POLÍCIA MILITAR DO ESTADO DE GOIAS
COMANDO DA ACADEMIA DE POLÍCIA MILITAR
DIRETORIA DE ENSINO E PESQUISA
MBA EM GESTÃO DE POLÍCIA OSTENSIVA

JONATHAN HUMBERTO FREITAS FERREIRA

ATUAÇÃO DA POLÍCIA MILITAR NOS CRIMES CIBERNÉTICOS

GOIÂNIA-GO
2024

JONATHAN HUMBERTO FREITAS FERREIRA

ATUAÇÃO DA POLÍCIA MILITAR NOS CRIMES CIBERNÉTICOS

Artigo Científico apresentado como exigência para conclusão da disciplina de Trabalho de Conclusão de Curso da Pós-Graduação de MBA em Gestão de Polícia Ostensiva do Comando da Academia de Polícia Militar de Goiás, sob a orientação do Prof. Thiago Henrique.

GOIÂNIA-GO

2024

ATUAÇÃO DA POLÍCIA MILITAR NOS CRIMES CIBERNÉTICOS

MILITARY POLICE ACTIVITY IN CYBER CRIMES

Jonathan Humberto Freitas Ferreira[1]
Thiago Henrique Costa Silva[2]

Resumo

Os crimes cibernéticos representam uma adaptação significativa das práticas criminosas à era digital, são infrações cometidas pela internet ou sistemas de informática visando ganhos ilícitos, afetando o espaço digital e envolvendo ações ilegais contra sistemas computacionais para acessar e usar dados pessoais. Esses crimes incluem phishing, lavagem de dinheiro digital, golpes financeiros, comércio ilegal de produtos, abuso sexual online e tráfico de pessoas. Na era da informação, a revolução tecnológica e a internet trouxeram mudanças significativas, mas também desafios como a segurança de dados e a privacidade. Cibercriminosos exploram a conectividade e o anonimato da internet para atividades ilícitas, dificultando sua identificação e detenção devido à capacidade de operar além das fronteiras nacionais.

Dada a dificuldade de capturar esses criminosos, é crucial um esforço colaborativo entre a comunidade e a segurança pública, para fortalecer a segurança digital e promover a conscientização sobre práticas seguras online.

Palavras-chave: Cibercrimes; Segurança na rede; Ataques através da internet.

Abstract

Cybercrimes represent a significant adaptation of criminal practices to the digital age, involving offenses committed through the internet or computer systems aimed at illicit gains, affecting the digital space by engaging in illegal actions against computer systems to access and use personal data. These crimes encompass phishing, digital money laundering, financial scams, illegal product trade, online sexual abuse, and human trafficking. In the information age, technological revolution and the internet have brought significant changes but also challenges such as data security and privacy. Cybercriminals exploit the connectivity and anonymity of the internet for illicit activities, complicating their identification and apprehension due to their ability to operate beyond national borders.Given the difficulty in apprehending these criminals, collaborative efforts between the community and law enforcement are crucial to strengthen digital security and promote awareness of safe online practices.

Keywords or Palabras clave: Cybercrimes; Network security; Attacks over the internet

[1] Aluno do Curso de Formação de Oficiais, Especialização em Polícia e Segurança Pública do Comando da Academia de Polícia Militar de Goiás, email: jonathan2011.rv@gmail.com. Telefone: (64) 9.9261-0952.

[2] Orientador. Professor e pesquisador da Universidade Estadual de Goiás (UEG). Graduado em Direito (UFG), Economia (IESB) e Especialista em Direito Público (UniGoiás), Penal e Processual Penal, e Perícia Contábil (USCS). Doutor em Agronegócio (UFG) e Doutor e Mestre em Direito Agrário (UFG). Email: thiagocostasilva.jur@gmail.com. Lattes: http://lattes.cnpq.br/0761167066175470. Telefone: (62) 9.979-3628

1 INTRODUÇÃO

O presente trabalho tem pretensão, ou até mesmo a ambição, de demonstrar a necessidade de uma atuação específica, estratégica e inteligente da segurança pública no cenário digital.

O crime sempre existiu, com denominações diferentes. Em tempos passados crime e pecado não indissociáveis, e com o tempo, com estudos científicos e a evolução bibliográfica de estudiosos, a etimologia do crime e sua genética foi ganhando contornos mais estruturados. Hoje, em termos jurídicos é denominado como um comportamento, seja comissivo ou omissivo, direcionado a um fim específico, de violar um bem jurídico penalmente protegido pelo ordenamento jurídico. (BARRETO, p. 36)

Conforme doutrina, uma característica peculiar dos cibercriminosos brasileiros é a de que eles concentram as fraudes contra pessoas e empresas brasileiras, sendo uma das razões para isso justamente a legislação vaga, que não pune esses criminosos de forma eficaz, com os bandidos virtuais passando pouco ou nenhum tempo presos. (Assolini apud BARRETO, p. 37)

Cabe destacar que na ciência criminológica o crime é observado de uma maneira diversa, sendo uma atuação massiva e reiterada que causa um dessabor ou transtorno social onde há o consenso de sua punibilidade, isso de acordo com a doutrina moderna.

Entretanto, de tempos em tempos a ação delitiva acontece em diferentes circunstâncias e ambientes. Busca-se sempre uma brecha na vigilância, onde há uma inexpressiva ausência de proteção.

O desenvolvimento de grandes centros urbanos provocou o encurtamento de distâncias e o aumento populacional deram origem ao crescimento da criminalidade e da violência. Há quem diga que o crime ocorre na convergência e encontro de vítima potencial, autor audaz e ambiente carente de vigia. (OLIVEIRA)

Assim, havendo tal encontro, fatalmente ocorrerá o crime. No que tange a esse terceiro elemento trazido, “ambiente carente de vigia”, ele pode se dar em diversas localidades, como, bairros abastados, residências em que seus proprietários estão viajando, estabelecimentos que não tenham sistema de vigilância e proteção, entre diversos outros.

Ocorre que, hoje em dia o maior fluxo monetário se dá no ambiente digital. Além disso, as inovações tecnológicas e progresso da maneabilidade de dados se dão contemporaneamente

nesse ambiente. Ou seja, na internet é possível basicamente armazenar integralmente dados pessoais e sensíveis a respeito de indivíduos, famílias, grupos, ou até mesmo de nações.

