas em redes sociais possibilita que os criminosos pratiquem os delitos por meios anônimos ou se passando por outras pessoas.

Deste modo, diante do aumento da criminalidade virtual, surgiu a necessidade da criação de núcleos de investigação por parte dos órgãos de segurança pública que tivessem o conhecimento necessário, além dos meios eficazes para se apurar quem são os verdadeiros autores, através da quebra de sigilo telefônico, infiltração em meios cibernéticos, rastreamento de IPs, dentre outras estratégias.

Neste sentido, o Ministério Público passou a criar os Núcleos de Combate aos Crimes Cibernéticos em diversos estados do Brasil, atuando de maneira conjunta com as Delegacias Especializadas na Repressão de Crimes Cibernéticos, os núcleos de investigação especializados foram um meio desenvolvido para lidar com uma das modalidades de crimes que mais avançam nos últimos anos.

A atuação das Delegacias Especializadas em Crimes Cibernéticos tem trazido bons frutos para a elucidação da autoria nos crimes virtuais. A atuação em conjunto com órgãos da Polícia Civil de outros estados da Federação atua de maneira inteligente, cooperando entre si no cumprimento de mandados de prisão e busca e apreensão de computadores e aparelhos cibernéticos.

Além disso, a atuação do Ministério Público, por parte dos seus Núcleos de Combate Especializados em Crimes Cibernéticos, tem auxiliado a Polícia Civil na apuração da nova modalidade delitiva, resultando em diversas prisões e em operações bem sucedidas no Brasil, conforme demonstrado pelas reportagens extraídas dos portais da Polícia Judiciária e Ministério Público dos Estados da Federação.

Resta ainda a dúvida: apenas a criação dos núcleos especializados de investigação é o suficiente para solucionar a problemática da autoria nos crimes cibernéticos? E a resposta, apesar de incerta, caminha para uma negativa. Faltam meios de investigação adequados, estrutura material e o principal: profissionais com expertise na área de investigação digital.

Cabe ressaltar, por fim, que a criação dos Núcleos Especializados de Investigação demonstrou-se como uma forma eficaz e inovadora de se identificar os autores de crimes que evoluem diariamente. Todavia, investir nos órgãos de segurança pública é uma medida essencial, com o provimento de novos cargos e a criação de outros Núcleos Especializados para atender a demanda das investigações em *cybercrimes.*

REFERÊNCIAS

BAHIA. Ministério Público do Estado da Bahia. **Ato 341,** de 12 de junho de 2023. Salvador: Ministério Público do Estado da Bahia, 12 jun. 2023. Disponível em: https://nucciber.mpba.mp.br/quem-somos/legislacao/. Acesso em: 13 set. 2023.

BRAGA, Diego Campos Salgado. Métodos de investigações no âmbito cibernético. **Revista Jus Navigandi,** ISSN 1518-4862, Teresina, ano 24, n. 5681, 20 jan. 2019. Disponível em: https://jus.com.br/artigos/71463. Acesso em: 7 set. 2023.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília – DF: Presidência da República, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 11 set. 2023.

BRASIL. **Decreto-Lei 2.848**, de 7 de dezembro de 1940. Código Penal. Rio de Janeiro: Presidência da República, 1940. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 11 set. 2023.

BRASIL. **Lei 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 1.001, de 21 de outubro de 1969 - Código Penal Militar, e a Lei 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências. Brasília, DF: Presidência da República, 2012. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12735.htm. Acesso em: 13 set. 2023.

BRASIL. Ministério da Justiça e Segurança Pública. **Polícia Federal cria Unidade Especial para intensificar a repressão a crimes cibernéticos**. Brasília – DF: Ministério da Justiça e Segurança Pública, 2022a. Disponível em: https://www.gov.br/mj/pt-br/assuntos/noticias/policia-federal-cria-unidade-especial-para-intensificar-a-repressao-a-crimes-ciberneticos. Acesso em: 10 set. 2023.

