Revista Ibero-Americana de Humanidades, Ciências e Educação — REASE

OPEN ACCESS

doi.org/10.51891/rease.v11i6.19733

CRIMES CIBERNÉTICOS COMETIDOS CONTRA O PATRIMÔNIO PÚBLICO ENTRE 2019 E 2024 EM PALMAS-TO

Brand Rodrigues Cardoso Dias[1]
Maria Eduarda Evangelista Nascimento[2]
Pedro Victor Sousa de Freitas[3]
Fabiana Luiza Silva Tavares[4]

RESUMO: O presente trabalho tem por objetivo evidenciar os crimes cibernéticos, mais especificamente, dos acometidos contra o patrimônio público do Município de Palmas (TO), dentre o período de 2019 e 2024, com foco no estelionato eletrônico, ransomware e uso indevido de sistemas institucionais. Nesse hiato, a pesquisa avalia os impactos econômicos e sociais dos referidos delitos e analisa as estratégias de combate adotadas pelos órgãos públicos. Desse modo, utilizou-se da metodologia de pesquisa mista, para fins de coleta de dados e elaboração do presente artigo.

Palavras-chave: Cibersegurança. Crimes cibernéticos. Palmas-TO. Patrimônio público. *Ransomware*.

ABSTRACT: This paper aims to highlight cybercrimes, specifically those committed against the public assets of the municipality of Palmas (TO), between the years 2019 and 2024, focusing on electronic fraud, ransomware, and the misuse of institutional systems. During this period, the research evaluates the economic and social impacts of these crimes and analyzes the countermeasures adopted by public agencies. Thus, a mixed research methodology was employed for data collection and the development of this article.

Keywords: Cybercrimes. Cybersecurity. Palmas-TO. Public assets. *Ransomware*.

1. INTRODUÇÃO

É fato que, a evolução digital trajou diversos benefícios sociais, do mesmo modo, esse avanço estendeu-se para a Administração Pública, na oferta de serviços e na ampliação do acesso da população às políticas públicas. Muito se discute sobre as vantagens do desenvolvimento tecnológico, contudo, esse progresso também revelou vulnerabilidades estruturais e operacionais do sistema público, que vêm sendo sistematicamente exploradas por

[1]Graduando em Direito, Uninassau Palmas.
[2]Graduanda em Direito, Uninassau Palmas.
[3]Graduando em Direito, Uninassau Palmas.
[4]Mestre em direito e políticas públicas pelo Uniceub. Pós-graduada em direito penal e processo penal. Docência do Ensino Superior pela Unitins. Graduada em direito pela Unirg antiga Fafich de Gurupi 2005. Atualmente Professora na Uninassau, Palmas.

criminosos cibernéticos, resultando em ataques que comprometem a integridade, a disponibilidade e a confidencialidade de informações sensíveis e impactam diretamente o funcionamento da máquina pública.

Mormente, no Município de Palmas, capital do Tocantins, observou-se que entre o período de 2019 e 2024 houve um crescimento exponencial da prática de crimes cibernéticos direcionados ao patrimônio público. Dados extraídos da Secretaria da Segurança Pública do Tocantins (SSP-TO) indicam que, nesse período, foram registrados mais de 20 mil Boletins de Ocorrências relacionados a crimes cibernéticos, com destaque para o estelionato eletrônico, que representa aproximadamente 70% das investigações. O estelionato eletrônico, inclusive, destaca-se como o delito mais recorrente, refletindo uma tendência que também se manifesta em âmbito nacional, onde foram registrados mais de 235 mil casos em 2023, um aumento de 13% em relação ao ano anterior.

A sofisticação dessas práticas ficou evidente em operações como a "*Lost Line*", que desarticulou organizações criminosas altamente especializadas em fraudes virtuais, muitas das quais utilizavam métodos avançados como engenharia social, *phishing* e *ransomware*. Tais fatos indicam não apenas o alcance dessas atividades ilícitas, mas também a capacidade adaptativa dos criminosos diante das respostas estatais.

Além da análise da evolução e das tipologias mais frequentes — como crimes contra a honra, contra o patrimônio e contra a segurança dos sistemas — o trabalho também se dedica a avaliar os impactos econômicos (como o desvio de recursos e a paralisação de serviços essenciais) e os impactos sociais, especialmente a erosão da confiança pública nas instituições governamentais e o aumento da percepção de insegurança digital.

Com base no diagnóstico elaborado, propõem-se medidas estruturantes, tais como: o fortalecimento das políticas públicas de segurança cibernética, a adoção de tecnologias avançadas de monitoramento e detecção de ameaças, e a promoção de uma cultura institucional voltada à educação e conscientização cibernética, tanto entre os servidores públicos quanto entre a população em geral.