Considerando essa situação, por óbvio, e levando em conta que muitos hoje em dia carecem de ignorância ainda para proteger os próprios dados e ainda se tornar um ambiente fácil para aplicação de golpes, o crime tem se migrado para o ambiente digital, usando façanhas modernas, uma engenharia social mais sofisticada com detalhes que escapam o conhecimento leigo desse ambiente. (BARRETO, p. 27 - 29)

O desenvolvimento de novas tecnologias na sociedade tem um papel fundamental em aprimorar métodos que tornam as estratégias de prevenção e segurança mais acessíveis e eficazes. A tecnologia pode ser uma ferramenta valiosa no enfrentamento e na prevenção da violência.

Assim, o presente trabalho irá demonstrar de maneira esclarecida sobre a classificação dos crimes cibernéticos e como tem ocorrido de forma gradual e massiva, merecendo assim também e no mesmo compasso o progresso da atuação policial para inibir essas atividades.

Afinal, pode os crimes cibernéticos serem investigados ou reprimidos pela Polícia Militar? Tal reflexão é variável e envolve diversos fatores. O primeiro, legislação existente que dê margem de atuação da Polícia Militar nesse tipo de conduta. Segundo a estrutura organizacional da Polícia Militar, se a tropa está preparada para lidar com esse nicho e se tem preparação específica para atuar e combater a atuação criminal no meio digital.

Primordialmente, o policiamento ostensivo incide de forma imediata e repressiva, para cessar o delito em andamento e minimizar suas consequências. Assim, ponto chave que deve ser discutido, como que a Polícia Militar pode atuar para frear os efeitos deletérios dos crimes cibernéticos? Qual a forma e em que momento ela deve agir? Seria encargo da Polícia Militar ou tal atuação fica relegada às investigações da Polícia Civil?

Dada a crescente importância e prevalência dos crimes cibernéticos, é essencial que todas as forças policiais estejam preparadas para lidar, pelo menos inicialmente, com essas ameaças.

A Polícia Militar muitas vezes atua como a primeira linha de resposta em casos de crimes cibernéticos, especialmente quando estes têm consequências imediatas no mundo físico ou quando são reportados diretamente por vítimas ou instituições. Isso requer que os policiais militares tenham um conhecimento básico sobre como identificar e preservar evidências digitais até que especialistas possam assumir.

2 REVISÃO TEÓRICA

Neste capítulo, o qual está subdividido entre outros tópicos, demonstrar-se-á a importância do conhecimento e a utilidade dela no ambiente policial militar sobre os crimes cibernéticos.

A gestão do conhecimento surge como um pilar fundamental na Polícia Militar, direcionando a organização para aprimorar suas operações, estratégias e processos decisórios. Este enfoque no conhecimento abrange desde a identificação de informações chave, como técnicas de combate ao crime e legislação, até a aplicação prática dessas informações, por meio da experiência operacional e do uso de tecnologias inovadoras. O compartilhamento e a documentação eficiente desse saber, aliada ao emprego de plataformas digitais e à educação contínua, são vitais para incorporar o conhecimento nas atividades cotidianas e no planejamento estratégico da Polícia Militar. Tal esforço demanda não apenas recursos adequados, mas também uma cultura organizacional que valorize o conhecimento como um ativo estratégico crucial.

Além disso, no capítulo seguinte, após demonstração da importância do tema dentro da gestão do conhecimento, vai explorar o conceito e as classificações doutrinárias sobre esse tema, e sua incidência no plano prático.

Paralelamente, o enfrentamento dos crimes cibernéticos representa um desafio crescente, exigindo da Polícia Militar não apenas uma atualização constante em termos de legislação e técnicas de investigação, mas também a promoção da conscientização sobre segurança online e a cooperação tanto nacional quanto internacional. Esses crimes, que variam desde invasões de sistemas até violações de privacidade, transcendem fronteiras geográficas, demandando estratégias globais para sua prevenção e punição. A complexidade e a constante evolução desses delitos digitais requerem uma abordagem multifacetada que combine esforços de diferentes setores da sociedade, incluindo a adoção de legislações específicas como o Marco Civil da Internet e a Lei Geral de Proteção de Dados no Brasil, para efetivamente proteger os cidadãos e combater a criminalidade no ciberespaço.

Posteriormente, retratar a transição do crimes do plano concreto para o digital, e assim expor a importância de se conhecer o ambiente virtual para assim concretizar a atuação na repressão dos crimes que ocorrem nesse ambiente.

Por fim, após a obtenção e demonstração de dados, conclusão sobre a necessidade de uma especialização e aprofundamento sobre o tema.

2.1 GESTÃO DE CONHECIMENTO NO AMBIENTE POLICIAL MILITAR SOBRE CRIMES CIBERNÉTICOS

A administração do conhecimento nas forças da Polícia Militar representa um pilar crucial para o desenvolvimento e refinamento constantes de suas ações, estratégias e decisões.

Inicialmente, é necessário reconhecer as informações vitais para alcançar os objetivos da Polícia Militar. Isso engloba métodos de combate à criminalidade, táticas de vigilância, domínio da legislação pertinente, habilidades para manejar crises e mais.

Encoraja-se a produção de novos saberes a partir das vivências operacionais, treinamentos, exercícios simulados e pela incorporação de novas tecnologias. Investigação e desenvolvimento também são fundamentais, assim como a colaboração com entidades educacionais e outras organizações de segurança. A capacidade de transmitir conhecimentos e informações entre os integrantes é essencial para uma gestão eficaz do saber. Isso pode ser realizado através de plataformas de gestão do conhecimento, redes internas, encontros, capacitações e informativos.

É vital documentar e preservar os conhecimentos adquiridos de forma sistemática e acessível, utilizando-se de bases de dados, arquivos digitais e bibliotecas físicas.

O objetivo da administração do conhecimento é, sobretudo, sua aplicação prática nas atividades cotidianas e no planejamento estratégico da Polícia Militar, o que demanda formação contínua e a revisão de métodos a partir das experiências obtidas.

É primordial fomentar uma cultura que preze pela partilha de saberes, educação constante e inovação. Isso implica no reconhecimento e premiação das contribuições individuais ao acervo de conhecimento da entidade.

A implementação de tecnologias adequadas é crucial para apoiar a gestão do conhecimento.

A implementação bem-sucedida da gestão do conhecimento na Polícia Militar exige um comprometimento liderança, recursos suficientes e uma estratégia que valorize o conhecimento como um ativo estratégico vital para a organização.

Desse modo, é de suma importância o aperfeiçoamento sobre os crimes cibernéticos, seu progresso e gênese, e como se dão no plano concreto, para que assim se possa articular planos e estratégias no combate a essa inovadora modalidade criminosa.

