UNIVERSIDADE DO ESTADO DE MINAS GERAIS

FACULDADE DE POLÍTICAS PÚBLICAS E GESTÃO DE NEGÓCIOS

PROGRAMA DE PÓS-GRADUAÇÃO EM SEGURANÇA PÚBLICA E CIDADANIA CURSO DE MESTRADO PROFISSIONAL

ESTELIONATO EM AMBIENTE VIRTUAL: Desafios para agências policiais em Minas Gerais a partir do olhar da complexidade e das Ciências Policiais

Dissertação de mestrado

MARIANA FIGUEIREDO GONÇALVES FERREIRA

BELO HORIZONTE
2024

UNIVERSIDADE DO ESTADO DE MINAS GERAIS

FACULDADE DE POLÍTICAS PÚBLICAS E GESTÃO DE NEGÓCIOS

PROGRAMA DE PÓS-GRADUAÇÃO EM SEGURANÇA PÚBLICA E CIDADANIA CURSO DE MESTRADO PROFISSIONAL

MARIANA FIGUEIREDO GONÇALVES FERREIRA

ESTELIONATO EM AMBIENTE VIRTUAL: Desafios para agências policiais em Minas Gerais a partir do olhar da complexidade e das Ciências Policiais

Dissertação de mestrado

FAPPGEN /CBH /UEMG
BELO HORIZONTE
2024

UNIVERSIDADE DO ESTADO DE MINAS GERAIS

FACULDADE DE POLÍTICAS PÚBLICAS E GESTÃO DE NEGÓCIOS

PROGRAMA DE PÓS-GRADUAÇÃO EM SEGURANÇA PÚBLICA E CIDADANIA CURSO DE MESTRADO PROFISSIONAL

ESTELIONATO EM AMBIENTE VIRTUAL: Desafios para agências policiais em Minas Gerais a partir do olhar da complexidade e das Ciências Policiais

Dissertação de mestrado

Dissertação apresentada ao Curso de Mestrado Profissional do Programa de Pós-Graduação em Segurança Pública e Cidadania da Faculdade de Políticas Públicas e Gestão de Negócios da Universidade do Estado de Minas Gerais para exame de defesa.

Linha de pesquisa: Gestão e políticas públicas.

Aluna: Mariana Figueiredo Gonçalves Ferreira
Orientador: Prof. Dr. Thiago Penido
Coorientador: Prof. Dr. Francis Albert Cotta

FAPPGEN /CBH /UEMG
BELO HORIZONTE
2024

F383e Ferreira, Mariana Figueiredo Gonçalves.

Estelionato em ambiente virtual: desafios para agências policiais em Minas Gerais a partir do olhar da complexidade e das Ciências Policiais [manuscrito] / Mariana Figueiredo Gonçalves Ferreira. -- 2024.

105 f., enc.: il., color., 31 cm.

Dissertação (mestrado) – Universidade do Estado de Minas Gerais. Programa de Pós-graduação em Segurança Pública e Cidadania, 2024.

Orientador: Prof. Dr. Thiago Penido.

Coorientador: Prof. Dr. Francis Albert Cotta.

Bibliografia: f. 101-105.

1. Segurança pública. 2. Crime por computador - Investigação. 3. Ciências Policiais. I. Penido, Thiago. II. Cotta, Francis Albert. III. Universidade do Estado de Minas Gerais. Programa de Pós-graduação em Segurança Pública e Cidadania. IV. Título

CDU: 343.9

CDD: 355

Bibliotecária responsável: Gilza Helena Teixeira CRB6/1725

Dissertação defendida e aprovada em 30 de agosto de 2024, pela banca examinadora constituída pelos professores:

Prof. Dr. Thiago Penido - Orientador
Universidade do Estado de Minas Gerais - PPGSPCID/FaPPGeN

Prof. Dr. Francis Albert Cotta - Coorientador
Universidade Estadual de Montes Claros - Programa de Pós-Graduação em Ciências Policiais e Tecnologias Inovadoras - UINIMONTES

Prof. Dr. Sílvio José de Sousa Filho - Avaliador
Universidade Estadual de Montes Claros - Programa de Pós-Graduação em Ciências Policiais e Tecnologias Inovadoras

---

Prof. Dr. Rafael Moura - Avaliador
Universidade Estadual de Montes Claros - Programa de Pós-Graduação em Ciências Policiais e Tecnologias Inovadoras - UINIMONTES

Ao Santo Espírito de Sabedoria

que lança luz e entendimento sobre todas as coisas.

RESUMO

FERREIRA, Mariana Figueiredo Gonçalves. Estelionato em ambiente virtual: desafios para agências policiais em Minas Gerais a partir do olhar da complexidade e das Ciências Policiais.

Refletiu-se sobre os desafios apresentados às forças policiais diante da emergência do estelionato em ambiente digital em Minas Gerais, compreendido como um *fenômeno criminal complexo*. Partiu-se do pressuposto que o aumento do delito de estelionato digital durante a pandemia se tornou um indício de fenômeno criminal tendencioso a permanecer no âmbito digital, de modo que exige um estudo de estratégias de gestão policial, bem como fomento estratégico de técnicas para a continuidade do aprimoramento da atuação policial em ambientes digitais. Dessa forma, buscou-se investigar o fenômeno criminal de estelionato digital sob a égide da Teoria da Migração e suas implicações na atividade policial. No plano jurídico, objetivou-se perceber a complexidade do crime à distância e, diante disto, buscou- se compreender a natureza do delito de estelionato digital e perceber as alterações no Código Penal que condicionam o crime de estelionato à representação da vítima. Metodologicamente, realizou-se breve uma revisão de literatura e do arcabouço legal que tratam de cibercrimes no campo das Ciências Policiais. Na sequência, foram coletados dados estatísticos dos registros de crimes em ambiente virtual no território mineiro no período de 2018 a 2022. Interpretou-se, por meio de análise quantitativa, os dados absolutos dos Registros de Eventos de Defesa Social relativos ao Estelionato no período de 2018 a 2022, recorte temporal delimitado em decorrência da pandemia de Covid-19, ápice de 2019 a 2020, cenário que influenciou o aumento das relações remotas. Revisitou-se os estudos que traçaram o protocolo de atuação para Polícia Militar nos crimes cibernéticos, para propor atualizações que consideram as limitações de competências constitucionais investigativas pela Polícia Militar e a condição limitadas de atuação imediata nesse tipo de flagrante, além de analisar a atual condição de atuação da Polícia Civil nos mesmos delitos, em decorrência da resolução que condicionou a investigação pela Delegacia de Crimes Cibernéticos aos danos suportados acima de cem salários mínimos. Os resultados indicaram o aumento dos crimes cibernéticos, percebidos como um *fenômeno criminal complexo,* o que lança novos desafios para a atuação das agências policiais. Conclui-se que para o enfrentamento dessa modalidade criminosa é necessário conhecer esse fenômeno, desenvolver capacitações e criar protocolos integrados que envolvam as forças policiais, órgãos estatais, sociedade civil e empresas prestadoras de serviços.

Palavras-chave: Segurança Pública, estelionato digital, crimes patrimoniais, crimes cibernéticos, Ciências Policiais.

ABSTRACT

FERREIRA, Mariana Figueiredo Gonçalves. Fraud in a virtual environment: challenges for police agencies in Minas Gerais from the perspective of complexity and Police Sciences.

This study examines the challenges faced by law enforcement due to the emergence of digital fraud in Minas Gerais, recognized as a complex criminal phenomenon. It is posited that the increase in digital fraud during the pandemic indicates a criminal trend likely to persist in the digital realm, necessitating an exploration of police management strategies and the strategic development of techniques to enhance police operations in digital environments. The investigation delves into the digital fraud phenomenon through the lens of Migration Theory and its implications for police activity. Legally, the study aims to understand the complexity of distance crime, focusing on the nature of digital fraud and the changes in the Penal Code requiring victim representation for fraud cases. Methodologically, the study includes a brief literature review and an analysis of the legal framework addressing cybercrimes in the field of Police Sciences. Statistical data on virtual crime reports in Minas Gerais from 2018 to 2022 were collected. A quantitative analysis of the absolute data from Social Defense Event Records related to fraud was conducted for the specified period, marked by the Covid-19 pandemic, which influenced an increase in remote interactions. The study revisited protocols for Military Police action in cybercrimes, proposing updates that consider the constitutional investigative limitations of the Military Police and the restricted capacity for immediate action in such cases, alongside analyzing the current operational conditions of the Civil Police in these crimes, due to a resolution that limits cybercrime investigations to damages exceeding one hundred minimum wages. The results indicated an increase in cybercrimes, seen as a complex criminal phenomenon that presents new challenges for police agencies. The study concludes that addressing this criminal modality requires understanding the phenomenon, developing training, and creating integrated protocols involving police forces, state agencies, civil society, and service providers.