A pesquisa também destaca que, apesar de esforços já realizados, como a instalação de *firewalls* e a realização de treinamentos básicos, tais ações ainda são insuficientes diante do volume e da complexidade dos ataques. A carência de uma governança cibernética mais robusta e de protocolos claros de resposta a incidentes impede que os órgãos públicos na cidade de Palmas-TO atuem de forma proativa e eficaz frente às ameaças digitais.

Diante disso, conclui-se que o enfrentamento dos crimes cibernéticos no contexto do patrimônio público de Palmas-TO requer não apenas investimentos tecnológicos, mas, sobretudo, o desenvolvimento de uma estratégia integrada, baseada em educação permanente, fortalecimento institucional e cooperação intersetorial. O fortalecimento da Divisão de Repressão a Crimes Cibernéticos, aliado a políticas públicas específicas e à maior participação social, representa o caminho mais promissor para a mitigação dos riscos futuros e para a construção de uma gestão pública digital segura, eficiente e confiável.

1.1 ASPECTOS HISTÓRICOS E CONCEITOS DOS CRIMES CIBERNÉTICOS

O advento da internet e sua rápida expansão a partir da segunda metade do século XX provocaram transformações significativas na sociedade, especialmente no que diz respeito à forma de comunicação, acesso à informação e interação social. Contudo, juntamente com os avanços tecnológicos, surgiram também novos tipos de condutas criminosas, conhecidas como crimes cibernéticos, que representam um dos maiores desafios da atualidade no campo da segurança e da informação.

Historicamente, a origem da internet remonta à década de 1960, quando foi criada a ARPANET (*Advanced Research Projects Agency Network*) pelo Departamento de Defesa dos Estados Unidos, com o objetivo de garantir a comunicação segura entre instituições militares e acadêmicas. A consolidação dos protocolos de comunicação TCP/IP, na década de 1980, possibilitou a expansão da rede para outros centros de pesquisa, culminando, nos anos 1990, na abertura da internet ao público em geral. A popularização da *World Wide Web*, juntamente com o desenvolvimento dos Navegadores gráficos marcaram o início de uma era de hiperconectividade, com impactos significativos nas esferas econômica, política e social. Com a vasta ampliação do uso da internet, surgiram vulnerabilidades que passaram a ser exploradas por indivíduos e grupos organizados, o que resultou no surgimento de práticas criminosas digitais. Os primeiros registros de crimes cibernéticos ocorreram ainda nas décadas de 1980 e 1990, envolvendo invasões a sistemas computacionais, disseminação de vírus e fraudes financeiras. Ao longo dos anos 2000, observou-se a sofisticação desses delitos, com a proliferação de ataques por meio de *malwares, phishing, ransomware* e o uso de botnets para comprometimento em larga escala de sistemas.

Conceitualmente, os crimes cibernéticos são definidos como infrações penais cometidas por meio de tecnologias digitais, com o uso de computadores, redes de internet ou outros

dispositivos eletrônicos. Esses crimes podem ser classificados em duas categorias principais: os crimes cibernéticos próprios, que só existem devido à existência do ciberespaço, como é o caso da invasão de sistemas e sequestro de dados; e os crimes cibernéticos impróprios, que consistem na adaptação de delitos tradicionais ao meio digital, como o estelionato, a ameaça e a difamação virtual (SILVA, 2021).

A partir de 2010, os crimes cibernéticos passaram a atingir não apenas pessoas físicas e empresas privadas, mas também instituições públicas e infraestruturas críticas, como sistemas de saúde, energia, segurança pública e administração financeira. Nesse contexto, os crimes contra o patrimônio público tornaram-se recorrentes, principalmente com o uso de técnicas sofisticadas de invasão, fraudes em processos licitatórios digitais e desvio de verbas por meio de manipulação de sistemas.

A crescente ameaça da criminalidade digital impulsionou a formulação de marcos regulatórios específicos no Brasil, como a Lei nº 12.737/2012, conhecida como Lei Carolina Dieckmann, que tipificou crimes informáticos, e a Lei nº 13.709/2018, que instituiu a Lei Geral de Proteção de Dados Pessoais (LGPD). Além disso, o Marco Civil da Internet (Lei nº 12.965/2014) estabelece princípios, garantias, direitos e deveres para o uso da internet no país, incluindo disposições sobre segurança, privacidade e responsabilização.