A efetividade da Polícia Militar na investigação de crimes cibernéticos também depende de uma legislação clara e atualizada que defina os limites da atuação policial, os direitos das vítimas e as penalidades para os infratores.

Dado o caráter transnacional de muitos crimes cibernéticos, a cooperação entre diferentes forças policiais e agências, tanto em nível nacional quanto internacional, é essencial. A Polícia Militar pode ter que colaborar com outras entidades para rastrear e combater eficazmente redes de criminosos que operam além das fronteiras nacionais.

Além da atuação direta, a PM tem um papel importante na promoção da conscientização sobre crimes cibernéticos entre a população. Isso pode incluir campanhas educativas sobre práticas seguras na internet, identificação de golpes comuns e a importância de reportar tais crimes às autoridades.

Enquanto a PM pode não ser a principal responsável pela investigação de crimes cibernéticos, sua participação é vital na resposta inicial, na coleta de evidências e no suporte às unidades especializadas, exigindo constante atualização e cooperação entre diversas entidades para enfrentar esses desafios modernos.

2.2 CONCEITO DE CRIMES CIBERNÉTICOS

Os crimes cibernéticos são infrações realizadas através da internet ou por qualquer sistema de informática, com a finalidade de obter ganhos ou vantagens ilícitas. Estes atos ilícitos ocorrem no espaço digital. (OLIVEIRA, 2024)

Englobam todas as ações que, de acordo com a lei, são consideradas ilegais, injustas e reprováveis, executadas contra ou por meio de sistemas computacionais. Usam manobras invasivas, em que adentram banco de dados de caráter pessoal, obtém informações, e as utilizam em seu bel prazer.

Outras formas de referir-se a atos cibernéticos incluem, Cibercrimes, Delitos informáticos, Ilícitos na internet, Delitos virtuais, Infracções digitais, Delitos de computador, Ilícitos computacionais, Delitos eletrônicos, e, por fim, Infracções telemáticas.

Os crimes cibernéticos podem ocorrer à distância, em que a conduta e o resultado se desenvolvem em dois ou mais países, ou, podem se desenvolver em duas ou mais localidades dentro do mesmo país, à que se chama de crime plurilocal.

Conforme Ivette Senise Ferreira (2005, p. 261), os crimes cibernéticos puros são “[...] atos dirigidos contra um sistema de informática, tendo como subespécies atos contra o computador e atos contra os dados ou programas de computador.” (FERREIRA, Ivette Sanise. Direito & internet: aspectos jurídicos relevantes. 2. ed. São Paulo: Quartier Latin, 2005.).

Diversas normas preveem os crimes cometidos no âmbito cibernético, isso, inclusive, após convencionado internacionalmente no tratado de Budapeste, e promulgado por meio do Decreto nº 11.491 de 2023, que prevê o combate a esse tipo de crime. O computador serve tanto como alvo quanto como ferramenta para a realização do delito. São cometidos contra sistemas informáticos e se dividem em ações contra o hardware e ações contra dados ou softwares. (BARRETO, p. 25)

Tanto a realização quanto a conclusão do delito acontecem no ambiente virtual ou por meio de tecnologias da informação. O direito protegido é a segurança e a privacidade das informações processadas eletronicamente. Estes delitos são exclusivos do ambiente online.

Constituem ações que comprometem a proteção e a confiança nas informações, colocando em risco a estrutura dos sistemas informáticos.

A legislação atual prevê diversos exemplos que ocorrem no contexto atual e estão regulamentados, como, Invasão de dispositivo informático (art. 154-A do CP), Interrupção ou perturbação de serviço informático, telemático ou de informação de utilidade pública (art. 266 do CP), entre outros.

Lado outro, os crimes cibernéticos impuros, ou acessórios, são "condutas proibidas por lei, sujeitas a pena criminal e que se voltam contra os bens jurídicos que não sejam tecnológicos já tradicionais e protegidos pela legislação, como a vida, a liberdade, o patrimônio, etc." (Combate à pornografia infantojuvenil com aperfeiçoamentos na identificação de suspeitos e na detecção de arquivos de interesse. MINISTÉRIO PÚBLICO FEDERAL. Crimes cibernéticos. Brasília: MPF, 2018).

São executados utilizando mecanismos virtuais ou eletrônicos, ainda que essa técnica não seja explicitamente mencionada na definição legal do delito (o qual pode ser cometido por outras vias). Englobam atos realizados por meio de tecnologia da informação, o ambiente virtual é somente um dos possíveis meios para realizar o delito.

Trata-se de infrações já conhecidas que se adaptaram para usar a tecnologia de informação como meio de execução – recorrendo à internet para facilitar ou mascarar o ato ilícito, através de ações meticulosas, engenharia social, ludibriando as vítimas para que, em muitos casos, elas mesmas forneçam informações pessoais.

O foco não está em comprometer dados digitais, mas sim em atacar outros interesses jurídicos protegidos, atingindo o patrimônio particular, devassando a vida privada, e usando desses dados obtidos subvertendo o bem jurídico alheio.

Casos que exemplificam, são os crimes contra a honra praticados na internet, que envolvam trocas ou armazenamento de imagens com conteúdo de pornografia infantil,

estelionato, o Revenge Pornô, ou, também, sequestrando dados importantes para a pessoa e exigindo vantagem indevida para devolver esses dados, ataque comumente conhecido como "RANSWARE".

Cabe destacar que, em razão de sua repercussão que ultrapassa barreiras transnacionais, é até mesmo vislumbrando no âmbito internacional, estando regulamentada na Convenção sobre Crimes Cibernéticos de Budapeste. Essa convenção foi firmada em 23 de novembro de 2001, e promulgada no território nacional, por meio do decreto nº 11.491, em 12 de abril de 2023, o qual trata de diversos temas envolvendo crime cibernético.

Paralelo a isso, temos algumas normas que tem alinhamento com o assunto pertinente a proteção de dados no meio digital, como, o Marco Civil da Internet (Lei Nº 12.965, de 23 de abril de 2014), o qual estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil, e, a Lei Geral de Proteção de Dados (Lei Nº 13.709 de 14 de Agosto de 2018), que dispões sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Além disso, e sem maiores aprofundamentos, intrigante que por conta da possibilidade de atuação nos crimes cibernéticos, cada vez mais vem sendo necessário uma delimitação de competência jurisdicional para julgar essas condutas, pois, muitas vezes a atuação do agente ocorre num determinado lugar, mas o resultado se dá em outro.