Keywords: Public Security, Digital Fraud, Property Crimes, Cybercrimes.

LISTA DE SIGLAS

CBMMG	Corpo de Bombeiro Militar de Minas Gerais
CINDS	Centro Integrado de Defesa Social
COECIBER	Coordenadoria Estadual de Combate aos Crimes Cibernéticos
DGEOp	Diretriz Geral para Emprego Operacional
PCMG	Polícia Civil de Minas Gerais
PMMG	Polícia Militar de minas Gerais
REDS	Registro de Evento de Defesa Social
AISP	Área Integrada de Segurança Pública
BH	Belo Horizonte
DIAO	Diretriz Integrada de Ações e Operações
MG	Minas Gerais
PCMG	Polícia Civil do Estado de Minas Gerais
PMMG	Polícia Militar do Estado de Minas Gerais
REDS	Registro de Evento de Defesa Social
RISP	Região Integrada de Segurança Pública
SEJuSP	Secretaria de Estado de Justiça e Segurança Pública
SENASP	Secretaria Nacional de Segurança Pública
SISP	Sistema Integrado de Segurança Pública
UEMG	Universidade do Estado de Minas Gerais
IP	Internet Protocol
LGPD	Lei Geral de Proteção de Dados
DOU	Diário Oficial da União
CP	Código Penal
IA	Inteligência Artificial
GCC	Grupo de de Combate aos Crimes Cibernéticos

SMS	Short Message Service
ORCRIMS	Organizações Criminosas
SIDS	Sistema Integrado de Defesa Social
CGA	Centro de Gestão de Análise de Dados Estatísticos
DOP	Diretoria de Operações
NIC.br	Núcleo de Informação e Coordenação do Ponto BR

LISTA DE GRÁFICOS

LISTA DE QUADROS

LISTA DE FIGURAS

LISTA DE MAPAS

SUMÁRIO

1 INTRODUÇÃO

Com o advento da internet de forma globalizada, especialmente a partir da década de 1990[1], apresentaram-se inúmeras possibilidades e, ao mesmo tempo, desafios que impactaram as relações sociais. No campo criminal, emergiu o que se convencionou chamar de crime cibernético ou cibercrime. O aumento desse novo tipo de delito fez com que representantes das nações que compõe o G8 se reunissem em 2000 na cidade francesa de Lyon para tratar da questão[2]. Em 2001, realizou-se em Budapeste, a Convenção sobre o Crime Cibernético.

Entretanto, somente em 2023, o Brasil, ao aceitar o convite do Conselho da Europa, passou a ser um dos países que aderiram a tal instrumento internacional, fortalecendo assim os laços de cooperação com parceiros estratégicos no enfrentamento aos crimes cibernéticos. O Decreto n.º 11.491, que traz a decisão, foi publicado no Diário Oficial da União (DOU) no dia 12 de abril de 2023.

O instrumento orienta que cada parte dever adotar medidas legislativas e outras providências necessárias para tipificar como crime, em sua legislação interna, a conduta de quem causar, de forma dolosa e não autorizada, prejuízo patrimonial a outrem por meio de:

> a. qualquer inserção, alteração, apagamento ou supressão de dados de computador;
> b. qualquer interferência no funcionamento de um computador ou de um sistema de computadores, **realizada com a intenção fraudulenta de obter, para si ou para outrem, vantagem econômica ilícita** (Convenção de Budapeste. Título 2, Art. 8º, 2001, grifo nosso).

Nesse sentido, o crime de estelionato, que figura no Código Penal Brasileiro desde a sua primeira versão publicada em 1940, sofreu recente alteração em seu texto, sendo acrescidos novos tipos dentro do artigo 171, especialmente:

> **Fraude eletrônica**
> § 2º- A. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se a fraude é

1- De acordo com a Rede Brasileira para Educação, Pesquisa e Inovação (RNP), vinculada ao Ministério da Ciência, Tecnologia e Inovação, somente em 1992 o Brasil tem a primeira rede acadêmica, sendo que a abertura da internet comercial ocorreu em 1995. Disponível em: https://www.rnp.br/noticias/evolucao-da-internet-no-brasil#:~:text=A%20primeira%20rede%20acad%C3%AAmica%20brasileira,depois%2C%20em%20maio%20de%201995.

> cometida com a utilização de informações fornecidas pela vítima ou por terceiro induzido a erro por meio de redes sociais, contatos telefônicos ou envio de correio eletrônico fraudulento, ou por qualquer outro meio fraudulento análogo.
>
> § 2º- B. A pena prevista no § 2º- A deste artigo, considerada a relevância do resultado gravoso, aumenta-se de 1/3 (um terço) a 2/3 (dois terços), se o crime é praticado mediante a utilização de servidor mantido fora do território nacional.
>
> § 3º - A pena aumenta-se de um terço, se o crime é cometido em detrimento de entidade de direito público ou de instituto de economia popular, assistência social ou beneficência (Brasil, 1940).

De acordo com o Juiz Fernando Brandini Barbagalo, do Tribunal de Justiça do Distrito Federal e dos Territórios, a Lei n.º 14.155/21 alterou o crime de invasão de dispositivo informático ao aperfeiçoar sua redação e aumentar substancialmente suas penas (art. 154-A do CP). Na mesma alteração legislativa foram criados os crimes específicos de furto mediante fraude eletrônica (art. 155, § 4º-B do CP) e de fraude eletrônica (art. 171, § 2º - A do CP).

Como visto, foi acrescentado no art. 171 do Código Penal, que define o crime de estelionato, o § 2º - A, uma modalidade de estelionato qualificado, a qual recebeu o nomen iuris de "fraude eletrônica".

Para o magistrado, “a inovação legislativa chegou com algum atraso, pois as condutas que se enquadram em sua definição, assim como as equivalentes ao furto mediante fraude eletrônica, causam intranquilidade há algum tempo”. [3]

Criminosos que utilizam o ambiente virtual aperfeiçoaram suas técnicas e passaram a violar camadas de segurança, mesmo sem o uso de programas sofisticados, para descobrir entradas vulneráveis[4]. A maioria dos ataques utiliza a chamada Engenharia Social, que explora as permissões dos usuários do ambiente virtual em sistemas de computadores para acesso e obtenção de vantagens indevidas. O custo dessa empreitada é mínimo para o invasor, não lhe exigindo poder computacional sofisticado, tampouco conhecimento especializado em computação. Criatividade e poder de convencimento são as ferramentas comumente utilizadas[5].

2 - O Grupo dos Oito, conhecido como G8 é um fórum informal que reunia oito países desenvolvidos (Estados Unidos, Japão, Alemanha, Canadá, França, Itália, Reino Unido e Rússia). Seu objetivo era debater assuntos-chave relacionados à estabilidade econômica global, políticas nacionais e cooperação com as instituições econômico-financeiras internacionais. Disponível em: https://www.gov.br/mj/pt-br/assuntos/noticias/convencao-de-budapeste-e-promulgada-no-brasil.

A utilização dessas técnicas para obtenção de dados pessoais tornou-se uma grande preocupação para as organizações públicas, privadas e para os cidadãos. Em nível federal, o Ministério da Justiça e Segurança Pública do Brasil disponibiliza em sua página algumas orientações sobre os crimes digitais. O estudo das questões afetas à Engenharia Social é alvo de diversas áreas do conhecimento, tais como as Ciências da Informação, Ciências Jurídicas e Ciências Policiais.

De forma cotidiana, por meio de registros de boletins de ocorrências, as agências policiais constatam novas modalidades de crimes que utilizam tecnologias virtuais. A internet criou oportunidades para criminosos, como é exposto na "A Arte de Invadir. As verdadeiras Histórias por trás das ações de *hackers*, intrusos e criminosos eletrônicos", de autoria dos norte-americanos Kenin Mitnick e William Simon. O livro foi traduzido para o português e publicado em 2006. Na referida obra, os autores exploram a Engenharia Social e como *hackers* a utilizam para invadir e acessar informações não autorizadas[6].

A inserção dos novos meios informacionais como redes sociais e aplicativos de mensagens aumentou os processos de interação, as possibilidades de contatar pessoas e, assim, realizar fraudes[7]. Esse ambiente virtual proporciona uma sensação de segurança ao criminoso em virtude do anonimato e do baixo custo dos recursos necessários à aplicação de golpes.

Diante desse contexto, a pesquisa perfaz reflexões a partir de dados concretos sobre o "fenômeno criminal complexo" denominado estelionato em ambiente virtual em termos dos desafios enfrentados pela gestão policial diante desse tipo de cibercrime patrimonial. A despeito de ser um fenômeno de interesse de diferentes áreas do conhecimento, tais quais Criminologia, Ciências Jurídicas, Administração Pública, Segurança Pública e Estatística Criminal, optou-se por interpretá-lo sob o olhar das Ciências Policiais.