No contexto brasileiro, destaca-se ainda a atuação de órgãos especializados, como a Polícia Federal e as Delegacias de Repressão a Crimes Cibernéticos nos estados, que vêm enfrentando um aumento expressivo nos registros de ocorrências. Em Palmas-TO, observou-se que, entre os anos de 2019 e 2024 houve um crescimento significativo de ataques cibernéticos direcionados ao setor público, com impactos diretos sobre o erário, a integridade dos sistemas institucionais e a confiança da população na administração pública. Diante desse cenário, torna-se essencial compreender os aspectos históricos e conceituais dos crimes cibernéticos, não apenas para analisar sua evolução e complexidade, mas também para subsidiar políticas públicas de prevenção, investigação e repressão, especialmente em nível municipal e regional.

2. CONCEITO DE CRIMES CIBERNÉTICOS

O avanço tecnológico da informação e comunicação, mediante a facilidade de acesso a internet, surgiram novas modalidades de condutas ilícitas, conhecidas como crimes cibernéticos. Esses delitos se caracterizam pelo uso de sistemas informáticos como meio ou fim da prática criminosa.

Teixeira (2023) conceitua o crime de informática como aquele que utiliza sistemas informáticos como instrumento para alcançar um determinado resultado, bem como aquele praticado contra esses sistemas e meios. Essa definição inclui tanto os crimes que têm como alvo os sistemas computacionais quanto aqueles que os utilizam como meio para a prática delitiva.

De forma semelhante, Rossini (2004) propõe uma definição ampla, considerando o delito informático como qualquer conduta típica e ilícita, seja ela dolosa ou culposa, comissiva ou omissiva, realizada por pessoa física ou jurídica, com o uso da informática, em ambiente de rede ou fora dele. Além disso, destaca que tais condutas atentam contra a segurança informática, a qual envolve aspectos como integridade, disponibilidade e confidencialidade. Assim, evidencia-se que os crimes informáticos não se restringem ao ambiente virtual, podendo ocorrer em qualquer contexto que envolva sistemas informáticos.

Para Feliciano (2000), os crimes cibernéticos representam um fenômeno histórico-sociocultural recente, caracterizado pela elevada incidência de ilícitos penais que têm como objeto material ou meio de execução os componentes tecnológicos informáticos, como *hardware*, *software* e redes. Dessa forma, a abordagem do autor ressalta a estreita relação entre o desenvolvimento tecnológico e o surgimento de novas formas de criminalidade.

A Organização para a Cooperação e Desenvolvimento Econômico (OCDE, 1986) também contribui para a definição, entendendo o crime de informática como qualquer conduta ilegal, não ética ou não autorizada que envolva o processamento automático de dados e/ou a transmissão de dados. Essa concepção amplia o alcance do conceito, incluindo não apenas ações ilegais, mas também comportamentos não autorizados ou antiéticos. Além disso, Redivo (2022) destaca que os crimes cibernéticos consistem em atividades ilegais realizadas por meios eletrônicos digitais, utilizando a internet e diversos dispositivos como celulares, *notebooks*, computadores, entre outros. Essa conceituação evidencia a diversidade de dispositivos empregados e a abrangência das atividades ilícitas no ambiente digital.

Diante dessas definições, é possível perceber que os crimes cibernéticos englobam uma variedade de condutas ilícitas que envolvem o uso de tecnologias informáticas, seja como meio de execução ou como alvo da ação criminosa. A compreensão desses conceitos é fundamental para o desenvolvimento de políticas públicas eficazes no combate a essas infrações.

2.1 LEGISLAÇÃO SOBRE CRIMES CIBERNÉTICOS NO BRASIL

Com o avanço das tecnologias da informação e comunicação, o Brasil passou a enfrentar novos desafios na esfera penal, demandando atualizações legislativas para combater a criminalidade no ambiente digital.

Diversas normas foram elaboradas ou adaptadas para tratar dos chamados crimes cibernéticos, que envolvem a utilização de sistemas informáticos como meio ou fim da atividade criminosa.

A legislação brasileira avançou significativamente nesse campo, especialmente com a promulgação da Lei nº 12.737, de 30 de novembro de 2012, conhecida como Lei Carolina Dieckmann. Esse diploma legal alterou o Código Penal ao tipificar, pela primeira vez, a invasão de dispositivos informáticos, preenchendo uma lacuna existente até então no ordenamento jurídico.

A Lei nº 12.737, surgiu após um caso amplamente divulgado, no qual a atriz Carolina Dieckmann teve fotos pessoais acessadas e divulgadas indevidamente após a invasão de seu computador. O episódio evidenciou a necessidade de atualizar a legislação diante das novas formas de violação de direitos na internet.