Há algumas passagens esparsas que estabelecem a competência, mas não abrange todo e qualquer envolvendo crime cibernético, como o estelionato eletrônico, definido no art. 171, §4º,do CP:

§ 4º Nos crimes previstos no art. 171 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), quando praticados mediante depósito, mediante emissão de cheques sem suficiente provisão de fundos em poder do sacado ou com o pagamento frustrado ou mediante transferência de valores, a competência será definida pelo local do domicílio da vítima, e, em caso de pluralidade de vítimas, a competência firmar-se-á pela prevenção.

Para além disso, e ainda procurando precisar, afinar ou definir para uma compreensão maior do assunto sobre crimes cibernéticos, cita-se algumas condutas que podem caracterizar os crimes cibernéticos.

Estupro virtual, o qual, segundo entendimento do eminente e brilhante professor Rogério Greco, para caracterizar o "estupro virtual", não há necessidade de contato físico entre o agente e a vítima, "que poderá estar a milhares de quilômetros de distância do seu agressor" (GRECO,

2023, p.2033). Há evidente tendência jurisprudencial a respaldar esse entendimento da caracterização do “estupro virtual” sem contato físico direto, como no caso do brilhante voto do Ministro Rogério Schietti no HC 478.310 PA2018/0297641-8-PA.

Sextorsão, que consiste na utilização de informações, fotos e vídeos de teor sexual para constranger a vítima a fazer algo mediante a ameaça de divulgação desse conteúdo. Em grande parte, exige que a vítima exiba o seu próprio corpo e execute ações através de ligações web, ou, grave a si fazendo ações de caráter sexual e encaminhe para o autor.

Fraude por e-mail, que é um tipo de golpe que usa o e-mail para enganar as vítimas e fazê-las revelar informações pessoais ou transferir fundos para contas fraudulentas. Nesses casos, simula-se ser uma empresa que necessita do fornecimento de informações pessoas para corrigir alguma irregularidade encontrada na conta. Após o ganho desses dados, fornecidos com esse ardil, utiliza-se para o saque indevido da vantagem.

Ciberextorsão, ou, sequestro de dados (“Ransomware”), que é extorquir alguém por meio do sequestro de dados sensíveis e pessoais de alguma pessoa para que ela colabore na obtenção de ganho ou vantagem ilícita do agente.

Pirâmide financeira digital, que são modelos de negócio nos quais a principal fonte de receita advém da captação de novos participantes, que pagam uma taxa para ingressar. Essa prática é considerada fraudulenta, pois seduz investidores iniciantes com a expectativa de lucros rápidos e elevados. Tais esquemas são marcados por um baixo custo inicial para participação, vendas desbalanceadas de produtos ou, em muitos casos, a ausência de um produto real, limitadas informações sobre o investimento e seus potenciais riscos, a obscuridade em relação à empresa envolvida, e a oferta de ganhos desproporcionais.

Jogos de azar ilegais, cada vez mais crescente, que consiste numa prática irregular adotada por alguns influenciadores nas redes sociais. Além de jogos de azar, rifas sem regulamentação, e jogos de apostas. São consideradas criminosas por conter, em grande maioria, algum algoritmo que já induz ao prejuízo dos participantes, fragilizando o patrimônio dos envolvidos e criando falsas expectativas, os quais se dão em grande parte no meio digital.

Golpe do PIX, podendo caracterizar tanto estelionato, furto, roubo, ou até mesmo extorsão, dependendo da maneira como é praticada e se foi empregado violência ou grave ameaça na ação delituosa.

Armazenamento de pornografia infantil, conduta lamentável e abjeta, que infelizmente praticada e comercializada, inclusive, no seio do mercado negro ingresso na mais profunda camada da internet, conhecida como “Deep Web”, ou “Dark Web”.

Clonagem de Whatsapp, de modo que a intenção do agente é devassar a comunicação da vítima e assim expor suas intimidade e vida privada.

Em seguimento, e aliado à isso, até mesmo tomando progressivamente espaço no contexto social e sendo utilizado em alguns golpes, a INTELIGÊNCIA ARTIFICIAL – IA. A IA facilita alguns trabalho, torna menos oneroso a elaboração de texto, edição de mídia, entre muitas outras funções, até mesmo ocorrendo em tempo real. Não muito tempo, alguns agentes se valeram dessa ferramenta poderosa para tentar extorquir uma vítima, de modo que a usaram para simular ser a filha dela. O intrigante da situação, é que a IA simulou instantaneamente e com as mesmas características da filha, com voz, feições, e todo o perfil, quase coagindo a vítima a desfazer de seu patrimônio para salvar sua filha, fato esse ocorrido ainda no mês de março do ano corrente (2024). (VILARINHO. 2024)

Assim, perceba-se a importância de se compreender os crimes cibernéticos para então explorar a relevância de procurar meios e estratégias para combater esse modo de execução. O crime, assim como o ser humano, também evoluiu e com ele seus métodos e estratégias. Hoje ele explora a deficiência ou ignorância tecnológica e informática do homem, donde armazena praticamente todos os dados referentes à sua vida íntima, privada e particular. Essa relação entre crime e internet se torna mais danoso ante os prejuízos potenciais de causar a um indivíduo, à coletividade, bem como à administração pública. Por isso, há a necessidade de aprofundar o conhecimento dos meios e técnicas utilizadas para o cometimento desses crimes com a finalidade de aprimorar a interceptação dessas condutas, com intuito de impedir sua consumação ou exaurimento.

2.3 A ERA DIGITAL E A MIGRAÇÃO DA CRIMINALIDADE PARA O AMBIENTE VIRTUAL

Vivemos atualmente a era da informação, definido pela transição de tecnologias tradicionais, como as analógicas e mecânicas, para sistemas digitais avançados. Essa evolução teve início no século passado, acelerada pela chegada dos computadores pessoais, da internet e dos dispositivos móveis.

Ocorreram progressos notáveis na área de tecnologia da informação e comunicação, revolucionando completamente as formas de interação social, métodos de trabalho, processos educacionais e entretenimento. A capacidade de gerar, compartilhar e acessar uma quantidade imensa de dados de maneira rápida e eficaz é uma das principais conquistas desta época.

Graças à internet e às plataformas de mídia social, a comunicação e colaboração entre indivíduos ao redor do globo são facilitadas, ocorrendo quase que instantaneamente. Nunca foi tão fácil obter informações, com uma riqueza de conteúdo educacional e informativo disponível na internet para aqueles conectados.