3 - Disponível em: https://www.tjdft.jus.br/institucional/imprensa/campanhas-e-produtos/artigos-discursos-e-entrevistas/artigos/2022/o-novo-crime-de-fraude-eletronica-e-o-principio-da-legalidade.

4 - Disponível em: https://www.gov.br/mj/pt-br/assuntos/sua-protecao/sedigi/crimes-digitais.

5 - A Engenharia Social é uma técnica de manipulação que explora erros humanos para obter informações privadas, acessos ou coisas de valor. No crime cibernético, esses golpes de "hacking humano" tendem a atrair usuários desavisados para expor dados, espalhar infecções por malware ou dar acesso a sistemas restritos. Disponível em: https://www.kaspersky.com.br/resource-center/definitions/what-is-social-engineering.

Coloca-se como problema de pesquisa a seguinte questão: como as agências policiais podem enfrentar os desafios apresentados pelo "fenômeno criminal complexo" do estelionato em ambiente virtual? A hipótese que se coloca é que se torna necessário primeiramente conhecer esse (in) visível fenômeno em sua multidimensionalidade e complexidade, em seguida criar rotinas e protocolos integrados entre as agências policiais, instituições públicas e privadas, além da sociedade civil, para enfrentamento a esse tipo de cibercrime patrimonial. Por fim, é necessária capacitação dos envolvidos para criar competências necessárias.

Diante do problema e hipótese, elegeu-se como objetivo geral desta dissertação refletir sobre o "fenômeno criminal complexo" do estelionato em ambiente virtual, como um tipo de cibercrime patrimonial. Como objetivos específicos têm-se: analisar teoricamente a multimensionalidade dessa modalidade criminosa e apresentar dados quantitativos que lancem luz sobre ela.

6 - Kevin David Mitnick (1963-2023) foi programador e hacker norte-americano, que passou a atuar como assessor de segurança na Web. Sua obra é composta pelos seguintes livros: The Art of Deception: Controlling the Human Element of Security (2002), The Art of Intrusion: The Real Stories Behind the Exploits of Hackers, Intruders & Deceivers (2005), Ghost in the Wires: My Adventures as the World's Most Wanted Hacker (2011) e The Art of Invisibility (2017).

7 - O Marco Civil da Internet (Lei n.º 12.965/2014) foi sancionado em 2014 e regula os direitos e deveres dos internautas.

2 CIÊNCIAS POLICIAIS E O DESAFIO DOS CRIMES CIBERNÉTICOS

Este estudo se insere na linha da gestão pública, especificada na gestão das agências policiais, com fulcro nas Ciências Policiais e a urgente a implementação de políticas de Segurança Pública eficazes para além da sociedade física, por meio da promoção do conhecimento sobre a (in)segurança digital.

No cenário contemporâneo, o mundo enfrenta uma multiplicidade de riscos e ameaças que transcendem fronteiras nacionais e desafiam as capacidades tradicionais dos Estados. (Barreto; Fonseca, 2023). A globalização e a interdependência tecnológica são características marcantes da nova Modernidade Líquida, conforme denomina Bauman (1999). Tais mudanças demandam reformas profundas nos conceitos e estratégias de segurança, tanto nacional quanto internacionais.

A despeito de a atual segurança pública ainda lidar com problemas e ameaças tradicionais, as novas tecnologias avançadas trazem à tona problemas relativamente novos e de difícil compreensão, o que acarreta em novas vulnerabilidades. Dentre esses problemas, destaca-se aqui o crime cibernético patrimonial, especialmente no que tange aos novos golpes praticados, tipificados como estelionato digital.

O estelionato digital envolve fraudes financeiras realizadas por meio de meios eletrônicos e, conforme será tratado adiante nessa dissertação, tem relação direta com a segurança econômica da presente sociedade mineira. Para Barreto e Fonseca (2023), na atual formatação, o crime explora, além da Engenharia Social, falhas de segurança cibernética para acessar informações sensíveis e realizar transações reais, mas desencadeadas por meios fraudulentos, o que acarreta prejuízos significativos às vítimas. A natureza complexa, conforme capítulo próprio, e transnacional do estelionato digital torna sua repressão e prevenção especialmente desafiadoras, para tanto, no âmbito externo passa por projetos de cooperação internacional, principalmente no que tange à sua execução por organizações

criminosas (ORCRIMS) e desenvolvimento de novas capacidades tecnológicas (Barreto, Fonseca, 2023).

Observado como nova ameaça recorrente ao patrimônio privado, o estelionato digital inclui-se como uma das áreas críticas das vulnerabilidades do mundo em rede, e carece de adoção de estratégias inovadoras de segurança cibernética, bem como um estudo acurado de Inteligência que procuraria a interligação da alteração legislativa de condicionar o crime à representação e os interesses de organizações criminosas diversas, assuntos que não serão objetos desta dissertação. A interconexão global facilita a disseminação de técnicas fraudulentas e a coordenação entre criminosos, o que justifica o estudo e a busca de respostas com alta prioridade para a segurança pública dos estados brasileiros, países e organizações internacionais.

As respostas tradicionais, como ocupação de espaços físicos da sociedade e aplicação da lei por meio do uso das forças de segurança, tornam- se insuficientes para enfrentar as novas ameaças. Portanto, é necessário desenvolver um novo paradigma de segurança pública, que integre a segurança cibernética como um dos componentes centrais, de forma a contemplar a cooperação entre as entidades e órgãos setores públicos, senão também privados, após a criação de regulamentação rigorosa para tais cooperações, atualmente já previstas na Lei de licitações e contratos, situações que podem oportunizar o desenvolvimento contínuo de tecnologias de proteção.

Em 2023, o Ministério da Justiça e Segurança Pública oportunizou aos integrantes das agências responsáveis pela segurança pública o Curso Detecção de Fraudes Eletrônicas em Períodos de Crise e expôs que o aumento da urbanização e as transformações sociais, culturais e econômicas ampliaram os riscos da criminalidade digital, de modo que a anonimidade oferecida pelos espaços cibernéticos passou a facilitar a atuação de criminosos (Barreto, Fonseca, 2023).

Em que pese as instituições se preocuparem com os tradicionais problemas de roubo e homicídio, por questões lógicas de quebra da ordem pública e sensação subjetiva de segurança da sociedade ser abruptamente quebrada, há que ser reconhecido pelas forças de

segurança pública do Brasil que os problemas de segurança cibernética existem e são relevantes para cada instituição, pois geram perda do poder estatal de agir, descredibilidade institucional de atuação e causam efeitos de sensação de insegurança em longo prazo e em longa escala, pois passa-se a crer que o Estado não é capaz de proteger e de ocupar espaços sociais fictos novos. Tais problemas não podem ser resolvidos isoladamente por cada estado da federação, porque exigem mobilização ampla e a coprodução da segurança entre todos os atores relevantes para responder eficazmente aos desafios colocados pelo estelionato digital como desafio para as Ciências Policiais.

2.1 Ciências Policiais: fundamentos

Historicamente, as Ciências Policiais emergem como um ramo científico voltado à compreensão e enfrentamento de questões sociais, especialmente na acepção de segurança nacional, conforme mencionado na obra "Ciências Policiais: conceito, objeto e método da investigação científica" elaborada por Azor Lopes da Silva Júnior *et al* (2023, p. 40). O estudo trata da análise da evolução das Ciências Policiais no contexto europeu, e correlaciona-se à observância das grandes mudanças sociais, dos riscos e ameaças à segurança, bem como às respostas estatais (Silva Júnior *et al*, 2023, p. 44).

Conforme a obra, as novas ameaças transnacionais incluem, dentre outras, o uso ilícito da ciência, das tecnologias, e o crime organizado. Além disso, questões como pandemias e a dependência de infraestruturas em rede, mantém o cenário de segurança ainda mais hostil. Diante desse contexto, os Estados carecem de desenvolver novas capacidades e colaborar de forma mais estreita, seja em âmbito nacional, seja em âmbito internacional (Silva Júnior *et al*, 2023, p. 45).

Infere-se das obras que abordam o objeto e os fundamentos das ciências policias que a segurança nacional atual, como denominada por Silva Júnior *et al* (2023), não se limita mais apenas à proteção territorial e à defesa militar, mas engloba a proteção dos direitos e

> A segurança humana, proposta pelo PNUD em 1994, enfatiza a proteção das vidas humanas e a realização das pessoas, redefinindo a função do Estado e das forças policiais. As novas exigências de segurança requerem uma abordagem mais **integrada, envolvendo setores públicos e privados, e uma mobilização social para enfrentar eficazmente os problemas de segurança** (Silva Júnior *et al*, 2023, p. 41; Grifo nosso)[8].

