ESTRATÉGIAS DE POLÍTICAS PÚBLICAS NO COMBATE AOS CRIMES CIBERNÉTICOS: uma análise crítica

Stanley Araújo Pena *
Cid Gonçalves Filho **
João Pedro Lima de Medeiros Galiza ***
Júnio Souto Marques ****

RESUMO: O estudo insere-se no contexto do crescimento exponencial dos crimes cibernéticos e seus impactos na segurança pública nacional e internacional. Objetivou-se analisar criticamente as políticas públicas existentes e propor estratégias eficazes e sustentáveis para o enfrentamento dessa modalidade criminal em expansão. A metodologia adotada baseou-se em revisão bibliográfica sistemática, com recorte temporal de 2018 a 2024, abrangendo bases acadêmicas como Scielo, Portal Capes, Spell e revistas especializadas em segurança pública. Os resultados indicam que os crimes cibernéticos, em razão de sua sofisticação técnica, transnacionalidade e impacto social, exigem políticas públicas adaptativas, integradas e tecnologicamente atualizadas. Constatou-se que medidas como educação digital, investimento em tecnologias de defesa cibernética, cooperação internacional, fortalecimento legal e institucional, além da ampliação da cultura de cibersegurança, são fundamentais para ampliar a resiliência digital do Estado e da sociedade. Conclui-se que a eficácia das políticas públicas está condicionada a um esforço contínuo, colaborativo e inovador, com participação articulada do setor público, da iniciativa privada e da sociedade civil. Recomenda-se, como trabalhos futuros, o aprofundamento na análise da eficácia das cooperações internacionais, das tecnologias emergentes como IA e *blockchain*, e da governança cibernética comparada em diferentes países.

Palavras-chave: crimes cibernéticos; segurança pública; políticas públicas; prevenção digital; estratégias governamentais.

DOI: https://doi.org/10.36776/ribsp.v7i18.244

Recebido em 01 de agosto de 2024.	Aprovado em 20 de agosto de 2024.

* Universidade FUMEC. ORCID: https://orcid.org/0000-0002-2472-7170 - CV: http://lattes.cnpq.br/2788915842391085
** Universidade Federal de Minas Gerais (UFMG). CV: http://lattes.cnpq.br/3574306384505737 .
*** Polícia Militar de Minas Gerais (PMMG).
***** Polícia Militar de Minas Gerais (PMMG).

PUBLIC POLICY STRATEGIES TO COMBAT CYBERCRIMES: A critical analysis

ABSTRACT: This study is situated within the context of the exponential growth of cybercrimes and their impact on national and international public security. Its objective was to critically analyze existing public policies and propose effective and sustainable strategies to address this expanding criminal phenomenon. The adopted methodology was based on a systematic literature review, with a temporal scope from 2018 to 2024, covering academic databases such as Scielo, Portal Capes, Spell, and journals specialized in public security. The findings show that cybercrimes, due to their technical complexity, transnational nature, and social impact, demand adaptive, integrated, and technologically updated public policies. The study identified that digital education, investment in cybersecurity technologies, international cooperation, legal and institutional strengthening, and the promotion of a cybersecurity culture are essential for improving state and societal digital resilience. It is concluded that the effectiveness of public policies depends on continuous, collaborative, and innovative efforts, with coordinated participation from the public sector, private entities, and civil society. Future studies should further explore the effectiveness of international cooperation, the use of emerging technologies such as AI and blockchain, and comparative models of cyber governance across different nations.

Keywords: cybercrimes; public security; public policy; digital prevention; government strategies.

1. INTRODUÇÃO

Não é recente o fato de que a revolução digital transformou a maneira como vive-se, trabalha-se e nos relaciona-se. No entanto, essa transformação trouxe consigo um aumento exponencial nos crimes cibernéticos, que se tornaram uma ameaça significativa à segurança individual, corporativa e nacional. Crimes como roubo de identidade, fraudes financeiras, invasões de privacidade e ataques a infraestruturas críticas estão se tornando cada vez mais comuns, exigindo uma resposta robusta e coordenada dos governos.

Os crimes cibernéticos emergiram como uma das principais ameaças à segurança pública na era digital. A rápida evolução da tecnologia, aliada à crescente interconectividade global, proporcionou novas oportunidades para atividades criminosas no ciberespaço. Esses crimes variam desde fraudes financeiras, roubo de identidade e espionagem, até ataques a infraestruturas críticas e disseminação de malwares humanos (Silva Bispo; Binto, 2023).

A natureza transnacional desses delitos dificulta a sua prevenção e combate, pois frequentemente envolvem criminosos operando de diferentes partes do mundo. Além disso, a sofisticação crescente das técnicas utilizadas pelos cibercriminosos desafia constantemente os mecanismos tradicionais de segurança e investigação. Dessa forma, os crimes cibernéticos representam um desafio complexo e dinâmico para a segurança pública, exigindo uma resposta igualmente inovadora e coordenada por parte das autoridades e instituições responsáveis pela manutenção da ordem e proteção dos cidadãos. Busca-se saber: como as políticas públicas podem ser eficazmente desenvolvidas e implementadas para combater os crimes cibernéticos de forma abrangente e sustentável?

O objetivo geral consistiu em analisar e propor estratégias de políticas públicas que possam ser eficazes no combate aos crimes cibernéticos, promovendo a segurança digital e a proteção dos cidadãos. Os objetivos específicos contemplam: identificar as principais formas de crimes cibernéticos e suas implicações para a segurança pública e privada; avaliar as políticas públicas atuais no combate aos crimes cibernéticos em diferentes países e contextos. Propor novas estratégias de políticas públicas baseadas em melhores práticas e inovações tecnológicas e analisar a viabilidade e os desafios na implementação dessas estratégias em diferentes contextos socioeconômicos e culturais.