Avanços Tecnológicos Constantes: A inovação em tecnologias como a inteligência artificial, a robótica e as blockchain, ou moedas virtuais, que facilitam as transações comerciais entre particulares.

Além disso, as empresas estão se reformulando para operar no ambiente digital, abrangendo áreas que vão do e-commerce à telemedicina e serviços financeiros digitais.

Com isso, vem surgindo novas carreiras, enquanto cresce a demanda por habilidades digitais e tecnológicas, como digital influencers, e congêneres.

A tecnologia e inovação abre portas para avanços significativos em educação, desenvolvimento social e crescimento econômico. Contudo, concomitante a isso, a era digital também traz desafios significativos, como preocupações com a privacidade, a segurança dos dados, o acesso desigual à tecnologia e questões éticas em torno da IA, tendo em consideração que muitos aproveitam das facilidades para o cometimento de condutas infracionais.

Assim, diante do que fora exposto até agora, nota-se uma transição do crime para espaços digitais, que representam uma evolução nas práticas ilícitas, adaptando-se ao advento da internet e ao mundo cada vez mais digitalizado. À medida que a sociedade se torna mais conectada digitalmente, os criminosos exploram o ciberespaço para realizar atividades ilícitas, tirando vantagem da conectividade generalizada, do potencial para anonimato e dos desafios que a jurisdição transnacional.

Essa mudança para o digital abarca uma série de práticas criminosas, tais como, phishing (criminosos ludibriam pessoas para adquirir dados pessoais e financeiros); lavagem de dinheiro digital; golpes envolvendo instituições financeiras e o emprego de moedas virtuais para transações ilícitas; comércio de produtos ilegais; abusos sexuais via online e tráfico de pessoas, entre outros.

Ante à sua capacidade de operar além das fronteiras nacionais, permitindo que os criminosos ajam de qualquer local do mundo, muitas vezes em locais com legislações pouco rigorosas sobre o cibercrime, a rapidez e a possibilidade de anonimato que a tecnologia proporciona também tornam a identificação e a detenção dos infratores mais complicadas.

Dessa forma, percebe-se a necessidade de despender esforços entre as comunidades e organizações internacionais, além de governos, bem como o setor privado também, no sentido

de fortalecer a segurança digital, promover a conscientização sobre práticas seguras na internet e fomentar a colaboração internacional.

No âmbito da Policia Militar, isso envolve desenvolver e aprofundar mais ainda sobre o assunto, conhecer outras localidades que já desenvolvam um trabalho direcionado no combate a esse tipo de crime, mesmo que envolva instituições diversas, melhorar as técnicas de investigação cibernética e incentivar a cooperação entre diferentes atores para compartilhar informações e estratégias eficazes no combate ao crime digital.

3 METODOLOGIA

A metodologia adotada nesta pesquisa visa investigar a gestão de conhecimento sobre os crimes cibernéticos e como que são apuradas esse tipo de conduta pela Polícia Militar do Estado de Goiás (PMGO). Para alcançar esse propósito, serão seguidas diversas etapas que compreendem levantamento bibliográfico e documental, coleta de dados, tabulação e análise de dados, além de considerações éticas.

3.1 Coleta de Dados:

A coleta de dados será realizada por meio de encaminhamento de ofício às instituições coirmãs dos diversos entes federativos de nossa república para saber e compreender se há departamento especializado na apuração de condutas envolvendo crimes cibernéticos e a forma como procedem. Essas diferentes abordagens permitirão uma compreensão abrangente e multifacetada do tema em estudo.

3.2 Tabulação e Análise de Dados:

Os dados coletados serão tabulados e analisados qualitativamente, utilizando técnicas de análise de conteúdo e estatística descritiva. Serão identificados padrões, tendências e desafios, fornecendo subsídios para reflexões e recomendações futuras.

3.6 Aspectos Éticos:

Será solicitada autorização formal via Sistema Eletrônico de Informações (SEI) para realização da pesquisa dentro da PMGO e para encaminhamento de ofício às Polícias Militares de outros Estados.

4 RESULTADOS E DISCUSSÃO

Para melhor conclusão, há a necessidade de se perquirir a pesquisar para melhor afinamento do campo de pesquisa, de modo que foi realizada através de um questionário online com seis questões de múltipla escolha, coletando um total de 24 respostas, por meio da plataforma digital Google Forms. Os dados foram analisados utilizando percentuais para melhor compreensão da concordância ou discordância dos respondentes em relação às afirmações propostas, tendo como alternativas múltiplas em todos os questionamentos as opções, “concordo totalmente”, “concordo parcialmente”, e , “não concordo”.

Contudo, antes da apresentação dos resultados, faz-se necessário breve exposição. Este trabalho analisa as percepções sobre a capacitação da Polícia Militar frente aos desafios impostos pelos crimes cibernéticos. A metodologia utilizada, foi a quantitativa, na qual, das 24 respostas coletadas, percebeu-se que há a necessidade premente de capacitação da Polícia Militar. Os resultados indicam uma forte concordância de que os crimes estão migrando para plataformas virtuais e que há necessidade significativa de especialização das forças policiais nesse âmbito.

Assim, a digitalização crescente das atividades cotidianas tem sido acompanhada por um aumento correspondente na incidência de crimes cibernéticos. E mais do que isso, é significativo a maneira audaz, ou, o modo de operar e agir dos criminoso, que cada dia mais se tornam mais ardilosos e engenhosos no cometimento desses crimes. Por conta do mecanismo utilizado, é de fulcral urgência também capacitar a tropa para se equiparar em termos de conhecimento, para assim, tomar providência para se prevenir essas condutas infracionais.

Este trabalho investiga a percepção sobre a preparação e resposta da Polícia Militar a tais ameaças, crucial para o desenvolvimento de políticas de segurança pública eficazes.

Então, separando-se por tópicos, expor-se-á os dados obtidos.

4.1. Percepção sobre a migração do crime para o ambiente virtual

A maioria dos participantes (91,7%) concorda totalmente que o crime está migrando do ambiente físico para o virtual, refletindo a preocupação crescente com a segurança cibernética.