Portanto, as Ciências Policiais são um reflexo das transformações sociais, tecnológicas e políticas, de modo que se torna imprescindível que as respostas estatais sejam aprimoradas com os desafios, por meio de propostas colaborativas e que reconheçam a complexidade e a interconexão dos riscos contemporâneos, conforme conceitos de Edgar Morin. Para tanto, as Ciências Policiais não apenas devem acompanhar as mudanças, mas também devem desempenhar um papel crucial na formulação de estratégias inovadoras e eficazes para garantir a segurança em um mundo cada vez mais complexo e interdependente.

Nos “Tópicos especiais em Ciências Policiais” de Luciano Loiola da Silva *et al*. (2022), o capítulo escrito por Luciano Loiola da Silva no ano de 2022 sobre "Os Princípios Jurídicos Norteadores da Atividade Policial" (p. 295), são abordados diversos princípios que guiam a atuação das forças de segurança pública.

Dentre esses princípios, destacam-se os da legalidade, juridicidade, tipicidade, proporcionalidade, eficiência, participação, aproximação dos serviços às populações, desburocratização, prossecução ou indisponibilidade do interesse público, além de citar como princípios também a prevenção e a precaução, não comumente citados em outros âmbitos das ciências da administração (Silva, 2022, p.310).

Se a atividade policial é pautada nesses princípios, as ciências policias, por intermédio de seu objeto de estudo, também carecem de observá-los. Conforme a obra, o princípio da legalidade exige que todas as ações policiais estejam em conformidade com a lei, de forma a garantir que nenhum ato seja arbitrário. A juridicidade vai além da legalidade, requerendo que a atividade policial observe os princípios gerais do direito e os valores constitucionais. A tipicidade refere-se à necessidade de que qualquer conduta policial esteja claramente descrita em lei. Por fim, o princípio da proporcionalidade assegura que as ações policiais

8 – Disponível em: https://www.undp.org/pt/brazil/sobre-o-pnud.

sejam adequadas, necessárias e proporcionais ao objetivo a ser alcançado, evitando excessos e abusos de poder (Silva, 2022, p.302).

A prevalência dos direitos fundamentais, conforme previsto da Constituição da República Federativa do Brasil (CRFB/88), enfatiza o respeito à dignidade da pessoa humana e às garantias dela decorrentes, tratando-se de um fundamento do Estado Democrático de Direito. A eficiência, como delineado na Carta Magna brasileira, impõe que a administração pública, incluindo as forças policiais, exerça suas funções de maneira imparcial, transparente, eficaz e sem burocracia, visa sempre o bem comum e a qualidade dos serviços prestados à sociedade (Silva, 2022, p. 306). A eficiência na atividade policial, derivada do princípio expresso do artigo 37 da CRFB/88, deve ser avaliada não apenas em termos econômicos, mas considerando os impactos sociais sobre os cidadãos, o que coaduna diretamente com a perspectiva de gestão pública policial eficiente para com os crimes patrimoniais cibernéticos.

Para Silva (2022, p. 307) existem, dos importantes, mas pouco usuais, princípios da participação, aproximação dos serviços às populações e desburocratização. Esses princípios destacam a importância da inclusão dos cidadãos na gestão pública e na colaboração com o poder público para o bem-estar coletivo. Eles norteiam a aproximação dos serviços policiais para com a comunidade e podem promover uma gestão mais participativa e transparente.

Apesar do nome *iuris* ser pouco usual, o princípio da prossecução é conhecido como princípio da indisponibilidade do interesse público, da vertente da Administração Pública que atua com o binômio supremacia e indisponibilidade do interesse público. Insta saber que o objetivo final da Administração deve ser sempre o interesse coletivo, principalmente e principiologicamente nas Ciências Policias.

A Constituição da República, ao estabelecer a promoção do bem de todos como objetivo fundamental, reforça que as ações do Estado, incluindo a atividade policial, devem buscar o interesse comum da sociedade. Significa que, na dinâmica atual do aumento exponencial de crimes específicos, deve o Estado promover soluções para tais demandas sociais. No caso

desta dissertação, a avaliação da demanda social perfaz o aumento dos registros de estelionato praticado pelo meio internet, a ser tratado nos capítulos seguintes.

Por sua vez, os princípios da prevenção e da precaução mencionados, tratam da importância de ações proativas para evitar danos sociais. Portanto, a polícia deve atuar não apenas em resposta a crimes já ocorridos, mas também preventivamente para evitar que danos aconteçam, de forma a garantir a segurança e o bem-estar da população (Silva, 2022, p. 311). Uma das grandes questões que se apresenta, permeia a forma de prevenção de delitos cibernéticos, especialmente no que tange ao estelionato digital. Algumas das pesquisas revisitadas e ações implementadas pelas agências permeiam ideias de conscientização e divulgação dos golpes mais frequentes por meio de cartilhas, com o fim de levar à população o modo de atuação dos agentes e evitar a concretização do resultado por meio do conhecimento.

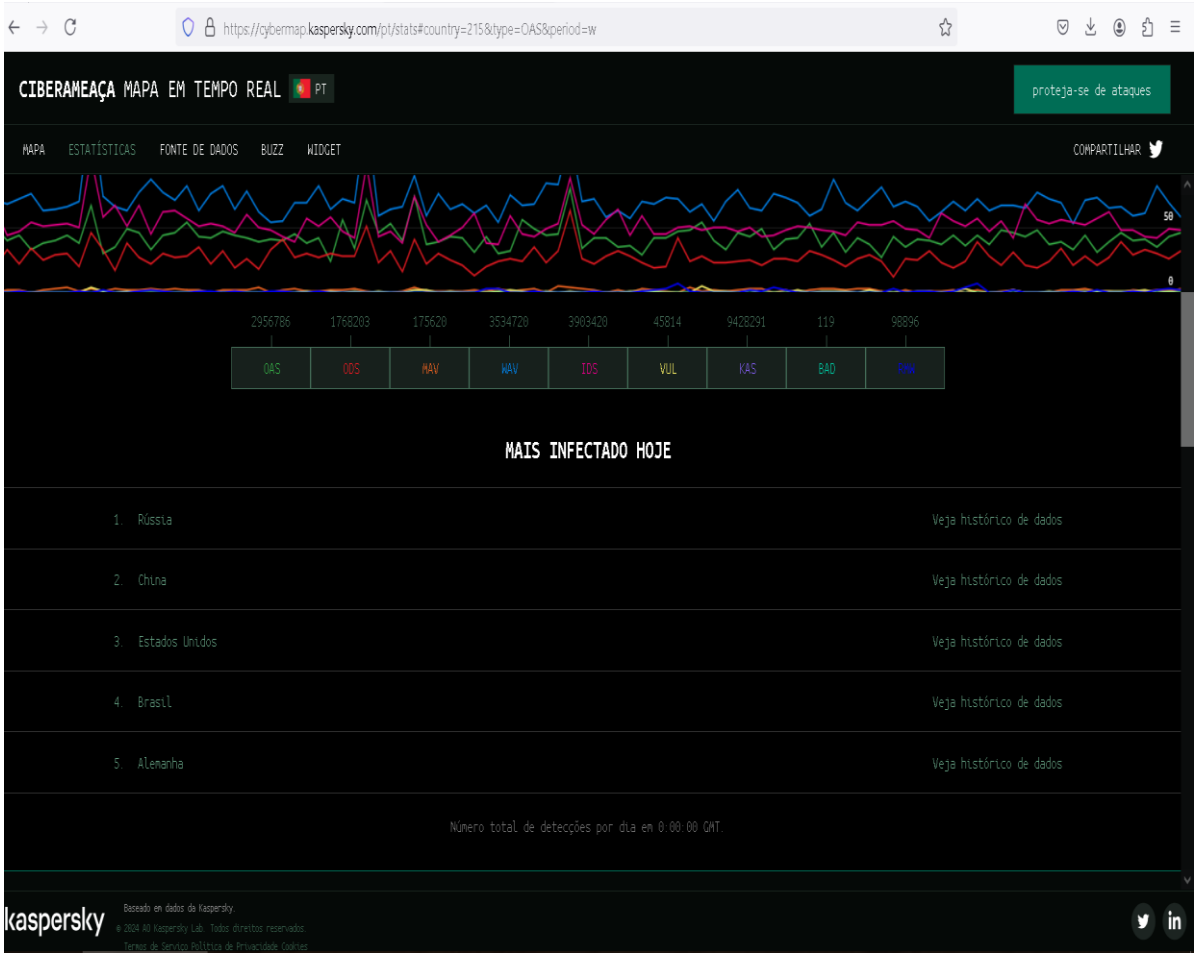
Em sua conclusão, Loiola da Silva enfatiza que os princípios jurídicos são essenciais para a interpretação do ordenamento jurídico vigente e para a boa execução da atividade policial. A prática policial, devido às suas especificidades e ao grande impacto no cotidiano dos cidadãos, deve ser orientada por normas claras e precisas para evitar injustiças e ilegalidades (Silva, 2022, p.316). Não contrário à legalidade, mas em consonância com o artigo 37 da CF e devido à natureza discricionária da atividade policial e às lacunas deixadas pelo legislador, os princípios jurídicos servem como fundamento às Ciências Policiais e norte para atuações policiais legítimas, legais e eficientes em situações onde a legislação pode ser insuficiente ou ambígua ou se tratar de delitos complexos, como são os cibernéticos, conceitos que serão adiante detalhados.