BRASIL. Superior Tribunal Militar. **Crimes Cibernéticos**: provedores do Brasil não conseguem mais identificar cibercriminosos pelo endereço IP.Brasília – DF: Superior Tribunal Militar, 2022b. Disponível em: https://www.stm.jus.br/informacao/agencia-de-noticias/item/12031-provedores-do-brasil-nao-conseguem-mais-identificar-cibercriminosos-pelo-endereco-ip-informacao-foi-noticiada-durante-simposio-na-jmu. Acesso em: 10 set. 2023.

BRASÍLIA – DF. Ministério Público do Distrito Federal e Territórios. **NCYBER e DRCC deflagram operação contra grupo responsável por prejuízo milionário ao BRB**. Brasília – DF: Ministério Público do Distrito Federal e Territórios, 2022. Disponível em: https://www.mpdft.mp.br/portal/index.php/comunicacao-menu/sala-de-imprensa/noticias/noticias-2022/13933-ncyber-e-drcc-deflagram-operacao-contra-grupo-responsavel-por-prejuizo-milionario-ao-brb. Acesso em: 13 set. 2023.

CAMPELO, Marcelo. Crimes Cibernéticos – Phishing – Furto – Estelionato - Art. 155 e Art. 171 do Código Penal. **Migalhas,** 14 mar. 2023. Disponível em:

https://www.migalhas.com.br/depeso/382987/crimes-ciberneticos--phishing--furto. Acesso em: 8 set. 2023.

DEMARTINI, Felipe. Cuidado: apps de proxy podem envolver usuários em crimes ou fraudes. **Canaltech,** 14 abr. 2023. Disponível em: https://canaltech.com.br/seguranca/cuidado-apps-de-proxy-podem-envolver-usuarios-em-crimes-ou-fraudes-246742/. Acesso em: 8 set. 2023.

GOIÁS. Secretaria de Estado e Segurança Pública. **Governo do Estado publica lei que institui criação de seis novas delegacias em Goiás**. Goiânia: Secretaria de Estado e Segurança Pública, 2017. Disponível em: https://www.seguranca.go.gov.br/ultimo-segundo/governo-do-estado-publica-lei-que-institui-criacao-de-seis-novas-delegacias-em-goias.html. Acesso em: 16 set. 2023.

JESUS, Damásio de; MILAGRE, José Antonio. **Manual de Crimes Informáticos.** São Paulo: Saraiva, 2016.

MASSON, Cleber. **Código Penal Comentado.** 7. ed. São Paulo: Método, 2019.

MATO GROSSO DO SUL. Ministério Público do Estado de Mato Grosso do Sul. **MPMS passa a contar com núcleo de apoio no combate aos crimes cibernéticos**. Campo Grande – MS: Ministério Público do Estado de Mato Grosso do Sul, 2021. Disponível em: https://relatorioanual.mpms.mp.br/qualitativo/mpms-passa-a-contar-com-nucleo-de-apoio-no-combate-aos-crimes-ciberneticos/. Acesso em: 13 set. 2023.

MINAS GERAIS. Ministério Público do Estado de Minas Gerais. **MPMG alerta**: invasão de perfis no *Instagram* é um dos crimes cibernéticos de maior incidência neste início de 2022. Belo Horizonte: Ministério Público do Estado de Minas Gerais, 2022. Disponível em: https://www.mpmg.mp.br/portal/menu/comunicacao/noticias/mpmg-alerta-invasao-de-perfis-no-instagram-e-um-dos-crimes-ciberneticos-de-maior-incidencia-neste-inicio-de-2022.shtml. Acesso em: 10 set. 2023.

PARÁ. Polícia Civil do Estado do Pará. **Policiais civis do Pará prendem no Centro-Oeste sete investigados por golpe na internet**. [S.l]: Polícia Civil do Estado do Pará, 2023. Disponível em: https://www.pc.pa.gov.br/noticia/policiais-civis-do-para-prendem-no-centro-oeste-sete-investigados-por-golpes-na-internet. Acesso em: 16 set. 2023.