Justifica-se a crescente dependência das tecnologias digitais em praticamente todos os aspectos da vida moderna torna a segurança cibernética uma questão crítica. A relevância do tema pode ser entendida no sentido de que, investir em políticas públicas voltadas para a cibersegurança é fundamental para proteger as infraestruturas críticas, garantir a integridade dos dados e salvaguardar os direitos dos cidadãos no ambiente digital. Além disso, tais políticas podem estimular o desenvolvimento de tecnologias inovadoras e promover um ambiente de confiança que favoreça o crescimento econômico e a inclusão digital.

A revisão da literatura foi baseada no amparo teórico dos principais autores que tratam do tema proposto. A revisão bibliográfica se baseou nos principais portais como o Scielo, Portal Capes e o Spell, além de revistas específicas de segurança pública. É importante considerar também, uso do recorte temporal considerando as publicações dos últimos cinco anos, ou seja, o intervalo entre 2018 de 2024. Além disso, também foram selecionadas as publicações utilizando boleadores ou descritores: crimes virtuais, crime cibernéticos, segurança pública, enfrentamento, estratégia, em português e inglês para posterior análise crítica das publicações selecionadas.

2. REFERENCIAL TEÓRICO

2.1 Conceito e alcance da segurança pública

Segurança pública significa manter as pessoas protegidas de danos ou perigos. É responsabilidade do governo garantir que todos estejam protegidos contra crimes, terrorismo e desastres naturais. Isso pode envolver coisas como a presença de policiais e bombeiros, a construção de infraestruturas sólidas e a implementação de planos de emergência. A segurança pública é importante para que todos se sintam seguros e possam viver suas vidas sem medo (Gomes; Medrado, 2023).

Silva e Silva (2019) assinalam que segurança pública refere-se ao estado de estar protegido contra perigo ou ataque. É a proteção de pessoas e propriedades contra roubo ou danos. Exemplos de medidas de segurança pública incluem: policiais patrulhando bairros para coibir crimes; câmeras de vigilância em locais públicos para monitorar atividades; postos de segurança nos aeroportos para prevenir o terrorismo e equipes de resposta a emergências para lidar com desastres naturais. Estes exemplos ilustram como a segurança pública é importante para manter uma sociedade segura e estável. Sem medidas de segurança pública em vigor, as pessoas correriam o risco de sofrer danos e os bens ficariam vulneráveis a roubo ou danos.

De acordo com Santos (2020), a segurança pública é a função dos governos que garante a protecção dos cidadãos, das pessoas no seu território, das organizações e das instituições contra ameaças ao seu bem-estar – e à prosperidade das suas comunidades. Para enfrentar os desafios crescentes na área da segurança pública, as instituições e organizações públicas responsáveis podem recorrer à sua própria inteligência para enfrentar antecipadamente possíveis ameaças. Otimizam as suas estruturas internas, utilizam sinergias e equilibram cuidadosamente os custos e benefícios das suas medidas.

As organizações de segurança pública incluem serviços de aplicação da lei, bombeiros e serviços médicos de emergência. As questões de segurança pública que um município, condado, estado ou jurisdição federal pode enfrentar incluem uso de narcóticos, invasão de propriedade, roubo, assédio, delinquência juvenil, vida não autorizada, ruído, lixo, comportamento social inadequado, embriaguez e outros problemas de qualidade de vida (Silva; Marques, 2019).

Geralmente, as organizações estão envolvidas na prevenção e proteção contra eventos que possam pôr em perigo a segurança do público em geral devido a perigos significativos, ferimentos ou danos materiais, tais como crimes ou desastres (naturais ou provocados pelo homem) (Gomes; Medrado, 2023).

2.2 Políticas de segurança pública no Brasil

A segurança pública no contexto brasileiro é o estado de normalidade que permite o usufruto da segurança dos direitos e o cumprimento dos deveres. Pode ser interpretada como a manutenção da ordem pública, isto é, de conjunto de valores, de princípios e de normas que se pretendem ser observadas numa sociedade (Lima; Barbosa, 2020).

A sua alteração ilegítima constitui uma violação de direitos básicos, geralmente acompanhada de violência, que produz eventos de insegurança e criminalidade. É um processo, ou seja, uma sequência contínua de fatos ou operações que apresentam determinada unidade ou que se reproduzem com certa regularidade, que compartilha uma visão focada em componentes preventivos, repressivos, judiciais, de saúde e sociais (Silva Bispo; Binto, 2023).

De acordo com Lima (2021), é um processo sistêmico, pela necessidade da integração de um conjunto de conhecimentos e ferramentas estatais que devem interagir a mesma visão, compromissos e objetivos. Deve ser também otimizado, pois depende de decisões rápidas, medidas saneadoras e resultados imediatos.

Sendo a ordem pública um estado de serenidade, apaziguamento e tranquilidade pública, em consonância com as leis, os preceitos e os costumes que regulam a convivência em sociedade, a preservação deste direito do cidadão só será ampla se o conceito de segurança pública for aplicado. Isto implica uma disposição ideal dos elementos que nela interagem, de modo a permitir-lhe um funcionamento regular e estável, asseguratório da liberdade coletiva e individual.

A segurança pública não pode ser tratada apenas como medidas de vigilância e repressão, mas como um sistema integrado e otimizado envolvendo instrumento de prevenção, coação, justiça, defesa dos direitos, saúde e social. O processo de segurança pública se inicia pela prevenção e busca de peças de dano, no tratamento das causas e na (re)inclusão na sociedade do sujeito (Silva; Marques, 2019).