2.2 Crimes Cibernéticos

Em consulta realizada no dia 29 de julho de 2024 à fonte aberta estatística denominada Kaspersky, que mantém vigilância e estatísticas atualizadas em tempo real sobre fraudes e invasões cibernéticas (genericamente denominados, mas que possuem tipos específicos) o

Brasil figurou como 4º (quarto) país mais infectado do mundo nesse dia específico. Foi realizado o monitoramento e houve pouca alternância de colocação no mês de julho de 2024, permanecendo atrás apenas da Rússia, China e Estados Unidos. Quanto ao histórico de estatísticas do referido *site*, na semana do dia 22 ao dia 29 de julho de 2024, o Brasil figurou como 4º país mais atacado da América do Sul, com 3,4% dos ataques mundiais, bem como figura ainda em 5º lugar da América do Sul no que tange à estatística mensal do mês de Julho de 2024 (FIG. 1)[9].

Figura 1 – Países mais atingidos do mundo pelas fraudes e invasões cibernéticas no dia 29 de julho de 2024



Fonte: https://cybermap.kaspersky.com/pt/stats.

De interessante reflexão são os ataques considerados pelo Kaspersky e pelo CertBR, bem como amostra total de dados solicitados para análise e obtidos, mas em razão da delimitação

9 - Disponível em: https://cybermap.kaspersky.com/pt/stats.

do objeto, esta dissertação ser aterá ao crime de estelionato praticado pelo meio digital e ao banco de registro de ocorrências policiais do Estado de Minas Gerais.

O Curso Detecção de Fraudes Eletrônicas em Períodos de Crise, já mencionado no título 2, objetivava em 2023 capacitar os profissionais para identificar e mitigar fraudes eletrônicas e compreender a relação entre crises e segurança pública. O curso abordou com detalhes os desafios enfrentados pelos profissionais responsáveis pela segurança pública durante a pandemia de Covid-19, com foco no aumento das fraudes eletrônicas e teve como produto a produção de uma cartilha informativa (Brasil,2020).

A cartilha do Ministério da Justiça destacou a migração do crime para o ambiente virtual devido a fatores como isolamento social e o crescimento do comércio eletrônico, teorias não citadas, mas correlatas às teorias sociológicas da migração e adaptação do crime.

Percebe-se que o material produzido é suscinto e completo, possui como público alvo as forças policiais brasileiras e pode ser amplamente difundida nas agências por sua didática clara e objetiva. Possui resumidamente o tratamento dos assuntos:

1. **Contextualização**: explora as mudanças tecnológicas e sociais durante a pandemia e destaca a dependência da sociedade da tecnologia e seus impactos na segurança pública.
2. **Engenharia Social**: define Engenharia Social e suas classificações e aborda a exploração das vulnerabilidades humanas.
3. **Modalidades de Engenharia Social pelo Uso da Tecnologia**: analisa diferentes tipos de fraudes e golpes aplicados através da internet, como phishing e outros esquemas.
4. **Atuação do Profissional de Segurança Pública**: fornece estratégias para a prevenção e combate a fraudes eletrônicas, enfatizando a importância da cibersegurança.

Recomenda-se a divulgação do a cartilha do Ministério da Justiça nas agências, pois esta inicia com a descrição da pandemia de Covid-19 e suas consequências globais, situação que aqui se percebe como marco histórico referência ou ponto de virada. Essas consequências globais também foram trabalhadas por Alexandre Herculano Junqueira em sua pesquisa

publicada em 2022, ambos os trabalhos atrelam o fato de que a crise sanitária forçou uma adoção massiva de tecnologias digitais e expôs as vulnerabilidades da sociedade à época. Como exemplos, cita-se o aumento do uso da internet para trabalho remoto, entretenimento, telemedicina e comércio eletrônico, e, com isso, a criação de um ambiente propício para crimes cibernéticos (Leite, 2018; Barreto; Fonseca, 2023). Quanto à essa última situação, percebe-se que, ao viés do trabalho atual, não houve propriamente a criação do ambiente, mas apenas exposição do risco da não ocupação, pelo leviatã, do ambiente virtual, acarretando no sopesamento da importância da vigilância estatal.

Quanto à Engenharia Social, têm-se o conceito interessante de estudo apresentado pelo Ministério da Justiça e fora descrita como o uso de manipulação psicológica para obter informações confidenciais (Brasil, 2022, p. 13). Esse conceito torna-se essencial para a percepção da atual prática do delito, e será abordado nesta dissertação em capítulo específico. A produção ensina ainda como identificar fraudes e golpes baseados na exploração das vulnerabilidades humanas e considera a importância da conscientização e da educação para a prevenção de ataques.

O desenvolvimento das tecnologias pela segurança pública no contexto da crise da Modernidade requer uma abordagem proativa e integrada para garantir a segurança e a integridade dos sistemas digitais. Por fim, a produção da cartilha do governo federal é uma enfatização à necessidade de atualização constante e treinamento contínuo dos profissionais de segurança pública para enfrentar as fraudes eletrônicas em tempos de crise e a cartilha produzida pelo Ministério da Justiça é plausível de retransmissão pelas agências estatais aos seus integrantes.

2.3 Trabalho policial e delitos patrimoniais digitais: o estado da arte

Ao realizar uma revisão de literatura sobre o tema, observou-se que em 2018, num momento temporal pré-pandemia de Covid-19, Leite (2018) realizou a pesquisa intitulada “A Polícia Militar de Minas Gerais na era dos crimes cibernéticos: diretrizes para uma proposta de

estratégia preventiva e protocolo de atuação", apresentada ao Curso de Especialização em Gestão Estratégica de Segurança Pública, do Centro de Pesquisa e Pós-Graduação da Academia de Polícia Militar de Minas Gerais. O pesquisador identificou nos registos de boletins de ocorrência modalidades delituosas cibernéticas tais como a invasão de dispositivo informático.

Leite (2018) propôs uma estratégia preventiva que consiste em fornecer aos policiais conhecimentos sobre o tema, bem como para a comunidade destinatária dos serviços da PMMG. O pesquisador sugeriu a adoção de duas linhas de ação, concomitantes e complementares: atualizar a Diretriz Integrada de Ações e Operações do Sistema de Defesa Social de Minas Gerais (DIAO) e inclusão de anexos ao Registro de Eventos de Defesa Social (REDS), o que foi realizado. Propôs a criação de uma comissão interna para a definição de protocolos básicos para atuação em caso de crimes cibernéticos.

A investigação teve o mérito de mostrar que o fenômeno do crime cibernético constituía preocupação de agências policiais em países como Estados Unidos, Reino Unido, Alemanha, China, Austrália, Canadá, Holanda, Índia, Estônia, que já possuíam estruturas formais voltadas para ações de *cyber policing* (Leite, 2018, p. 81).

Logo após a realização dessa pesquisa eclodiu a pandemia de Covid-19. Nesse momento, foram disponibilizados novos meios informacionais e de interação, tais como redes sociais e aplicativos de mensagens. Ampliaram-se os acessos, reuniões e atividades laborais em ambientes virtuais em decorrência da restrição do direito de locomoção e de outras medidas que visam a contenção da pandemia.

Após a pandemia do Covid-19 foram integradas ao cotidiano das pessoas e das instituições estatais e privadas novas tecnologias de informação e de comunicação. Essas tecnologias se incorporaram ao mercado, e impactaram os processos de produção, venda e distribuição de bens e serviços. As relações econômicas se expandiram para o ciberespaço. Parte-se do pressuposto de que a pós pandemia de Covid-19, a inserção de inovações tecnológicas no ambiente virtual potencializou os delitos digitais.