Como resultado, o artigo 154-A foi incluído no Código Penal, prevendo sanções para quem invadir dispositivos informáticos alheios com o objetivo de obter, adulterar ou destruir dados, ou ainda instalar *softwares* maliciosos. O dispositivo legal estabelece que invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com a finalidade de obter, adulterar ou destruir dados ou informações sem autorização do titular, ou instalar vulnerabilidades para obter vantagem ilícita, sujeita o infrator à pena de detenção de três meses a um ano, além de multa (BRASIL, 2012).

> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo, ou instalar vulnerabilidades para obter vantagem ilícita: Pena: detenção de 3 (três) meses a 1 (um) ano, e multa." (BRASIL, 2012).

Assim, observa-se que a legislação brasileira vem se modernizando para enfrentar os desafios impostos pela criminalidade digital. Contudo, considerando a constante evolução das tecnologias e das estratégias utilizadas por criminosos no ambiente virtual, é essencial que o processo legislativo permaneça dinâmico e responsivo. Além disso, faz-se necessário investir

na capacitação contínua dos órgãos de segurança pública, do Judiciário e dos operadores do Direito, a fim de garantir a efetividade da aplicação dessas normas no combate aos crimes cibernéticos e na proteção dos direitos fundamentais dos cidadãos na esfera digital.

2.2 A FRAGILIDADE DA INFRAESTRUTURA DIGITAL E O CRESCIMENTO DOS CRIMES CIBERNÉTICOS CONTRA O PATRIMÔNIO PÚBLICO

A crescente digitalização dos serviços públicos tem proporcionado ganhos em eficiência, acessibilidade e transparência. No entanto, esse avanço também expõe fragilidades estruturais que tornam os sistemas governamentais alvos cada vez mais frequentes de crimes cibernéticos. A limitação de investimentos em segurança da informação, aliada à obsolescência de muitos sistemas, favorece a atuação de agentes mal-intencionados, capazes de acessar dados sensíveis, paralisar serviços essenciais e desviar recursos financeiros por meio de métodos tecnológicos sofisticados.

Entre as práticas criminosas mais recorrentes contra o patrimônio público destacam-se os ataques de *ransomware*, fraudes por *phishing*, engenharia social e invasões a sistemas operacionais. Esses ataques objetivam, em geral, obter acesso indevido a informações sigilosas, fraudar pagamentos ou comprometer o funcionamento de serviços públicos estratégicos, como saúde, educação e transporte. As fraudes financeiras, por exemplo, envolvem desde a falsificação de registros digitais até a realização de transferências indevidas, comprometendo recursos que deveriam ser destinados ao interesse coletivo.

Em Palmas, capital do Tocantins, o aumento dessas ocorrências tem sido expressivo. De acordo com dados do Painel de Estatísticas Criminais da Secretaria da Segurança Pública do Estado (SSP-TO), os crimes cibernéticos classificados como estelionato eletrônico aumentaram de 227 ocorrências em 2019 para 1.368 em 2023, representando um aumento de mais de 500% em cinco anos. Somente no primeiro semestre de 2024, já haviam sido registrados 709 casos, o que indica a continuidade da tendência de crescimento desses crimes na esfera digital.

Informações levantadas pela Divisão Especializada de Repressão a Crimes Cibernéticos (DRCC) revelam que muitas dessas infrações envolvem o uso de credenciais institucionais obtidas de forma ilícita, como contas de e-mail corporativas de servidores públicos, além da inserção de dados falsos em sistemas de folha de pagamento e uso indevido de plataformas digitais de gestão pública. Em casos mais graves, houve a paralisação de serviços municipais de

saúde e educação devido à instalação de *malwares* e à execução de ataques de *ransomware*, nos quais os criminosos exigiram resgate em criptomoedas para liberar os sistemas sequestrados.

A complexidade desses crimes é acentuada pelo uso de tecnologias que dificultam a identificação dos autores, como VPNs, navegadores anônimos, criptografia de ponta a ponta e ferramentas de *spoofing*. As técnicas utilizadas demonstram não apenas a sofisticação das ações criminosas, mas também as deficiências nas medidas de proteção adotadas por órgãos públicos locais, o que torna o setor público altamente vulnerável à atuação de quadrilhas especializadas.