Segundo Damasceno *et al*., (2024), as taxas de criminalidade dos últimos anos revelam que Brasil se tornou um país mais violento em que a taxa de homicídios dolosos cresceu 7,8% entre 2022 e 2023, atingindo 24,3/100 mil habitantes. A taxa de estupro em 2022 alcançou 26,1 casos para cada 100 mil mulheres representando 50.617 casos de estupro em todo o país.

No contexto brasileiro, a responsabilidade pelos serviços internos de segurança pública é atribuída às unidades federativas, cada uma delas dispondo de forças policiais compostas por agentes civis e militares. Enquanto os militares exercem a função de policiamento ostensivo e repressão imediata

ao crime, os civis, atuando como polícia judiciária, realizam atividades de investigação. Assim como os demais serviços prestados pelo Estado, a segurança pública deve obedecer aos princípios constitucionais, entre eles o da eficiência, que pressupõe a prestação de serviços com qualidade e o uso racional dos recursos públicos. Além disso, a busca por eficiência na segurança pública contribui não apenas para a contenção do crime, mas também para a melhoria do ambiente social e econômico, ao mitigar os efeitos nocivos da criminalidade sobre pessoas e patrimônios.

No domínio da Segurança Pública, surgiram recentemente muitos novos desafios, tais como conflitos geopolíticos, ataques cibernéticos, terrorismo e o aumento da migração. Uma das tendências mais fortes é o aumento do *networking* e da cooperação entre as organizações relevantes, que só se intensificará no futuro.

De acordo com Lima e Barbosa (2020), o setor público é definido por cadeias de valor que gerem questões cada vez mais complexas e interligadas – como os cuidados de saúde, a imigração ou o sistema judicial. A tecnologia está a apoiar estas cadeias de valor na procura de maiores níveis de eficiência, mas devem ser implementadas estrategicamente para garantir que a segurança e a defesa sejam priorizadas. O autor reforça que as organizações de segurança pública devem investir no desenvolvimento de suas estratégias digitais e no aproveitamento de dados para otimizar processos e atender às necessidades da população. Santos (2023) aponta os principais desafios da segurança pública no Brasil incluem a ascensão da violência, criminalidade, crime organizado e desordem urbana, que levaram à militarização das atividades de segurança pública. Este processo de militarização aumentou nos últimos dois anos, com os militares ocupando posições de poder no governo brasileiro.

Chaves (2020) postula que o Brasil enfrenta o desafio de analisar grandes quantidades de dados para identificar fatores que influenciam a evolução dos crimes. Um modelo de tomada de decisão baseado na análise de big data é proposto para apoiar a identificação dos locais mais perigosos com base em correlacionar dados na localização e no número de crimes. Além disso, existem problemas de governança nas redes políticas de segurança pública brasileira, com fraca capacidade de governança devido às funções históricas das secretarias de segurança pública brasileiras.

2.3 Conceito de crimes cibernéticos e cibercrimes

O desenvolvimento da tecnologia de informação e comunicação torna a vida moderna mais conveniente. No entanto, o aumento dos crimes cibernéticos que exploram essa tecnologia emergiu como um problema social grave. Desde o início da pandemia de Covid-19, mais utilizadores da *internet* em todo o mundo tornaram-se dependentes da *internet* em todas as áreas, incluindo educação, transações financeiras e trabalho a partir de casa (Silva Bispo; Binto, 2023).

Crime cibernético é um termo geral que descreve uma infinidade de atividades criminosas realizadas por meio de um computador, rede ou outro conjunto de dispositivos digitais. Considere-se o crime cibernético como o guarda-chuva da vasta gama de atividades ilegais que os criminosos

cibernéticos cometem. Isso inclui ataques de *hacking*, *phishing*, roubo de identidade, *ransomware* e *malware*, entre muitos outros (Lima, 2023).

Os problemas na definição do crime cibernético começam pela própria terminologia como ilustra Corrêa *et al*., (2022). É utilizado um verdadeiro arsenal de terminologia, por vezes em combinação com os prefixos cibernético, computador, *e-mail*, *internet*, digital ou informação. Os termos são cogitados, aplicados aleatoriamente, refletem sobreposições de conteúdo ou refletem lacunas importantes.

Segundo Barros (2023), a terminologia alternativa para o cibercrime inclui, por exemplo, "crime no ciberespaço"; "crime virtual"; "crime relacionado com informática"; "crime eletrônico"; "crime eletrônico"; "crime possibilitado pela tecnologia"; "crime de alta tecnologia". A variabilidade nos termos e na linguagem do crime cibernético destaca a falta de um léxico partilhado entre os profissionais que trabalham na área.

Chaves (2020) destaca que o crime cibernético representa uma séria ameaça para indivíduos, empresas e entidades governamentais e pode resultar em perdas financeiras significativas, danos à reputação e comprometimento de registros. À medida que a tecnologia avança e mais pessoas dependem de dispositivos e redes digitais para operações padrão, a ameaça do crime cibernético continua a aumentar, tornando mais crítico do que nunca tomar medidas para se proteger contra ele.

Durante esta dependência, os danos causados pelos crimes cibernéticos aumentaram constantemente. Os crimes cibernéticos se referem não apenas a crimes *online*, mas também a novas formas de crimes baseadas no uso indevido de tecnologias recentemente desenvolvidas (Barroso; Silva, 2022).