Desafios se colocam para as forças policiais, seja em termos preventivos quando na investigação. Em Minas Gerais estabeleceu-se limitação de valores para investigação. O valor de golpe deve estar acima de cem salários mínimos para que ocorra a investigação. De acordo com a Convenção de Budapeste (2001):

> **Título 3 - Sistema de plantão 24 por 7**
>
> Artigo 35 - Sistema de plantão 24 por 7
>
> 1. Cada Parte indicará um órgão de contato disponível 24 horas por dia, 7 dias por semana, de modo a assegurar a assistência imediata para investigações ou procedimentos relacionados a crimes de computador e de dados, ou para a obtenção de provas eletrônicas de uma infração penal. Tal assistência incluirá a facilitação, ou, se permitido pelas leis e costumes jurídicos locais, a adoção direta das seguintes medidas:
>
> a. o fornecimento de suporte técnico;
>
> b. a conservação de dados de acordo com os artigos 29 e 30;
>
> c. a coleta de provas, o fornecimento de informação jurídica e a localização de suspeitos.
>
> 2.a. O órgão de contato da Parte deve ser capaz de se comunicar com o órgão de contato de outra Parte de forma rápida.
>
> b. Se o órgão de contato indicado por uma Parte não integrar a autoridade ou autoridades dessa mesma Parte, responsáveis pela assistência mútua internacional ou por extradição, o órgão de contato deve ser capaz de se coordenar com tal autoridade ou autoridades de forma breve.
>
> 3. Cada Parte assegurará que pessoal treinado e bem equipado estará a postos, de modo a facilitar a operação do sistema.

Dessa forma, diante dos comandos da Convenção sobre o Crime Cibernético, serão necessários ajustes para o seu cumprimento pelo Brasil e consequentes desdobramentos em nível dos estados da Federação, o que impactará diretamente as ações da força policial responsável pela investigação dos delitos.

Para compreensão do cenário dos crimes cibernéticos, após investigação realizada por Leite (2018) por meio dos dados extraídos dos Armazéns de Segurança Pública, identificou-se significativo aumento dessa modalidade criminosa. Além disso, foram observadas alterações legislativas e o início de registros inéditos, como invasão de dispositivo informático.

Na pesquisa de Leite (2018), como proposição de protocolos de atuação em casos de crimes cibernéticos, sugeriu-se a adoção de duas linhas de ação concomitantes e complementares:

a gestão interinstitucional para a atualização da Diretriz Integrada de Ações e Operações (DIAO) e a criação de uma comissão interna para definir protocolos básicos de atuação. A DIAO, que norteia a atuação policial em casos específicos e está disponível para consulta no REDS, foi atualizada, assim como foram incluídos campos parametrizados no REDS.

Leite (2018) indicou que um percentual significativo dos crimes monitorados pela Coordenadoria Estadual de Combate aos Crimes Cibernéticos estava diretamente relacionado à falta de medidas de autoproteção por parte das vítimas. Esta dissertação relativiza essa questão ao analisar teorias de oportunidade e vitimização da criminologia junto com teorias pactualistas, que não eximem o Estado de sua responsabilidade de proteção ao cidadão.

Uma análise qualitativa realizada por meio de questionários com o público interno revelou diferenças geracionais entre policiais militares de Minas Gerais. Policiais da geração X apresentaram menor domínio de tecnologias em comparação com gerações mais jovens (Leite, 2018).

Outro dado relevante da pesquisa de campo foi que apenas 3% dos respondentes afirmaram possuir alto nível de conhecimento sobre crimes cibernéticos. Quando 49% dos respondentes, em uma amostra de 32.999 policiais, relataram baixo conhecimento conceitual sobre a modalidade criminosa, inferiu-se a necessidade de aprimoramento na Educação de Polícia Militar. Além disso, na simulação de um crime cibernético, 61% dos policiais forneceram respostas inadequadas sobre as primeiras ações a serem tomadas pela vítima, o que destaca a necessidade de definição institucional de estratégias preventivas e protocolos de atuação efetivos.

A pesquisa de Leite permite uma visão geral sobre o histórico de atualizações pela Polícia Militar em relação aos crimes digitais. Enquanto a pesquisa atual foca no crescimento do fenômeno, Leite abordou o surgimento de "uma nova criminalidade focada no ambiente conectado" (Leite, 2018, p.79), destacando fatores como o desenvolvimento tecnológico, pouca regulação da internet, analfabetismo digital e características geracionais.

Sobre a questão da legislação a partir de 2008, foi tratada a regulação da internet no Brasil, especialmente pelo Marco Civil da Internet (Lei n.º 12965/14), promulgada após outras legislações, como as Leis n.º 11829/08 e n.º 14737/12, que alteraram o Estatuto da Criança e do Adolescente e o Código Penal Brasileiro, respectivamente. Leite (2018) concluiu pela necessidade de investimentos em prevenção, dado que muitos crimes investigados poderiam ser evitados com medidas adequadas de autoproteção.

O Protocolo de Atuação produzido em 2018, como resultado da investigação no Curso de Especialização em Gestão Estratégica de Segurança Pública, iniciou-se com a questão de como tornar efetiva a atuação da Polícia Militar de Minas Gerais na prevenção e repressão aos crimes cibernéticos. Confirmou-se a hipótese de que a atuação da PMMG não era efetiva e foram desenvolvidas estratégias preventivas e protocolos de atuação, dos quais alguns foram implementados, como mudanças em sistemas informáticos e inclusão de diretrizes, embora insuficientes para o aumento significativo dos crimes cibernéticos nos anos subsequentes.

Egon Bittner (2003), um sociólogo e criminologista austríaco-americano, é conhecido por suas contribuições significativas para a compreensão das complexidades e desafios do trabalho policial. Sua obra "Aspectos do Trabalho Policial" de Egon Bittner (2003), oferece uma análise profunda sobre a natureza do policiamento e as tensões inerentes ao exercício dessa profissão.

Bittner argumenta que a atividade policial não se trata apenas da aplicação da lei, mas também envolve a manutenção da ordem social. Ressalta que os policiais frequentemente atuam como agentes de controle social, lidando com situações complexas e ambíguas nas quais as linhas entre o legal e o ilegal nem sempre são claras, o que permeia a fragilidade do

flagrante do estelionato digital. Destaca ainda a discrepância entre a abordagem legal e a aplicação da lei na prática (Bittner, 2003, p. 102).

O trabalho de Egon Bittner pode lançar luz sobre o aumento dos crimes patrimoniais cibernéticos e a técnica dos crimes de colarinho branco Ele argumenta que a atividade policial envolve uma série de tomadas de decisão complexas e, muitas vezes, ambíguas, pois no contexto dos crimes cibernéticos, essa complexidade é ampliada, já que os policiais enfrentam desafios para compreender a natureza técnica desses crimes e a falta de fronteiras físicas claras. No caso dos crimes patrimoniais cibernéticos, tal complexidade é exacerbada pela natureza técnica dos crimes. Os policiais são confrontados com desafios para compreender a dinâmica digital e a vastidão do ciberespaço, resultando em dificuldades na identificação e investigação desses crimes, além dos limites da técnica de policiamento preditivo tradicionais.

Poder-se-ia pensar, por vezes, na extrema colocação de policiais em rede não mais como indivíduos infiltrados, mas como verdadeiras Inteligências Artificiais que rastreassem os autores. Logicamente, embora existam tecnologias de Inteligência Artificial e protótipos de robôs, ainda não se conhece documentado até o término desse trabalho, tal experiência registrada pelas polícias mundiais. A ideia que mistura ser humano e máquina soa distante e bem semelhante à ficção científica, mas perfaz uma realidade próxima, indiciada pelo fenômeno social de abstenção de sentimentos e imparcialidade absolutamente legal que tem se buscado nas forças policiais.

De volta ao tangível e atual serviço policial, policiais e tecnologias atuam de forma integrada para a prevenção e repressão criminal, a exemplo dos GPS nas viaturas e aparelhos radiocomunicadores portáteis, computadores de bordo nas radiopatrulhas, aplicativos de consulta a bancos de dados, programas avançados de reconhecimento facial, câmeras de alta resolução e visão noturna em aeronaves policiais, até o uso de câmeras de corpo que transmitem a ação policial em tempo real, para além dos drones. Porém, nenhuma delas, embora possam estar atreladas ao fardamento, chega a ser parte do corpo ou da mente do policial, tal qual um chip implantado sob a pele ou uma IA policial lançada na rede.

O conceito de segurança pública precisa evoluir para incluir fatidicamente a proteção contra crimes cibernéticos patrimoniais, como o estelionato digital, ao lado das ameaças tradicionais. Essa abordagem deve ser multidisciplinar, envolvendo a colaboração entre governos, empresas de tecnologia, instituições financeiras e a sociedade civil, conceito de sociedade em rede tão instrínseco à gestão pensada em 2024. Além disso, não se nega que é essencial educar os cidadãos sobre os riscos cibernéticos e as práticas de segurança digital, para fins de reduzir a vulnerabilidade individual e coletiva, mas a atuação sobre a prevenção apenas sobre a ação da vítima não pode ser a única alternativa prática de atuação, haja vista a atuação necessária sobre o ambiente sem vigilância e também sobre o autor motivado, como importa a principal teoria sociológica adotada em Minas, qual seja, ambiental do crime.

Em última análise, o enfrentamento eficaz a essa tipologia de crimes requer uma abordagem multidisciplinar e colaborativa, pois envolve conhecimento técnico, investigativo e legal e até mesmo cultural-policial para desvendar práticas ilícitas complexas e garantir a mínima prestação de serviço.