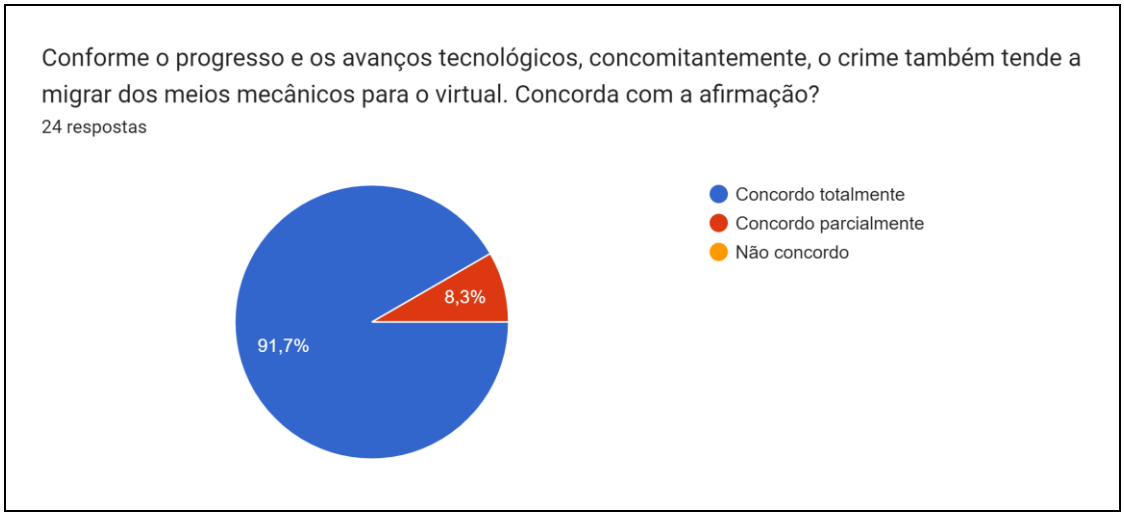

Figura 1. Percepção sobre a migração do crime para o ambiente virtual. Extraído de pesquisa através do Google Forms.

4.2. Compreensão e capacitação da Polícia Militar

Apesar de 37,5% concordarem totalmente e 50% concordarem parcialmente que a Polícia Militar compreende o que são crimes cibernéticos, a confiança na capacidade de resposta a esses crimes é mais baixa. Somente 12,5% concordam totalmente que a Polícia Militar está preparada, enquanto 50% não concordam com essa afirmação.

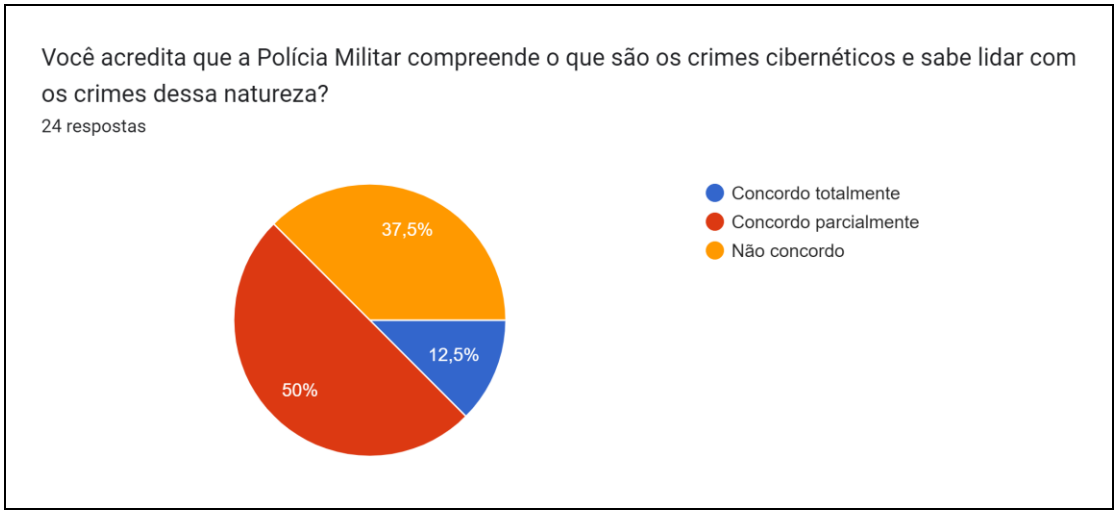

Figura 2. Compreensão dos crimes cibernéticos. Extraído de pesquisa através do Google Forms.

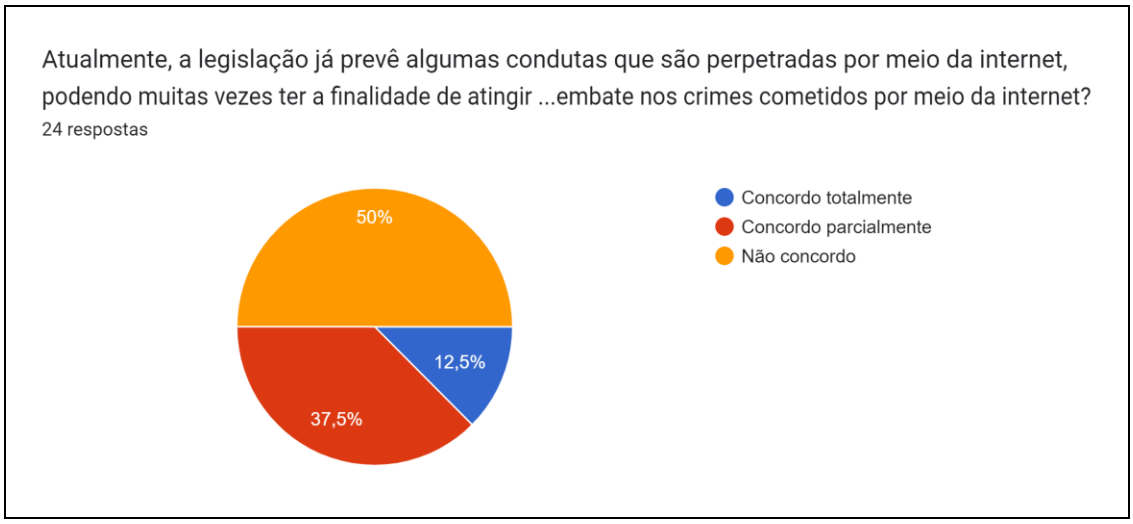

Figura 3. Preparo da Polícia no combate aos crimes cibernéticos. Extraído de pesquisa através do Google Forms.

Cabe destacar que a pergunta formulada na imagem anterior, em seu inteiro teor, era a seguinte, “Atualmente, a legislação já prevê algumas condutas que são perpetradas por meio da internet, podendo muitas vezes ter a finalidade de atingir dados armazenados, ou valendo-se dela como meio para algum fim. Você concorda que a Polícia Militar está suficientemente preparada para o embate nos crimes cometidos por meio da internet?”