3. TIPOS DE CRIMES CIBERNÉTICOS

As tipologias dos crimes cibernéticos são diversas e evoluem constantemente, sendo essenciais para um enfrentamento eficaz. Podem ser classificadas conforme os bens jurídicos tutelados e os métodos utilizados:

Crimes contra a honra: previstos nos artigos 138 a 140 do Código Penal, abrange calúnia, difamação e injúria praticadas por meios eletrônicos, especialmente em redes sociais, onde a disseminação de conteúdos ofensivos ocorre em larga escala, prejudicando a honra e a imagem de pessoas e instituições.

Crimes contra o patrimônio: incluem o furto mediante fraude (art. 155, §4º-B) e o estelionato (art. 171), ambos na modalidade eletrônica, como fraudes financeiras, clonagem de cartões e ataques de *ransomware*. Na cidade de Palmas-TO, os registros de estelionato eletrônico cresceram de 227 casos em 2019 para 1.368 em 2023, com 709 ocorrências no primeiro semestre de 2024, conforme dados da SSP-TO, demonstrando o avanço dessas práticas.

Crimes contra a segurança dos sistemas informáticos: envolvem a invasão de dispositivo informático (art. 154-A), disseminação de malwares, espionagem cibernética e sabotagem de infraestruturas críticas. Em Palmas/TO, há registros de tentativas de invasão a sistemas públicos, principalmente nas áreas de saúde e educação, muitas vezes utilizando engenharia social para obter acessos indevidos.

Essas tipologias evidenciam a complexidade dos crimes cibernéticos e seus impactos, especialmente na administração pública, cuja dependência de sistemas informatizados torna os danos ainda mais significativos. Assim, a compreensão dessas condutas é essencial para a formulação de políticas públicas e estratégias de prevenção e resposta adequadas às ameaças digitais enfrentadas por municípios como a cidade de Palmas-TO.

3.1 DESAFIOS NA INVESTIGAÇÃO DE CRIMES CIBERNÉTICOS

As tipologias de crimes cibernéticos são vastas, dinâmicas e em constante evolução, sendo essencial compreendê-las para a formulação de estratégias eficazes de enfrentamento. Segundo Bomfati (2020), uma classificação funcional pode ser construída com base nos alvos e métodos utilizados pelos agentes, dividindo os crimes em três grandes categorias: Crimes contra a honra: incluem calúnia, difamação e injúria praticadas em meios digitais, especialmente por meio de redes sociais. Esses crimes, embora muitas vezes não envolvam diretamente o patrimônio público, têm efeitos significativos sobre a reputação de servidores e instituições, podendo gerar crises administrativas e desinformação.

Na cidade de Palmas-TO, houve registros de ataques coordenados a gestores públicos, com divulgação de dados pessoais e manipulação de imagens, o que demonstra a necessidade de ações de proteção digital da imagem institucional. Crimes contra o patrimônio: representam a esmagadora maioria dos crimes cibernéticos investigados pela Delegacia de Repressão a Crimes Cibernéticos (DRCC) em Palmas. Entre 2019 e 2024, os registros de Boletins de Ocorrência cresceram de forma expressiva, como demonstrado a seguir:

BO´s Registrados	Inquéritos	Prisões em flagrante
1.049	30	0
1.015	114	2
2.847	177	1
4.408	152	0
3.854	127	0
3.911	53	1

Dados referentes ao período de 01/01 a 12/2024.

A análise desses números revela não apenas o aumento contínuo da criminalidade digital, mas também a sobrecarga investigativa das autoridades, que enfrentam dificuldades operacionais para transformar a maioria dos BOs em inquéritos aprofundados. Ainda mais relevante é a constatação de que cerca de 70% das investigações estão relacionadas a estelionatos digitais, muitas vezes aplicados contra órgãos públicos, servidores ou recursos vinculados à administração. Outros 15% envolvem fraudes eletrônicas, como manipulação de sistemas e boletos falsos; 3% correspondem a furto mediante fraude; e 12% se distribuem entre outros tipos de delitos digitais.

Casos registrados na cidade de Palmas demonstram, por exemplo, o uso de perfis falsos de secretarias municipais para aplicar golpes via PIX, a emissão de boletos bancários adulterados com o logotipo da prefeitura e a utilização de e-mails institucionais de servidores para enganar fornecedores ou desviar recursos. Essas práticas configuram ataques patrimoniais sofisticados, geralmente articulados por grupos especializados, que exploram falhas em sistemas de segurança, engenharia social e tecnologias de anonimização.

Crimes contra a segurança dos sistemas: envolvem invasões, disseminação de *malwares*, espionagem digital e sabotagem de infraestruturas críticas. Em Palmas-TO, ainda que em menor número, ocorreram casos de *ransomware* com bloqueio de sistemas da saúde e da educação, e tentativas de acesso indevido a bancos de dados estratégicos da administração. Esses ataques, mesmo quando frustrados, revelam a fragilidade de setores essenciais e o risco potencial de comprometimento institucional em larga escala.