3 OS ELEMENTOS CONSTITUTIVOS DE ELUCIDAÇÃO DO DELITO DE ESTELIONATO

3.1 O tratamento jurídico-normativo do delito de estelionato e sua configuração na atividade policial

No Brasil, o termo "estelionato" foi introduzido no Código Penal do Império em 1832, sendo descrito no artigo 264, que tratava de crimes contra a propriedade. O crime evoluiu no ordenamento jurídico brasileiro, para representar as mudanças sociais e tecnológicas ao longo do tempo. O estelionato, definido no artigo 171 do Código Penal Brasileiro, é um crime contra o patrimônio que se caracteriza pela obtenção de vantagem ilícita, induzindo ou mantendo alguém em erro, mediante ardil, artifício ou qualquer outro meio fraudulento.

O crime tem como elemento nuclear a fraude que significa a intenção deliberada de enganar a vítima para obter benefícios indevidos, e a pena prevista é de reclusão de um a cinco anos, além de multa. Observa-se que o tratamento jurídico do estelionato evoluiu com as recentes alterações legislativas que buscaram adequar a legislação às novas modalidades desse crime, impulsionadas pelo avanço tecnológico (Brasil, 1940).

Importa dizer que o pacote anticrime, por meio da Lei nº 14.155, de 27 de maio de 2021, trouxe importantes modificações para o artigo 171 do Código Penal como a tipificação específica do estelionato cometido mediante fraude eletrônica, incluindo-se fraudes praticadas pela internet, dispositivo eletrônico ou outros meios digitais. As mudanças incluíram o aumento da pena para “golpes” praticados com utilização de informações fornecidas pela vítima ou terceiros, induzidos a erro por meio de redes sociais, contatos telefônicos ou e-mails fraudulentos, e a qualificação de pena se o crime for praticado utilizando servidor mantido fora do território nacional (Brasil, 1940).

A popularização da internet e das redes sociais transformou a prática do estelionato. A internet, que teve origem na década de 1960 e se popularizou nos anos 1990 no Brasil, oferece novas plataformas, não para a prática de fraudes, mas predestinadas a esse fim.

Ocorre que as redes sociais como Facebook, Instagram e WhatsApp são frequentemente usadas para aplicar golpes, conforme as diversas cartilhas emitidas pelas polícias do Brasil, mas ainda há a necessidade de atualizar as técnicas de combate a esses crimes.

A cartilha publicada pela Polícia Civil de Minas Gerais apresenta uma análise mais detalhada sobre os principais golpes que têm vitimado a população, com ênfase em métodos de prevenção e estratégias de combate. O documento aborda algumas modalidades mais comuns, como os golpes por telefone, internet, e contatos presenciais (Minas Gerais, 2022) [10].

Não se trata de transferir ao particular a responsabilidade, mas de atuar preventivamente sobre um dos fatores do delito, para tanto, a cartilha sugere práticas de autoproteção, como a verificação de fontes de informação, a não divulgação de dados pessoais a terceiros desconhecidos, a cautela ao realizar transações financeiras *online*, a famosa verificação em dois fatores, dentre outros (Brasil, 2022, p. 11). Trata ainda da necessidade de colaboração entre cidadãos e autoridades, para fomentar a denúncia de atividades suspeitas.

Quanto à atuação policial no enfrentamento ao estelionato, as agências passam por uma fase de adaptação das estratégias tradicionais de policiamento às novas modalidades do crime. A Polícia Militar de Minas Gerais (PMMG), por exemplo, tem desenvolvido e aprimorado estratégias específicas para enfrentar o estelionato digital, como destaca a pesquisa de Alexandre Junqueira Herculano sobre os impactos da internet para a prática do crime de estelionato. Cita-se no trabalho que na PMMG *tem investido em treinamento e capacitação de seus agentes para lidar com crimes cibernéticos. Isso inclui a criação de unidades especializadas, como o Grupo de Combate aos Crimes Cibernéticos* (GCCC), que atua na investigação e repressão de delitos cometidos no ambiente digital (Junqueira, 2022, p. 66).

O Sistema de Registro de Eventos de Defesa Social (REDS) é utilizado em Minas pela PMMG, PCMG, CBMMG para registrar esses crimes, embora tenha limitações quanto à análise da especificidade dos termos usados para descrever os meios de fraude, ou seja, cada golpe, a não ser que seja analisado registro a registro pelo histórico. As análises foram

10 - Disponível em: https://www.policiacivil.mg.gov.br/pagina/servico-cartilhas-pcmg.

realizadas nesta pesquisa, e o monitoramento é realizado hodiernamente, além da pesquisa identificada junto ao centro de Pesquisa e Pós-Graduação da PMMG elaborada por Herculano (2022). Ambos os dados e análises demostram e coadunam um aumento nos crimes de estelionato cometidos por meio eletrônico (internet ou SMS) de 2018 a 2022.

Conclui-se, pois, que no atual cenário, a PMMG e a PCMG têm adotado estratégias para enfrentar o estelionato, pois, a despeito do início da pesquisa em 2022, o delito já foi identificado como um *outlier* (ponto fora da curva na estatística). Algumas ações como as campanhas educativas pelos responsáveis preventivos (PMMG) para alertar a população sobre os golpes mais comuns e como se proteger, treinamento e capacitação dos agentes investigadores para lidar com crimes cibernéticos específicos, algumas cooperações interinstitucionais também foram observadas nas agências (Herculano, 2022, p. 67), além da atualização dos programas e do uso de inteligência artificial para integrar sistemas de registro de ocorrência que melhoraram a análise de dados e a formulação de estratégias, bem como a abertura dos dados para análise por todos os agentes, situação importante para percepção do fenômeno criminal pelas forças públicas.

Apesar dos avanços, o enfrentamento ao estelionato digital enfrenta desafios significativos, como o fator de as medidas aplicadas estarem focadas na vítima e a dificuldade de identificação e localização dos criminosos, que muitas vezes operam de fora do país ou com ocultação de IP[11]. A natureza anônima da internet e a rápida evolução das tecnologias utilizadas pelos criminosos exigem uma constante atualização das técnicas investigativas e uma maior cooperação interestadual.

Ainda sobre a análise científica de Herculano (2022, p. 43), que realizou apanhado histórico e o estudo de diversos temas fundantes para a temática ora trabalhada, identificou-se a sistemática organização em Quadros das figuras típicas de estelionato no Brasil:

11- Disponível em: https://www.kaspersky.com.br/resource-center/definitions/what-is-an-ip-address

Quadro 1 – Quadro de autoria do autor Herculano (2022)

Ordenaçãopenal	**Previsão**
Código Penalde 1832 (1832 –1890)	Art. 264. Julgar-se-ha crime de estellionato: 1º A alheação de bens alheios como próprios, ou a troca das cousas, que se deverem entregar por outras diversas. 2º A alheação, locação, aforamento, ou arrentamento da cousa própria jáalheada, locada, aforada, ou arrentada á outrem. 3º A hypotheca especial da mesma cousa á diversas pessoas, não chegando oseu valor para pagamento de todos os credores hypothecarios. 4º Em geral todo e, qualquer artifício fraudulento, pelo qual se obtenha de outrem toda a sua fortuna ou parte della, ou quaesquer títulos.
Código Penal de1890 (1890–1932)	Art. 338: Julgar-se-á crime de estelionato: 1° - alhear a coisa alheia como própria, ou trocar por outras coisas, que se deverem entregar; 2º - alhear, locar ou aforar a coisa propria já alheada, locada ou aforada; 3º - dar em caução, penhor, ou hipoteca, bens que não puderem ser alienados;4º- alhear os objetos dados em penhor agrícola, sem consentimento do credor, ou por qualquer modo defraudar a garantia pignoratícia;5º - usar de artifícios para surprehender a boa fé de outrem, iludir sua vigilancia, ou ganhar-lhe a confiança; e, induzindo-o a erro ou engano por esses e outros meios astuciosos, procurar para si lucro ou proveito; 6º - abusar de papel com assignatura em branco, de que se tenha apossado, ou lhe haja sido confiado com obrigação de restituir ou fazer delle uso determinado, e nelleescrever ou fazer escrever um acto, que produza effeito jurídico em prejuizo daquelle que o firmou; 7º - abusar, em proprio ou alheio proveito, das paixões ou inexperiência de menor, interdicto, ou incapaz, e fazei-o subscrever acto que importe effeito jurídico em damno delle ou de outrem, não obstante a nulidade do acto emanada da incapacidade pessoal; 8º - usar de falso nome, falsos títulos ou de qualquer ardil para persuadir a existencia de empresas, bens, credito, influencia e supposto poder e por esses meios induzir alguém a entrar em negócios, ou especulações, tirandopara si qualquer proveito, ou locupletando-se da jactura alheia; 9º- usar de qualquer fraude para constituir outra pessoa em obrigação, que nãotiver em vista, ou não puder satisfazer ou cumprir; 10º - fingir-se ministro de qualquer confissão religiosa e exercer as funcções respectivas para obter de outrem dinheiro ou utilidade; 11º - alterar a qualidade e o peso dos metaes nas obraas que lhe forem encomendadas; substituir pedras verdadeiras por falsas, ou por outras de valor inferior; vender pedras falsas por finas, ou vender com ouro ou prata, ouqualquer metal fino,objectos de diversa qualidade. Penas – de prisão cellular por um a quatro annos e multa de 5 a 20% do valor do objecto sobre que recahir o crime. Paragrapho único. Se o crime de número 6 deste artigo fôr cometido por pessoa a quem o papel houvesse sido confiado em razão do emprego ou profissão, ás penas impostas se accrescentará a de privação do exercício da profissão, ou suspensão do emprego, por tempo igual ao da condemnação.
Ordenação penal vigente	**Previsão**
Consolidaçãodas leis penais. (1932 - 1940)	(Acrescenta o parágrafo segundo ao art. 338 do Código Penal de 1890) § 2º Incorrerá nas penas de prisão cellular por um a quatro anos aquelle que fraudulentamente emittir cheque, sem ter sufficiente provisão de fundos em poder do saccado, além da multa de 10% sobre o respectivo montante.