4.3. Necessidade de especialização e treinamento

A necessidade de especialização é enfaticamente apoiada, com 83,3% dos participantes concordando totalmente com a necessidade de capacitação específica para atuação em crimes cibernéticos. Além disso, 66,7% concordam totalmente que o conhecimento sobre crimes cibernéticos deve ser incluído na grade curricular dos cursos de formação da Polícia Militar.

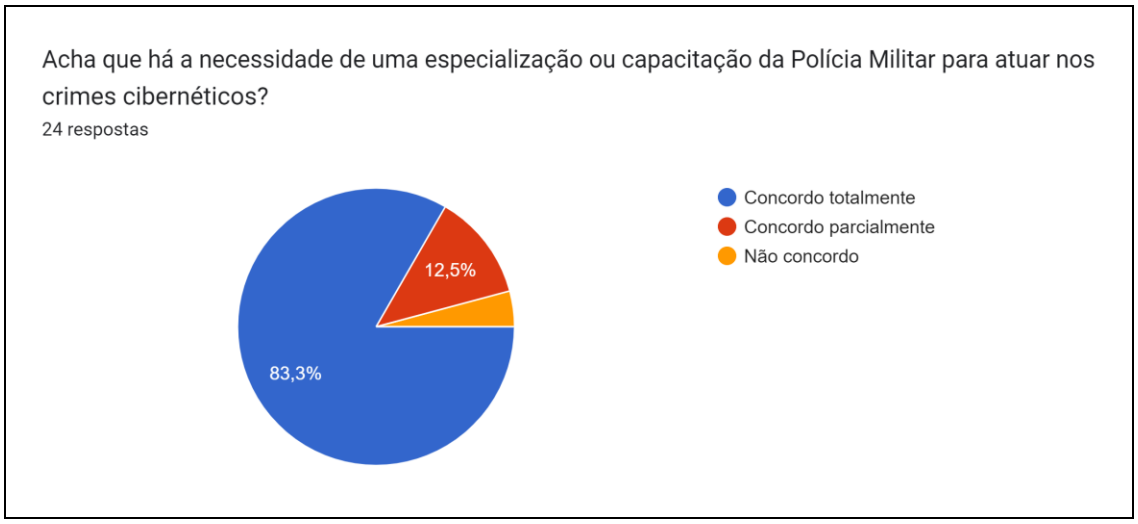

Figura 4. Necessidade de capacitação na Polícia Militar. Extraído de pesquisa através do Google Forms.

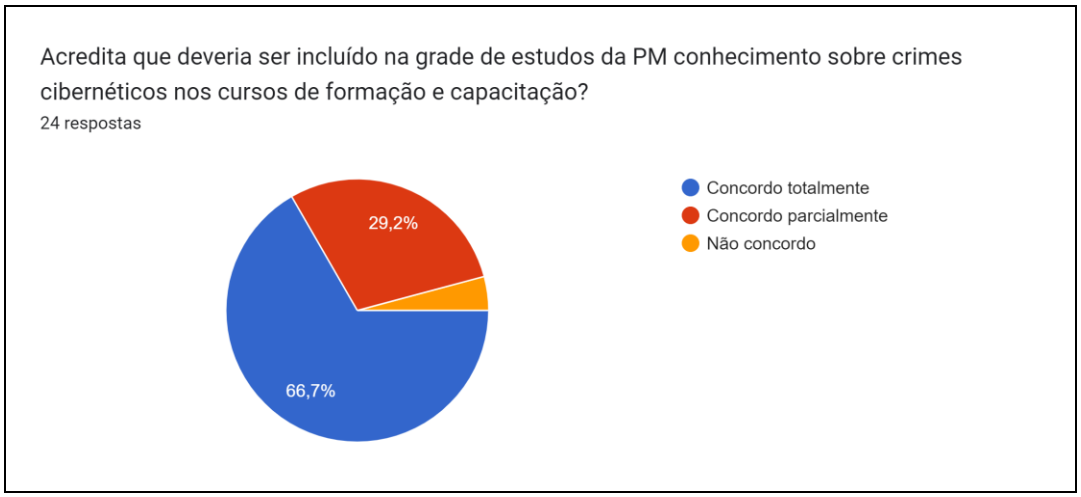

Figura 5. Necessidade de especialização. Extraído de pesquisa através do Google Forms.

4.4. Importância do conhecimento técnico específico

A maioria (62,5%) também concorda totalmente que é importante para a Polícia Militar ter conhecimento sobre as especificidades mecânicas e lógicas dos sistemas de computação para efetivamente combater crimes cibernéticos.

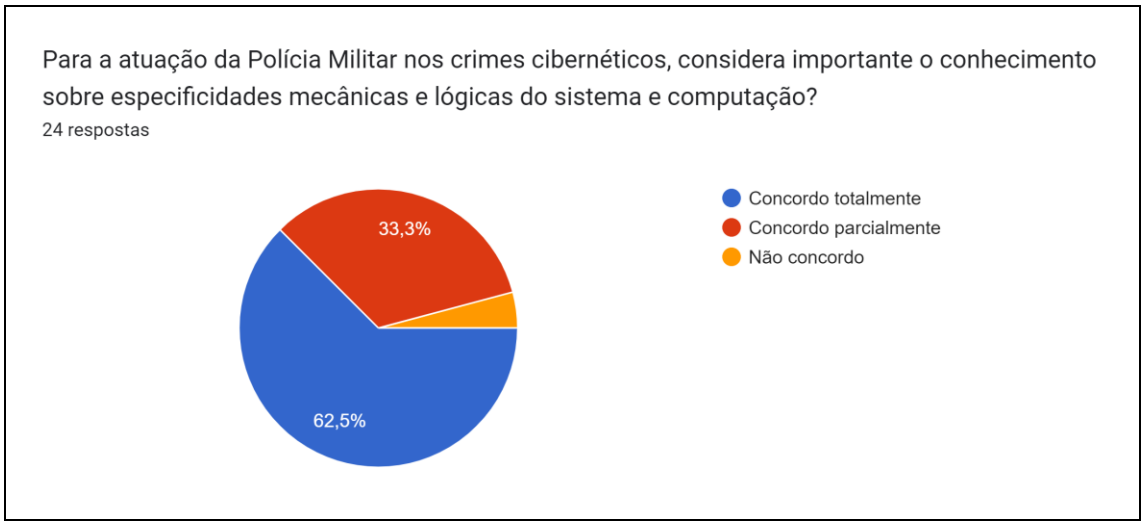

Figura 6. Importância do conhecimento técnico específico. Extraído de pesquisa através do Google Forms.