PRADO, Luiz Regis. **Curso de Direito Penal Brasileiro.** 13. ed. rev. atual. São Paulo: Revista dos Tribunais, 2014.

RIO GRANDE DO SUL. Polícia Civil do Estado do Rio Grande do Sul. **Operação Sem Fronteiras desarticula associação criminosa do Rio Grande do Sul especializada em extorsão sexual cibernética**. Porto Alegre: Polícia Civil do Estado do Rio Grande do Sul, 2022. Disponível em: https://www.pc.rs.gov.br/operacao-sem-fronteiras-desarticula-associacao-criminosa-do-rio-grande-do-sul-especializada-em-extorsao-sexual-cibernetica. Acesso em: 12 set. 2023.

SANTA CATARINA. Ministério Público do Estado de Santa Catarina. **CyberGAECO do MPSC, Ministério da Justiça e Polícia Civil do Estado do Piauí deflagram "Operação Pessinus"**. Florianópolis: Ministério Público do Estado de Santa Catarina, 2023. Disponível

em: https://www.mpsc.mp.br/noticias/cybergaeco-do-mpsc-ministerio-da-justica-e-policia-civil-do-estado-do-piaui-deflagram--operacao-pessinus. Acesso em: 13 set. 2023.

SÃO PAULO (Estado). **Decreto 65.241**, de 13 de outubro de 2020. Cria, no Departamento Estadual de Investigações Criminais – DEIC, a Divisão de Crimes Cibernéticos – DCCIBER e dá providências correlatas. São Paulo: Assembleia Legislativa do Estado de São Paulo, 2020. Disponível em: https://www.al.sp.gov.br/repositorio/legislacao/decreto/2020/decreto-65241-13.10.2020.html. Acesso em: 13 set. 2023.

TAKAHASHI, Victor. **A atuação do Ministério Público no combate aos crimes cibernéticos.** 2022. Artigo Científico (Curso de Direito) – Escola de Direito, Negócios e Comunicação, Pontifícia Universidade Católica de Goiás, Goiânia-GO, 2022. Disponível em: https://repositorio.pucgoias.edu.br/jspui/bitstream/123456789/6381/1/Artigo%20-%20Victor%20Shin%20Iti%20Monteiro%20Takahashi.pdf. Acesso em: 12 set. 2023.

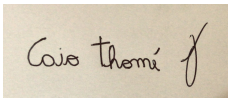
TUNHOLI, Murilo. Proxy x VPN: entenda as principais diferenças entre os serviços. **Techtudo,** 1 maio 2023. Disponível em: https://www.techtudo.com.br/listas/2023/05/proxy-x-vpn-entenda-as-principais-diferencas-entre-os-servicos-edsoftwares.ghtml. Acesso em: 7 set. 2023.

República Federativa do Brasil
Ministério da Educação
Fundação Universidade Federal de Mato Grosso do Sul

Termo de Autenticidade

Eu, **CAIO ERIK PEREIRA THOMÉ**, acadêmico(a) regularmente apto(a) a proceder ao depósito do Trabalho de Conclusão de Curso intitulado **"A PROBLEMÁTICA SOBRE A APURAÇÃO DA AUTORIA NOS CRIMES CIBERNÉTICOS E A ATUAÇÃO DOS NÚCLEOS ESPECIALIZADOS DE INVESTIGAÇÃO"**, declaro, sob as penas da lei e das normas acadêmicas da UFMS, que o Trabalho de Conclusão de Curso ora depositado é de minha autoria e que fui instruído pelo meu orientador acerca da ilegalidade do plágio, de como não o cometer e das consequências advindas de tal prática, sendo, portanto, de minha inteira e exclusiva responsabilidade, qualquer ato que possa configurar plágio.

Três Lagoas/MS, 30/10/2023.