Essas três categorias demonstram como os crimes cibernéticos podem ter consequências diretas sobre a governança, o orçamento público e a confiança dos cidadãos nas instituições. Em um cenário onde os Boletins de Ocorrência ultrapassam 4 mil registros anuais e os índices de estelionato digital dominam o perfil das investigações, torna-se imprescindível fortalecer as defesas institucionais por meio de políticas públicas, capacitação de servidores e investimentos contínuos em infraestrutura cibernética.

Além disso, a compreensão detalhada das tipologias é fundamental para que o poder público possa não apenas reagir aos ataques, mas antecipar-se a eles, monitorando vulnerabilidades, desenvolvendo protocolos de resposta e fortalecendo a cooperação entre os setores de tecnologia, jurídico e segurança institucional. Na cidade de Palmas-TO, os números confirmam que a criminalidade digital é uma realidade concreta e crescente e enfrentá-la exige uma abordagem articulada, preventiva e estratégica.

3.2 IMPACTOS ECONÔMICOS E SOCIAIS NO SETOR PÚBLICO

Os crimes cibernéticos direcionados ao patrimônio público têm consequências profundas e de longo alcance, tanto no aspecto econômico quanto no social. No plano financeiro, o desvio de recursos públicos por meio de fraudes eletrônicas, a interrupção de serviços causadas por ataques a sistemas operacionais e os custos com a recuperação de dados comprometem seriamente o orçamento da administração. Recursos que deveriam ser aplicados

em áreas essenciais como: saúde, educação e infraestrutura, que acabam direcionados para medidas emergenciais de contenção e restauração de sistemas atacados.

Na cidade de Palmas-TO, os efeitos desse tipo de crime têm sido cada vez mais evidentes. Segundo dados oficiais da Delegacia de Repressão a Crimes Cibernéticos (DRCC), a capital registrou um total de 20.400 Boletins de Ocorrência relacionados a crimes cibernéticos entre 2019 e 2024. O ano com maior incidência foi 2022, com 4.408 registros, seguido por 2024 com 3.911 e 2023 com 3.854. O que indica a manutenção da tendência ascendente. No mesmo período, foram instaurados mais de 668 inquéritos policiais, e ao menos quatro prisões em flagrante foram efetuadas, um número que, embora aparentemente baixo, revela a complexidade da investigação e da responsabilização nesse tipo de delito.

A maioria dessas ocorrências está ligada a crimes contra o patrimônio, com estelionatos representando cerca de 70% dos casos investigados, seguidos por fraudes eletrônicas (15%), furtos mediante fraude (3%) e outros crimes diversos (12%). Isso demonstra que as perdas para o erário público vão além dos valores diretamente desviados: incluem também os gastos com a contratação de serviços técnicos emergenciais, o reforço de sistemas de segurança digital e os prejuízos indiretos decorrentes da paralisação de serviços.

Socialmente, os impactos são igualmente graves. Crimes cibernéticos que comprometem serviços públicos essenciais geram transtornos à população e minam a confiança dos cidadãos nas instituições governamentais. Quando sistemas da saúde, educação ou assistência social são alvos de ataques, o prejuízo vai além do digital: atinge a prestação de direitos básicos e gera sensação de vulnerabilidade entre os usuários desses serviços.

Outro fator crítico é o roubo e a exposição de dados sensíveis, como informações pessoais de servidores, prontuários médicos, dados financeiros e cadastros de beneficiários de programas sociais. A circulação indevida dessas informações amplia o risco de fraudes secundárias, como golpes por telefone e uso indevido de identidade para abrir contas, solicitar empréstimos ou acessar sistemas públicos em nome de terceiros.

Na cidade de Palmas-TO, alguns dos ataques cibernéticos identificados

resultaram na falsificação de boletos bancários, fraudes via PIX em nome da prefeitura e paralisação de plataformas de atendimento eletrônico. Esses eventos não apenas impactaram as finanças públicas, mas também prejudicaram diretamente a imagem institucional da

administração municipal, criando a percepção de desorganização, negligência e insegurança digital.

Assim, os impactos econômicos e sociais dos crimes cibernéticos vão além dos prejuízos imediatos. Eles afetam a confiança pública, comprometem políticas sociais e evidenciam a necessidade urgente de planejamento estratégico em segurança digital. É imprescindível que o poder público trate a cibersegurança como parte integrante da gestão pública moderna, adotando medidas preventivas eficazes, fortalecendo a resposta institucional a incidentes e promovendo uma cultura organizacional voltada à proteção de dados e sistemas.