A partir dos dados e gráficos apresentados, observa-se uma marcante e predominante concordância entre os participantes quanto ao deslocamento dos crimes para o meio virtual, evidenciando um entendimento amplo sobre como as formas de criminalidade estão evoluindo em resposta ao progresso tecnológico. Esse entendimento indica uma conscientização sobre a natureza mutável do crime na era digital e a necessidade subsequente de ajustar as estratégias de segurança pública.

Embora exista uma aceitação razoável de que a Polícia Militar entende o conceito de crimes cibernéticos, a confiança na sua capacidade atual para gerenciar esses desafios é consideravelmente reduzida. Apenas uma minoria dos respondentes considera que a Polícia Militar está completamente equipada para enfrentar crimes cibernéticos, indicando uma possível deficiência em sua preparação e capacidade operacional.

A necessidade de especialização e formação específica em crimes cibernéticos é evidente e significativa, conforme demonstrado pelo alto índice de participantes (83,3%) que apoiam a importância de treinamentos direcionados. Adicionalmente, a maioria dos respondentes concorda que os conhecimentos sobre crimes cibernéticos devem ser integrados aos currículos de treinamento da Polícia Militar. Essa clara preferência por educação especializada reflete diretamente a complexidade e a necessidade de competências técnicas específicas para combater eficientemente os crimes cibernéticos.

A análise dos dados sublinha a necessidade de integrar conhecimentos técnicos aprofundados sobre sistemas e computação nas operações da Polícia Militar. O amplo apoio dos participantes a essa ideia revela que, além de um entendimento básico sobre crimes

cibernéticos, é essencial que haja uma compreensão detalhada das ferramentas e tecnologias utilizadas nesses crimes.

Assim, a pesquisa conclui que há uma necessidade urgente de reformular e fortalecer a capacitação da Polícia Militar em relação aos crimes cibernéticos. Isso não apenas aumentaria a eficácia da resposta policial, mas também alinharia as forças de segurança com as exigências contemporâneas de proteção e segurança no ambiente digital. O envolvimento dos respondentes indica um reconhecimento público da defasagem existente e uma chamada para ação no sentido de preparar melhor os oficiais para enfrentar essa nova fronteira de atividades criminosas.

Por fim, este estudo sublinha a importância de uma estratégia integrada que combine educação, treinamento especializado e desenvolvimento de competências técnicas para que a Polícia Militar não apenas acompanhe, mas efetivamente combata a crescente onda de crimes cibernéticos. A implementação de tais medidas não só fortaleceria a segurança interna, mas também reforçaria a confiança pública na capacidade das forças policiais de proteger os cidadãos nas diversas esferas de suas vidas.

5 - CONCLUSÃO

Em síntese, os crimes cibernéticos representam uma evolução significativa das práticas ilícitas, adaptando-se ao surgimento da internet e ao mundo cada vez mais digitalizado. Com a sociedade mais conectada digitalmente, os criminosos exploram o ciberespaço para realizar atividades ilícitas, aproveitando a ampla conectividade e o potencial de anonimato. Esses crimes englobam uma ampla gama de ações, desde phishing até lavagem de dinheiro, fraudes financeiras e abusos sexuais online.

Devido à capacidade dos cibercriminosos de operar além das fronteiras nacionais e à complexidade de rastrear e capturar esses infratores, é essencial um esforço colaborativo entre comunidades, organizações internacionais, governos e o setor privado. Esse esforço deve focar no fortalecimento da segurança digital, promoção da conscientização sobre práticas seguras na internet e incentivo à cooperação internacional.

A pesquisa apresentada indica que, embora a Polícia Militar tenha uma compreensão básica dos crimes cibernéticos, há uma necessidade urgente de especialização e formação específica. A maioria dos participantes apoia a inclusão de conhecimentos técnicos e treinamentos direcionados no currículo da Polícia Militar, destacando a complexidade e a necessidade de competências técnicas específicas para combater eficazmente esses crimes.

Portanto, a conclusão enfatiza a importância de reformular e fortalecer a capacitação da Polícia Militar em relação aos crimes cibernéticos. Integrar educação, treinamento especializado e desenvolvimento de competências técnicas é essencial para que as forças de segurança acompanhem e combatam eficazmente a crescente onda de crimes cibernéticos. Implementar tais medidas não só aumentaria a eficácia da resposta policial, mas também reforçaria a confiança pública na capacidade das forças policiais de proteger os cidadãos nas diversas esferas de suas vidas.

REFERÊNCIAS

MITNICK, Kevin D - **A arte de enganar**/ Kevin D. Mitnick; William L. Simon; Tradução: Kátia Aparecida Roque; revisão técnica: Olavo José Anchieschi Gomes. 1963.

BARRETO, Alesandro Gonçalves. **Manual de Investigação Cibernética à luz do Marco Civil da Internet**. Brasport livros e Multimídia LTDA. São Paulo. 2016.

VILARINHO, Juliana. **Criminosos usam deepfake de filha para dar golpe em mãe, mas falham; entenda**. Disponível em: (https://www.techtudo.com.br/noticias/2024/03/criminosos-usam-deepfake-de-filha-para-dar-golpe-em-mae-mas-falham-entenda-edsoftwares.ghtml). Acesso em: 15 de abril. 2024.

OLIVEIRA, Elenilcio Dauto de. ALEXANDRE, Weliton do Nascimento. **Direito digital no combate a crimes cibernéticos**. Disponível em: (https://www.nucleodoconhecimento.com.br/lei/combate-a-crimes-ciberneticos). Acesso em: 25 de fevereiro de 2024

NORTON. O que é crime cibernético? Disponível em: (http://br.norton.com/cybercrime-definition). Acesso em: 05 de março de 2024.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Disponível em: (https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm). Acesso em: 12 de abril. 2024.

BRASIL. Lei nº 12.737, de 30 de novembro de 2012. Disponível em: (http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm). Acesso em: 12 de abril de 2024.

BRASIL. Decreto nº 11.491, de123 de abril de 2023. Disponível em: (https://www.planalto.gov.br/ccivil_03/_Ato2023-2026/2023/Decreto/D11491.htm). Acesso em: 12 de abril de 2024.

BRASIL. Decreto nº 8.771, de 11 de maio de 2016. Disponível em: (http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2016/Decreto/D8771.htm). Acesso em: 12 de abril de 2024.