Assinatura do(a) acadêmico(a)

Orientações: O acadêmico ou acadêmica deverá preencher e assinar este documento e, após, uni-lo ao TCC e ao Termo de Depósito e Composição da Banca Examinadora em um único arquivo PDF. O acadêmico ou acadêmica deverá, então, proceder ao depósito desse arquivo PDF único, observando a data limite estipulada pelo Colegiado de Curso.

República Federativa do Brasil
Ministério da Educação
Fundação Universidade Federal de Mato Grosso do Sul

Termo de Depósito e Composição da Banca Examinadora

Eu, professor **LUIZ RENATO TELLES OTAVIANO** orientador(a) do(a) acadêmico **CAIO ERIK PEREIRA THOMÉ** autorizo o depósito do Trabalho de Conclusão de Curso intitulado **"A PROBLEMÁTICA SOBRE A APURAÇÃO DA AUTORIA NOS CRIMES CIBERNÉTICOS E A ATUAÇÃO DOS NÚCLEOS ESPECIALIZADOS DE INVESTIGAÇÃO"**.

Informo, também, a composição da banca examinadora e a data da defesa do TCC:

Presidente: LUIZ RENATO TELLES OTAVIANO

lº avaliador(a): HELOÍSA HELENA DE ALMEIDA PORTUGAL

2º avaliador(a): MOISÉS CASAROTTO

Data: 16 de Novembro de 2023

Horário: 10h00min

Três Lagoas/MS, 30/10/2023.

_____

Assinatura do(a) orientador(a)

Orientações: O acadêmico ou acadêmica deverá preencher e assinar este documento e, após, uni-lo ao TCC e ao Termo Autenticidade em um único arquivo PDF. O acadêmico ou acadêmica deverá, então, proceder ao depósito desse arquivo PDF único, observando a data limite estipulada pelo Colegiado de Curso.

ATA N. 409 DE BANCA DE DEFESA DE TRABALHO DE CONCLUSÃO DE CURSO

Aos **16 dias do mês de novembro de 2023**, às 10h00min, em sala de reuniões Google, sessão pública de defesa do Trabalho de Conclusão de Curso de Direito, do acadêmico **CAIO ERIK PEREIRA THOMÉ**, intitulado **A PROBLEMÁTICA SOBRE A APURAÇÃO DA AUTORIA NOS CRIMES CIBERNÉTICOS E A ATUAÇÃO DOS NÚCLEOS DE INVESTIGAÇÃO ESPECIALIZADOS**, na presença da banca examinadora composta pelos professores: presidente da sessão, Prof. Dr. Luiz Renato Telles Otaviano, primeira avaliadora a Profa. Dra. Heloísa Helena de Almeida Portugal e segundo avaliador o Dr. Moisés Casarotto. Após os procedimentos de apresentação, arguição e defesa, o presidente suspendeu a sessão para deliberação. Retomados os trabalhos foi divulgado o resultado, considerando o trabalho **APROVADO**. Terminadas as considerações e nada mais havendo a tratar, foi dada por encerrada a sessão, sendo lavrada a presente ata, que segue assinada pelo Presidente da Banca Examinadora e pelos demais examinadores presentes na sessão pública.

Três Lagoas, 16 de novembro de 2023.

Prof. Dr. Luiz Renato Telles Otaviano
Profª Dra. Heloísa Helena de Almeida Portugal
Dr. Moisés Casarotto

Documento assinado eletronicamente por **Luiz Renato Telles Otaviano**, **Professor(a) do Magistério Superior**, em 17/11/2023, às 07:00, conforme horário oficial de Mato Grosso do Sul, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Heloisa Helena de Almeida Portugal**, **Professora do Magistério Superior**, em 17/11/2023, às 09:34, conforme horário oficial de Mato Grosso do Sul, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Moisés Casarotto**, **Usuário Externo**, em 27/11/2023, às 15:02, conforme horário oficial de Mato Grosso do Sul, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.