Dado que a vida das pessoas existe no ciberespaço através de redes de informação e comunicação, a perpetração de crimes convencionais off-line também se movimentou *online*, agravando os casos e a gravidade dos crimes cibernéticos. O aumento destes novos tipos de crimes que exploram as tecnologias da informação e comunicação ultrapassou o desenvolvimento de medidas e legislação para os prevenir ou lidar. O anonimato do ambiente online também complicou a resposta ao crescimento da cibercriminalidade (Jesus; Silva, 2024).

2.4 Sobre os crimes cibernéticos ou cibercrimes (crimes virtuais)

Em 2020, a Polícia Federal relatou 791.790 casos de crimes cibernéticos, contra 300.000 em 2019. E, em uma amplitude maior, a estimativa é que os danos globais causados pelos crimes cibernéticos em 2015 atingiram 3 biliões de dólares e previu um aumento dos danos para 10,5 biliões de dólares em 2025 (Brasil, 2023).

Em 2020, a perseguição virtual e crimes semelhantes foram classificados como os crimes cibernéticos mais relatados no Brasil. Em comparação, a Coreia do Sul, conhecida como uma potência em tecnologia da informação, é um país atraente para os cibercriminosos. À medida que as tecnologias e serviços baseados na *internet* têm sido mais utilizados, o crime cibernético no país cresceu ainda mais. Em 2020, a

Coreia do Sul registrou um total de 234.098 casos de crimes cibernéticos, sendo a fraude na *internet* e a fraude financeira os mais proeminentes entre os crimes cibernéticos ocorridos (Barroso; Silva, 2022).

Segundo Chaves (2020), ao mesmo tempo, os danos causados por pirataria informática, roubo de identidade e assédio continuaram a aumentar. No *hacking*, os *cibercriminosos* obtêm acesso às informações dos usuários online, causando danos.

Em 2021, o governo coreano reprimiu intensamente o *hacking* e o DDoS. Como resultado, constatou-se que quatro em cada dez casos estavam relacionados ao crime de *hacking*, roubo de identidades e senhas.

O assédio *online* atinge pessoas independentemente da sua idade e é desenfreado devido ao anonimato facilmente disponível na *internet*. Esse assédio *online* e *cyberbullying* prejudicam ou ameaçam a reputação dos indivíduos através de mensagens, comentários ou mensagens diretas através de serviços de redes sociais.

O fácil vazamento de informações pessoais pelas redes sociais agrava os danos. Vários tipos de crimes cibernéticos que exploram ou infiltram sistemas de informação acontecem sem impedimentos e os seus danos tornam-se mais graves do que os crimes offline devido ao seu impacto e difusão.

A legislação e as medidas preventivas não conseguiram acompanhar os novos tipos de crimes que exploram as tecnologias da informação e comunicação. Pesquisas anteriores sobre crimes cibernéticos focaram principalmente nos fenômenos e suas causas, efeitos e prevenção. A maioria das pesquisas baseou-se na revisão da literatura e em análises de pesquisas baseadas em dados de percepção sobre crimes cibernéticos para determinar seus fatores criminais (Jesus; Silva, 2024).

Porém, para se chegar a medidas preventivas, Damasceno (2024) ressalta que é essencial analisar os crimes cibernéticos, especialmente porque e como as pessoas os cometem, com dados dos criminosos. Portanto, como um estudo exploratório, esta pesquisa visa examinar os crimes cibernéticos com duas questões de pesquisa: porque e como os criminosos cometem crimes cibernéticos e, em seguida, propor medidas preventivas.

A classificação dos crimes cibernéticos em três tipos, como tipos relacionados à integridade, relacionados ao computador e relacionados ao conteúdo, identificou os principais fatores criminais para cada tipo de crime cibernético que uma equipe de pesquisa, em estreita colaboração com uma organização policial de segurança cibernética, poderia usar para entrevistar policiais especializados em lidar com casos de crimes cibernéticos (Gomes; Medrado, 2023).

Barros (2023) assinala que o crime cibernético abrange um amplo espectro de atividades criminosas que envolvem diversas plataformas e tecnologias digitais. Vale a pena discutir muitos tipos de crimes cibernéticos, desde e-mails fraudulentos e atividades em mídias sociais até golpes financeiros e perseguição virtual (*stalk*), ataques virtuais, dentre outros.

Esquemas enganosos que assumem muitas formas. *E-mails* falsos enganam os destinatários, enquanto técnicas de engenharia social enganam as pessoas para que divulguem informações, como números de cartão de crédito, ou transfiram dinheiro para o invasor. Os esquemas de vendas piratas, nos quais os golpistas imitam marcas legítimas, são uma forma comum de golpes por e-mail. Golpes que usam plataformas de mídia social como *Facebook*, *Twitter*, *Instagram* e *TikTok* para enganar e fraudar as vítimas. Os exemplos incluem lojas online fictícias, ataques de engenharia social ou golpes de falsificação de identidade. As fraudes nas redes sociais muitas vezes exploram a confiança dos utilizadores, a ingenuidade e a tendência para partilhar excessivamente informações pessoais online (Jesus; Silva, 2024).

Araújo e Couto (2023) citam as atividades fraudulentas que visam instituições financeiras ou seus clientes e partes interessadas. As fraudes bancárias geralmente resultam em perdas financeiras significativas ou roubo de identidade, e as estratégias dos invasores geralmente envolvem táticas sofisticadas de *hacking* e engenharia social. Os exemplos incluem fraude de cartão de crédito, fraude em caixas eletrônicos e fraudes bancárias *online*.