4. CONCLUSÃO

A crescente incidência de crimes cibernéticos contra o patrimônio público em na cidade de Palmas-TO entre 2019 e 2024, com mais de 20.000 boletins de ocorrência registrados no período e uma predominância de 70% de casos relacionados a estelionatos digitais, revela não apenas falhas tecnológicas, mas também uma lacuna grave na formação digital de servidores e cidadãos. Nesse contexto, a educação e a conscientização cibernética emergem como pilares fundamentais para a mitigação dessas ameaças.

Muitos ataques bem-sucedidos exploram o desconhecimento básico de usuários em relação a práticas de segurança digital. A ausência de rotinas seguras, como a atualização frequente de sistemas, o uso de senhas robustas, a atenção a e-mails falsos e a verificação de links suspeitos cria um ambiente favorável à ação de cibercriminosos. Boa parte dos golpes registrados em Palmas envolveu, por exemplo, o uso de perfis falsos de secretarias municipais, fraudes via PIX e envio de boletos adulterados com logotipos oficiais.

Apesar de algumas ações preventivas já implementadas pelos órgãos públicos, como antivírus institucionais e *firewalls* básicos, essas medidas mostraram-se limitadas frente à complexidade dos ataques recentes, muitos dos quais envolvem engenharia social e *ransomware*. Os dados demonstram que, embora milhares de ocorrências sejam registradas anualmente (4.408 em 2022 e 3.911 em 2024), a resposta institucional ainda é tímida: o número de inquéritos instaurados é significativamente menor, e os casos de prisões em flagrante são esporádicos.

Nesse cenário, a promoção da educação cibernética contínua se torna uma estratégia indispensável. A capacitação de servidores públicos, especialmente aqueles com acesso a sistemas sensíveis, deve ser permanente, atualizada e obrigatória. Além disso, a inclusão de conteúdos sobre boas práticas digitais nas formações administrativas e nos treinamentos

internos é uma medida simples, mas altamente eficaz. O município pode, inclusive, estabelecer parcerias com universidades e órgãos de controle para criar trilhas formativas específicas para cada setor.

Por outro lado, campanhas de conscientização destinadas à população também são necessárias, uma vez que muitos dos golpes envolvem o uso indevido de marcas públicas e enganam cidadãos ao simular cobranças de impostos, taxas ou serviços. A informação preventiva, veiculada por canais oficiais e amplamente difundida, pode reduzir substancialmente a taxa de sucesso desses golpes.

Complementarmente, é necessário investir em medidas estruturantes. A instalação de sistemas de detecção e resposta a incidentes (SIEM, IDS/IPS), a adoção de autenticação multifatorial (MFA), o *backup* criptografado em nuvem e a auditoria recorrente de sistemas são mecanismos que precisam ser integrados ao planejamento orçamentário dos órgãos públicos municipais.

Por fim, é recomendável a criação de um protocolo municipal de resposta a incidentes cibernéticos, com fluxos bem definidos de notificação, isolamento, investigação e recuperação. A colaboração entre os setores público e privado, especialmente com empresas de tecnologia da informação, também pode favorecer a construção de soluções mais eficazes, com trocas de inteligência e resposta coordenada a ataques em andamento.

Em síntese, o combate aos crimes cibernéticos no setor público de Palmas/TO, não depende apenas de investimentos em tecnologia, mas, principalmente, da formação de uma cultura institucional de segurança digital, alicerçada na educação, prevenção e responsabilização coletiva. Diante da crescente sofisticação dos ataques e do aumento exponencial dos registros, é imperativo transformar a conscientização cibernética em política pública permanente.

REFERÊNCIAS

AGUIAR, Renan de Sousa; ARAÚJO NETO, Luis Gonzaga de; GUIDA, Maria dos Reis Ribeiro. *Crimes cibernéticos: análise do processo investigatório e os desafios para combatê-los*. Revista F&T, v. 27, out. 2023. Disponível em: https://revistaft.com.br/crimes-ciberneticos-analise-do-processo-investigatorio-e-os-desafios-para-combate-los/. Acesso em: 07 maio 2025.

ADRIELLE da Silva Bispo; EMANUEL Vieira Binto. Revista Ibero-americana de Humanidades, Ciências e Educação, 2023.

BERTHOLDI, Juliana. *Crimes cibernéticos*. 1. ed. São Paulo: Contentus, 2020. E-book. Disponível em: https://plataforma.bvirtual.com.br. Acesso em: 04 dez. 2024.

BOMFATI, Cláudio Adriano; KOLBE JÚNIOR, Armando. *Crimes cibernéticos*. 1. ed. Curitiba: Intersaberes, 2020. E-book. Disponível em: https://plataforma.bvirtual.com.br. Acesso em: 04 dez. 2024.

BRASIL. *Decreto-Lei nº 2.848, de 7 de dezembro de 1940*. Código Penal. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848.htm. Acesso em: 13 maio 2025.

BRASIL. *Lei nº 12.737, de 30 de novembro de 2012*. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal; e dá outras providências. Diário Oficial da União, Brasília, DF, 3 dez. 2012. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 7 maio 2025.

BRASIL. *Lei nº 12.965, de 23 de abril de 2014*. Marco Civil da Internet. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 13 maio 2025.

BRASIL. *Lei nº 13.709, de 14 de agosto de 2018*. Lei Geral de Proteção de Dados Pessoais. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 13 maio 2025.

BRASIL. *Lei nº 14.155, de 27 de maio de 2021*. Altera o Código Penal para agravar penas de crimes cometidos por meio eletrônico. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/L14155.htm. Acesso em: 13 maio 2025.

CONAMP – Associação Nacional dos Membros do Ministério Público. *Painel sobre crimes cibernéticos destaca desafios e cooperação internacional na investigação de delitos digitais*. CONAMP, 2023. Disponível em: https://www.conamp.org.br/imprensa/noticias/9062-painel-sobre-crimes-ciberneticos-destaca-desafios-e-cooperacao-internacional-na-investigacao-de-delitos-digitais.html. Acesso em: 07 maio 2025.

DANIEL Frederick Salustiano. Pontifícia Universidade Católica de Goiás, 2021.

EVA Barros dos Santos Macedo; ENIO Walcácer de Oliveira Filho. Revista JRG de Estudos Acadêmicos, 7(15), e151663-e151663, 2024.

FELICIANO, Guilherme Guimarães. *Criminalidade informática: perigo e prevenção*. In: MIR PUIG, Santiago (Comp.). *Delincuencia informática*. Barcelona: PPU, 1992.

GILABERTE, Bruno. *Crimes contra o patrimônio*. 2. ed. Rio de Janeiro: Freitas Bastos, 2020. E-book. Disponível em: https://plataforma.bvirtual.com.br. Acesso em: 04 dez. 2024.

HERNÁNDEZ Sampieri; FERNÁNDEZ; BAPTISTA. 2019.

IDESP – Instituto Daryus de Ensino Superior Paulista. *Forense Digital e Investigação Cibernética*. São Paulo: IDESP, 2025. Disponível em: https://idesp.com.br/pos_graduacao/forense-digital-e-investigacao-cibernetica/. Acesso em: 07 maio 2025.

KOLBE JÚNIOR, Armando. *Investigação de crimes digitais*. 1. ed. São Paulo: Contentus, 2020. E-book. Disponível em: https://plataforma.bvirtual.com.br. Acesso em: 04 dez. 2024.

OCDE. *Computer-related crime: analysis of legal policy*. Paris: OECD, 1986.

ROSSINI, Augusto Eduardo de Souza. *Informática, telemática e direito penal*. São Paulo: Memória Jurídica, 2004.

SILVA, João Paulo da. *Crimes Cibernéticos e Segurança da Informação*. São Paulo: Editora Jurídica Nacional, 2021.

TEIXEIRA, Tarcisio. *Crimes cibernéticos: análise do processo investigatório e os desafios para combatê-los*. Revista F&T, 2023.

TOCANTINS. Secretaria da Segurança Pública. *Divisão Especializada de Repressão a Crimes Cibernéticos – DRCC*. Palmas: SSP-TO, 2024. Disponível em: https://www.to.gov.br/ssp/divisao-especializada-de-repressao-a-crimes-ciberneticos-drcc/3t5q1veociuz. Acesso em: 15 maio 2025.

TOCANTINS. Secretaria da Segurança Pública. *Painel de Monitoramento da Incidência Criminal*. Palmas: SSP-TO, 2025. Disponível em: https://www.to.gov.br/ssp/estatisticas/37s2impwz72k. Acesso em: 15 maio 2025.

WENDT, Emerson; JORGE, Higor Vinicius Nogueira. *Crimes cibernéticos: ameaças e procedimentos de investigação*. 3. ed. Rio de Janeiro, RJ: Brasport, 2021. E-book. Disponível em: https://plataforma.bvirtual.com.br. Acesso em: 04 dez. 2024.