Elaborar golpes ao consumidor que exploram os pontos fracos e as armadilhas das tecnologias de compras on-line, como lojas on-line artificiais ou fabricadas, contas de vendedores falsas ou roubo de informações de cartão de crédito. Os casos de fraude no comércio eletrônico normalmente resultam em perdas financeiras tanto para os consumidores quanto para os varejistas online (Barroso; Silva, 2022).

De acordo com Corrêa *et al.*, (2022), um ataque de software altamente prevalente, programado para danificar e manipular sistemas de computador, introduzindo vírus, trojans ou *spyware* no sistema. O *malware* é um problema frequente em muitos casos porque tem como alvo PCs individuais e redes de computadores de nível empresarial. É mais comumente usado para interromper redes e roubar dados de usuários. Um tipo de ataque de *malware* que criptografa dados críticos das vítimas e declara um pagamento de resgate em troca de uma chave de descriptografia para recuperar o acesso. Paralisantes financeiramente tanto para indivíduos quanto para organizações, os ataques de *ransomware* geralmente levam à perda de dados e ativos, à devastação fiscal e à interrupção da produtividade.

O uso de *hackers*, ataques de malware ou outras atividades cibernéticas nas quais um usuário não autorizado tenta acessar dados confidenciais ou propriedade intelectual para obter vantagem competitiva sobre uma empresa ou entidade governamental. Os casos de espionagem cibernética envolvem frequentemente grupos patrocinados pelo Estado ou *hackers* individuais e podem ter importantes implicações políticas ou econômicas. Um dos casos mais significativos de espionagem cibernética foram os cinco *hackers* militares chineses indiciados por pirataria informática, espionagem econômica e outros crimes dirigidos a entidades públicas e privadas (Chaves, 2020).

De acordo com Damasceno (2024), o acesso não autorizado ou vazamento de dados confidenciais, como informações confidenciais, registros críticos ou acesso financeiro. As violações de dados podem ser atribuídas a uma ampla gama de fatores de risco, como senhas e protocolos de segurança cibernética fracos, vulnerabilidades de sistemas de *software* ou ameaças internas. As consequências podem resultar em dados comprometidos, danos financeiros ou reputações manchadas.

O relatório de investigações de violação de dados do autor destacou que 82% das violações envolveram um elemento humano.

Talvez o tipo mais comum de *software* malicioso que pode se autorreplicar e se espalhar para outros sistemas, muitas vezes causando danos a arquivos ou programas de computador. Exemplos de vírus de computador se espalham rapidamente para infectar arquivos e danificar sistemas de computador. Ataques distribuídos de negação de serviço, ou ataques DDoS, são programados para sobrecarregar uma rede ou site com tráfego, fazendo com que ele fique lento ou trave totalmente (Silva Bispo; Binto, 2023).

De acordo com Araújo e Couto (2023), uma forma digital de roubo de propriedade intelectual que envolve o uso ou distribuição não autorizada de material protegido por direitos autorais, como *software*, música ou filmes. Exemplos de pirataria de software incluem o uso de geradores de chaves ou software crackeado para ativar software pago sem licença. Fraude por e-mail que envolve técnicas como e-mails enganosos, fraudes em sites ou comunicações enganosas para enganar as vítimas, levando-as a compartilhar suas informações pessoais e dados confidenciais ou a clicar em *links* para *downloads* e sites maliciosos.

Em um contexto digital, o roubo de identidade refere-se à aquisição de dados privados de alguém para fins fraudulentos ou maliciosos. Os ativos alvo do roubo de identidade incluem números de segurança social, data de nascimento, detalhes de cartão de crédito ou contas *online*. Tipos específicos incluem roubo de identidade financeira, médica e fiscal; personificação de mídia social; e clonagem de identidade, quando uma pessoa usa a identidade de outra para ocultar a sua (Jesus; Silva, 2024).

Tem-se ainda, aqueles crimes que envolvem *cyberbullying*, *cyberstalking* e atos repetidos com a intenção de assustar, prejudicar, irritar ou envergonhar um determinado indivíduo. Atualmente, o assédio *online* é mais prevalente em sites de mídia social, aplicativos de namoro e fóruns/quadros de mensagens. Exemplos de assédio online incluem o envio de mensagens inadequadas e não solicitadas, fazer ameaças claras e intencionais ou distribuir fotos ou vídeos confidenciais de uma vítima (Barbosa, 2020).

Chaves (2020) destaca o fenômeno do terrorismo virtual como uma modalidade de ação violenta realizada por meio da *internet* e de tecnologias informáticas, caracterizada pela sua natureza destrutiva e por seu elevado potencial de impacto. Esse tipo de terrorismo compreende ações como a sabotagem de infraestruturas críticas, a indução de falhas sistêmicas de grande escala, o roubo de informações sensíveis e a disseminação de conteúdos ideológicos com forte carga política ou cultural. Observa-se uma crescente sofisticação nos métodos empregados pelos agentes envolvidos em práticas de ciberterrorismo, o que impõe desafios cada vez mais complexos para os sistemas de segurança e defesa cibernética, exigindo respostas integradas e contínua atualização tecnológica e normativa.

2.5 Crimes cibernéticos no Brasil

O cibercrime está a tornar-se cada vez mais difundido e, no entanto, a falta de consenso em torno do que constitui um cibercrime tem um impacto significativo na sociedade, na resposta jurídica e

política e na investigação acadêmica. As dificuldades na compreensão do crime cibernético começam com a variabilidade na terminologia e a falta de consistência na legislação sobre crimes cibernéticos entre jurisdições (Portalés *et al*., 2022). Nos dizeres de Araújo e Couto (2023, p. 56):

> Os ataques cibernéticos representam riscos significativos à segurança e à privacidade das pessoas no Brasil. O roubo de contas foi identificado como o tipo mais comum de fraude digital, sendo responsável por 72% dos golpes no país em 2022. Isso significa que a cada minuto uma nova conta é perdida. Os fraudadores usam dados vazados, chips clonados e técnicas de engenharia social, como links e e-mails falsos, para obter informações de acesso das vítimas. Além do roubo de contas, outros riscos muito comuns incluem roubo de identidade, fraude financeira, invasão de privacidade e extorsão. Os golpes podem ocorrer em diferentes etapas, desde a criação de contas falsas até a realização de transações fraudulentas. [...] Um dos motivos pelos quais as pessoas ficam mais vulneráveis a golpes é a falta de conscientização sobre segurança da informação - o que pode, por exemplo, levá-las a expor dados sensíveis e cair em golpes com mais facilidade.

Pires e Ferreira (2023) assinalam que as leis que tratam de crimes virtuais no Brasil incluem a Lei Carolina Dieckmann (Lei nº 12.737/2012) que foi criada após o caso de violação de privacidade da atriz Carolina Dieckmann, essa lei tipifica crimes cibernéticos, especialmente invasão de dispositivos eletrônicos, como computadores e smartphones. Cita-se o Marco Civil da Internet (Lei nº 12.965/2014), mesmo não focando especificamente em crimes virtuais, estabelece princípios, garantias, direitos e deveres para o uso da *internet* no Brasil, o que impacta indiretamente em questões relacionadas à segurança cibernética.

No Código Penal Brasileiro se tem alguns crimes cibernéticos são punidos com base no Código Penal Brasileiro, como crimes contra a honra (calúnia, difamação e injúria), estelionato, fraudes, entre outros, quando cometidos por meio da *internet* ou dispositivos eletrônicos. Vale citar a Lei de Interceptação Telefônica (Lei nº 9.296/1996), pois, embora não seja específica para crimes virtuais, regula a interceptação de comunicações telefônicas e telemáticas, incluindo *e-mails* e mensagens de texto, o que pode ser relevante em investigações de crimes cibernéticos (De Jesus; Da Silva, 2024).

Chaves (2020) cita a Lei do Acesso à Informação (Lei nº 12.527/2011) que não se trata especificamente de crimes virtuais, mas regula o acesso a informações públicas, o que pode ser relevante em investigações relacionadas à segurança cibernética.

Araújo e Couto (2023) indicam que o Brasil enfrenta um cenário crítico de crimes cibernéticos, com um aumento alarmante no número de ataques cibernéticos contra pessoas e empresas. Uma grave falta de sensibilização para a segurança da informação, aliada ao baixo investimento na segurança cibernética, contribui para a vulnerabilidade do país a estas ameaças. Na visão de Pompeu (2021), a sensibilização é a melhor forma de combater a criminalidade cibernética e proteger as nossas informações e infraestruturas digitais. Somente por meio da conscientização e da união de esforços entre Estado, setor privado e sociedade é possível construir um ambiente digital mais seguro e resiliente para o Brasil.

2.6 Prevenção de crimes cibernéticos

De acordo com Damasceno (2024), uma das principais estratégias na prevenção do crime cibernético é a utilização de proteção avançada de segurança cibernética. Isto inclui tecnologias fundamentais como *firewalls*, *software* antivírus e sistemas de detecção de intrusões, mas sistemas de segurança cibernética mais avançados estão a evoluir com inteligência artificial (IA) e aprendizagem automática (AA). A implementação das ferramentas adequadas de cibersegurança deve ser uma prioridade máxima para qualquer organização ou indivíduo que pretenda proteger-se contra-ataques cibernéticos e ameaças digitais.

Araújo e Couto (2023) mencionam a autenticação multifatorial (AM), comumente usada como autenticação de dois fatores, é um protocolo de segurança comum que evita violações de dados, *hackers* e outros ataques cibernéticos diretos. Em termos simples, este processo exige que os usuários forneçam duas ou mais formas de identificação para autenticar o acesso às suas contas, como a necessidade de uma senha e um código de acesso enviado a um dispositivo. Atualmente um protocolo de práticas recomendadas para organizações, o AM adiciona camadas extras de segurança cibernética às contas online, tornando muito mais difícil para os invasores acessarem seus dados.

Segundo postulam Araújo e Couto (2023), uma Rede Privada Virtual (RPV) é um serviço que permite aos usuários navegar na *internet* com segurança reforçada e anonimato. As RPVs são projetadas para criptografar atividades *online*, tornando muito mais difícil para os invasores cibernéticos interceptarem e roubarem seus dados. As RPVs atuam como intermediárias entre o seu dispositivo e o servidor de destino, adicionando sua própria camada de criptografia e roteando a comunicação por meio de seus próprios servidores. As RPVs são especialmente eficazes para ajudar na proteção contra fraudes por *e-mail*, como golpes de *e-mails fakes*, mascarando seu endereço IP e localização.

Como reforçam Araújo e Couto (2023), as contas de *e-mail* são um dos canais mais frequentemente explorados pelos ciberataques para violar o acesso a dados confidenciais e informações privadas. Tecnologias especializadas de segurança de *e-mail* podem ser aproveitadas para evitar essa atividade, o que inclui soluções como criptografia de *e-mail*, filtros de *spam* e *software* antivírus. A criptografia é uma tecnologia poderosa que protege o conteúdo do *e-mail* contra interceptação. Os filtros de *spam* detectam e evitam que e-mails injustificados e maliciosos cheguem à sua caixa de entrada, enquanto o *software* antivírus detecta e remove anexos maliciosos de *e-mails*.

Os cibercriminosos atacam frequentemente credenciais de senha. Além de criar senhas seguras e difíceis de hackear, os gerenciadores de senhas são aplicativos de *software* que armazenam com segurança várias credenciais de login em um banco de dados criptografado, todas bloqueadas por uma senha mestra. Os gerenciadores de senhas são comumente usados por organizações, equipes remotas e indivíduos para fornecer proteção extra de segurança ao navegar na *web*, mantendo as senhas com segurança em um espaço seguro. Os gerenciadores de senhas mais comuns incluem: *Password*, *KeePass*, *LastPass* e *iCloud Keychain* da Apple. No entanto, alguns gerenciadores de senhas apresentam riscos (Portalés *et al.*, 2022). Muitos ataques cibernéticos resultam de erro humano, como clicar em *links*

maliciosos ou baixar arquivos contendo vírus. O treinamento de conscientização sobre segurança tem como objetivo ajudar a educar os usuários sobre como identificar, evitar e mitigar melhor a ameaça de ataques cibernéticos. As formas mais comuns de treinamento são treinamento de conscientização baseado em computador e exercícios simulados de *phishing*, onde os funcionários recebem *e-mails* de *phishing* falsos para testar como reagem (Pires; Ferreira, 2023).

Como explica Santana (2021), muitas formas de ataques cibernéticos podem resultar na perda de dados críticos, o que pode ter graves repercussões financeiras e operacionais para indivíduos e organizações. As soluções de *backup* e recuperação de dados podem ajudar a mitigar os danos causados pela perda de dados, criando cópias de *backup* dos dados e garantindo uma recuperação mais rápida no caso de um ataque de *ransomware*, violação de dados ou outra forma de ataque cibernético. O arquivamento regular de dados é um protocolo de segurança *essencial* para garantir que se possa recuperar seus dados em caso de ataque.

Em geral, pode-se dizer que tecnologias mais avançadas de prevenção de crimes cibernéticos agora utilizam aprendizado de máquina e inteligência artificial para coletar e analisar dados, rastrear e rastrear ameaças, identificar vulnerabilidades e responder a violações. Por exemplo, os algoritmos de ML podem detectar e prevenir fraudes em transações financeiras, identificando padrões que indicam atividades fraudulentas e sinalizando-os para revisão. Da mesma forma, as tecnologias de IA podem detectar e prevenir ataques cibernéticos a redes e sistemas, analisando o tráfego de rede, identificando padrões anormais e respondendo a ameaças em tempo real.

3. CONSIDERAÇÕES FINAIS

O presente estudo abordou os crimes cibernéticos no contexto da segurança pública. Buscou-se saber como as políticas públicas podem ser eficazmente desenvolvidas e implementadas para combater os crimes cibernéticos de forma abrangente e sustentável. Ao analisar as principais formas de crimes cibernéticos, avaliar políticas públicas existentes e propor novas estratégias, foi possível identificar um conjunto de recomendações que podem fortalecer a segurança digital e a proteção dos cidadãos.

Pode-se dizer que uma abordagem multifacetada é essencial. Políticas públicas eficazes devem incluir a cooperação internacional, dado o caráter transnacional dos crimes cibernéticos, bem como a colaboração entre governos, setor privado e sociedade civil. A implementação de marcos regulatórios robustos, aliados a programas de educação e conscientização, é fundamental para construir uma cultura de segurança cibernética.

Adicionalmente, o investimento em tecnologia avançada e infraestrutura de segurança é crucial. Governos devem fomentar a pesquisa e o desenvolvimento de novas tecnologias de defesa cibernética, além de garantir que as forças de segurança tenham os recursos necessários para enfrentar ameaças

complexas. Programas de treinamento e capacitação contínua para profissionais de segurança cibernética também são essenciais para acompanhar a rápida evolução das técnicas de ataque cibernético.

Conclui-se que políticas públicas devem ser adaptáveis e dinâmicas, capazes de responder rapidamente às novas ameaças e vulnerabilidades. A criação de centros de resposta a incidentes cibernéticos e a promoção de um ambiente legal que incentive a denúncia de crimes cibernéticos podem melhorar significativamente a resiliência cibernética. Para que as políticas públicas sejam eficazes no combate aos crimes cibernéticos de maneira abrangente e sustentável, é necessário um esforço coordenado, inovador e contínuo.

A implementação das estratégias propostas neste estudo pode contribuir significativamente para um ambiente digital mais seguro, beneficiando não apenas a segurança dos indivíduos, mas também a integridade das infraestruturas críticas e o desenvolvimento socioeconômico. Portanto, a formulação de políticas públicas robustas e eficazes é um passo essencial para enfrentar os desafios apresentados pelos crimes cibernéticos na era digital.

Como sugestão para estudos futuros, pode-se realizar uma investigação aprofundada das políticas de cooperação internacional e suas efetividades na mitigação de ameaças transnacionais. Além disso, é possível explorar o impacto das novas tecnologias emergentes, como inteligência artificial e *blockchain*, na prevenção e detecção de crimes cibernéticos. Análises comparativas de modelos de governança cibernética em diferentes países e a avaliação da eficácia de campanhas educativas e de conscientização pública também são áreas promissoras.

REFERÊNCIAS

ARAUJO, Karolaine Rayala Balsanulfo; COUTO, Stephani Reis Oliveira. **Investigação e atualização:** abordando a complexidade dos crimes cibernéticos na sociedade moderna, 2023. Artigo Científico (Curso de Direito), Faculdade Evangélica de Goianésia, Goianésia, 2023.

BARBOSA, Mateus Israel Alves Crivinel. **Crimes virtuais:** a evolução dos crimes cibernéticos e os desafios no combate, 2020. Artigo Científico (Curso de Direito), Escola de Direito e Relações Internacionais, Pontifícia Universidade Católica de Goiás, Goiânia, 2020.

BARROS, Bruno Pereira. **Crimes cibernéticos:** dificuldade para obter indícios de autoria e materialidade, 2023. Artigo Científico (Curso de Direito) Escola de Direito, Negócios e Comunicação, Pontifícia Universidade Católica de Goiás, Goiânia, 2023.

BARROSO, Sinak Rháyner Vieira da Cunha Fernandes; SILVA, Valdirene Cássia da. **Os crimes cibernéticos e os desafios enfrentados no processo investigatório**, 2022. Artigo Científico (Curso de Direito) Centro Universitário Católico do Tocantins, 2022.

CHAVES, Sarah Rodrigues. **Crimes cibernéticos:** questionamentos acerca da vulnerabilidade nos crimes virtuais sexuais, 2020. Artigo Científico (Curso de Direito) Escola de Direito, Negócios e Comunicação, Pontifícia Universidade Católica de Goiás, Goiânia, 2020.

CORRÊA, Luciana *et al*. Balanço dos principais crimes cibernéticos ocorridos no município de Belém/PA no período de 2018 a 2020. **Research, Society and Development**, v. 11, n. 1, p. e43411125214-e43411125214, 2022.

DAMASCENO, Ailson Fernandes *et al*. Resenha do artigo intitulado "Os crimes cibernéticos e o direito à segurança jurídica: uma análise da legislação vigente no cenário brasileiro contemporâneo". **Revista Processus Multidisciplinar**, v. 5, n. 9, p. e091084-e091084, 2024.

FREITAS, Camila Cristina Gonzaga; GONÇALVES, Jonas Rodrigo; TORRES, Mateus Guimarães. A evolução do direito penal brasileiro relacionado aos crimes cibernéticos. **Revista JRG de Estudos Acadêmicos**, v. 6, n. 12, p. 296-311, 2023.

GOMES, Walyson Milhomem de Sousa; MEDRADO, Lucas Cavalcante. Crimes cibernéticos uma ponderação sobre a Lei 14.155 de 2021 aplicável ao crime de estelionato virtual. **Revista Ibero-Americana de Humanidades, Ciências e Educação**, *[S. l.]*, v. 9, n. 9, p. 1870–1894, 2023. DOI: 10.51891/rease.v9i9.11321.

JESUS, Brenda Cordeiro de; SILVA, Devanildo Braz da. Crimes cibernéticos: desafios da segurança pública e seu enfrentamento. In.: NOGUEIRA, Fernando Lopes; SILVA, Devanildo Braz da; FÉLIX, Ynes da Silva (Org.). **Gestão em segurança pública**. Campo Grande: Ed. UFMS, 2023. p. 165-226.

LIMA, Edenilson Machado. **O anônimato nos crimes cibernéticos e a ocultação delitiva**, 2021. Trabalho de Conclusão de Curso (Curso de Direito). Centro Universitário Luterano de Palmas, Palmas, 2021.

LIMA, Manoel Guilherme dos Santos de Castro; BARBOSA, João Batista Machado. **Crimes virtuais:** uma análise sobre as dificuldades do estado na persecução penal, 2020. Artigo Científico (Curso de Direito). Centro Universitário do Rio Grande do Norte, Natal, 2020.

OLIVEIRA, Bruna Larissa Campos; ALMEIDA, Andréia Alves. Modernização dos Crimes Sexting e Revenge Porn: No ambiente virtual contra a mulher. **Revista Ibero-Americana de Humanidades**, Ciências e Educação, v. 8, n. 1, p. 263-270, 2022.

PIRES, Andrielle Horaine Rodrigues; FERREIRA, Thais dos Santos. **Crimes cibernéticos:** suas principais vítimas. 2023.

POMPEU, Ana Luiza Brandão Calil. **Crimes Cibernéticos:** A ineficácia da Lei Carolina Dieckmann. 2022.

PORTALÉS, Leticia Fontestad et al. Polícia preditiva e "negritude": modelos para a reprodução de um estado sem direitos. **Revista Direito**. UnB. setembro-dezembro, v. 6, n. 3, p. 2357-8009, 2022.

SANTANA, Roque Felipe da Silva; SILVA, Mônica Antonieta M. da. Crimes cibernéticos: análise evolutiva da legislação penal brasileira e seus desafios, 2021. Artigo Científico (Curso de Direito). Universidade Católica do Salvador, Salvador, 2021.

SANTOS, Letícia Dutra de Oliveira. **Políticas públicas de educação digital:** prevenção e combate aos crimes cibernéticos, 2020. Monografia (Curso de Direito). UniEvangélica, Anápolis, 2020.

SILVA BISPO, Adrielle; BINTO, Emanuel Vieira. Crimes cibernéticos: da ineficácia da Lei Carolina Dieckmann na prática de crimes virtuais. **Revista Ibero-Americana de Humanidades, Ciências e Educação**, v. 9, n. 11, p. 354-369, 2023.

SILVA, Kaique Rodrigues; SILVA, Rubens Alves. Crimes cibernéticos: necessidade de novas ferramentas de investigação com encargos no ônus da prova. **Revista Artigos**. Com, v. 12, p. e2480-e2480, 2019.

SILVA, Rafael; MARQUES, Daniel. Crimes cibernéticos e sua competência. **Eticencontro de Iniciação Científica**-ISSN 21-76-8498, v. 15, n. 15, 2019.