Código Penalde 1940	Art. 171 (atual)

Fonte: Herculano (2022)

Percebe-se que o tratamento jurídico-normativo do estelionato no Brasil passou por modificações para se adequar ao fato social de cada época, o que permite inferir reflexão sobre as mudanças sociais e tecnológicas. Ocorre que, embora a adaptação das normas jurídicas ocorra após a evolução da sociedade (Faria, 2024).

A atuação contínua da polícia finda por perceber a mudança social de antemão, haja vista o contato com os problemas sociais e, atualmente, registros de ocorrências. No entanto, conforme determina o Estado Democrático de Direito, a atuação da atividade policial está estritamente condicionada às atuações legislativas, para respeito ao princípio da legalidade penal e administrativa. Nesse ínterim, a capacitação, que muitas vezes é exposta como fator inicial, na práxis se apresenta como último fator a ser pensado na tríade: novo fato social, que por sua vez demanda atuação policial; mudanças legislativas; treinamento policial pautado na alteração legislativa, que será tratado adiante (Santos, 2024).

As alterações do tratamento jurídico pela legislação são frequentes, como exposto no Quadro 1. Por sua vez, Luciano Cirino dos Santos, demonstra em sua dissertação “A fraude como elemento essencial para a configuração da tipicidade objetiva dos crimes contra a ordem tributária praticados por particulares” publicada em 2024, a exposição da dificuldade de identificação e delineamento do conceito de fraude:

> Na literatura jurídica brasileira existem raríssimas produções científicas de fôlego destinadas especificamente ao estudo da fraude penal. Normalmente, o tema é abordado, en passant, quando a doutrina nacional expõe, nos cursos de direito penal relativos à parte especial do Código Penal, o crime de estelionato previsto em seu art. 171. Entre nós, um desses raros estudos destinados à fraude penal foi o realizado por Nelson Hungria, em 1932, por ocasião do concurso que prestou "para a livre docência na cadeira de direito penal da Faculdade de Direito da Universidade do Rio de Janeiro". Conforme ressalta o próprio autor, o opúsculo foi originalmente publicado en 1932 e, posteriormente, republicado em 1934 "com alguns acréscimos e pequenas correções". Todavia, há que se dizer que até mesmo o estudo de Nelson Hungria - tradicionalmente citado pelos autores nacionais, inclusive os contemporâneos - também se encontra impregnado do objetivo de **analisar a fraude no contexto do crime de estelionato**. O antigo estudo de Nelson Hungria tem sido pano de fundo da nossa discussão doutrinária em torno da fraude penal. Basta manusear a literatura especializada

> nacional para perceber que as lições lançadas por Hungria há quase um século - ainda sob a vigência do Código Penal de 1890 (e reiteradas sob a vigência do Código Penal de 1940) - continuam sendo repetidas como se fossem um mantra. Os autores que apontam a fonte das lições que repetem, quando não indicam a obra específica de Nelson Hungria (publicada ainda sob a vigência do Código Penal de 1890), fazem referência ao volume VII do tratado intitulado Comentários ao Código Penal (publicado já sob a vigência do Código Penal de 1940), onde o tema é novamente analisado por Hungria - mediante exposição sintética do conteúdo de seu livro Fraude Penal - no contexto do Capítulo VI ("Do estelionato e outras fraudes") do Título II ("Dos crimes contra o patrimônio") da Parte Especial do Código Penal de 1940 (DL 2.848/40) (Santos, 2024; Grifo nosso).

Conforme bem citado por Santos (2024), as atuais referências e estudos sobre fraude remetem repetitivamente ainda à Nelson Hungria, renomado jurista brasileiro do século passado, que abordou a relação entre fraude e criminalidade como um refinamento da conduta ilícita no século XX, de modo que à época destacou que a fraude, ao contrário do roubo violento, representaria uma mudança na forma como os crimes patrimoniais estavam sendo cometidos, tal qual se observa atualmente quando do estudo da teoria da migração. Segundo Hungria, a sociedade moderna favoreceu o crescimento da fraude, substituindo a violência explícita por ações mais sutis e intelectuais, como o estelionato, que se tornou a forma predominante de lesão patrimonial (Hungria; Dotti, 2017, art. 155-196), o que permite inferir que o fenômeno apenas está se repetindo, e não inovando na ordem jurídica, pois trata-se apenas de novos meios de execução e engendramento.

Não obstante a importância da obra fundante, breves considerações carecem de ser feitas, porque Hungria explora as várias acepções da palavra "fraude", afirmando que esta é a antítese da violência. Dada vênia, percebe-se que o que se fez foi a comparação com os crimes violentos da época, análise objetiva e ainda hoje realizada pelas agências, no entanto, a despeito da práxis e da dogmática, a dedução imprescinde de se tornar indução, pois por meio da dialética e da teoria da complexidade de Morin, que demonstra que todas as coisas estão em rede e interligadas, é possível argumentar que o fenômeno atual resulta em criminalidade violenta, ao fornecer poder aquisitivo às organizações criminosas e alimentar a permanência da vantagem econômica dessas ORCRIMS paralelamente ao Estado.

Importa dizer que Hungria demonstrou de forma exime que, juridicamente, a fraude se confunde com o dolo contratual e constitui uma parte essencial do estelionato, o que o leva a distinção entre fraude penal e fraude civil e a sua busca em demonstrar, ainda em 1955, a

existência de uma diferenciação clara entre as fraudes em cada esfera. De forma brilhante, conclui que a distinção entre ilícitos civis e penais não é científica, mas sim uma conveniência política que varia conforme o tempo e o espaço, o que explica a atual expansão do Direito Penal na era da informação e da tecnologia. Sobre a análise de Santos (2024):

> O opúsculo de Nelson Hungria, na tentativa de estabelecer uma relação entre fraude e criminalidade, é iniciado com afirmação de que a fraude seria um **refinamento da conduta ilícita do homem moderno ao investir contra o patrimônio alheio**, constituindo - em sua visão lançada no início da década de 1930 - a forma predominante do crime patrimonial.Nelson Hungria enxergava "o ladrão violento" como "um retardatário ou um fenômeno. Consequentemente, salientando que a luta pelo sustento avançava predominantemente pela ação intelectual e que o Não mais o assalto brutal e cruento, mas a blandícia vulpiana, o enredo sutil, a aracnídea urdidura, a trapaça, a mistificação, o embuste. O latrocínio, a grassatio e a rapina foram sub-rogados pelo enliço, pela artimanha, pelo estelionato. A mão armada evoluiu para o conto do vigário. O trabuco e o punhal, que sublinhavam o sinistro dilema "a bolsa ou a vida", foram substituídos por um jogo de inteligência. O leão rompente fez-se raposa matreira. Na concepção de Nelson Hungria, a fraude, sob certo ângulo e em certa medida, deveria ser considerada "**como forma de uma - criminalidade evolutiva, em contraposição a uma criminalidade atávica, cuja característica seria a violência** ou - invocando Ferri - "como um atestado da evolução pela qual o homem tende incessantemente a distanciar-se de sua origem animal ou selvagem". Disso, Nelson Hungria salienta que a fraude não é um produto original do estado atual da civilização, posto que "**o ambiente social moderno apenas tem favorecido o primado ou a maior viabilidade da fraude**" tornando o homem "gradativamente menos propicio à violência", consequentemente, a **fraude seria apenas uma das muitas expressões "do instinto do menor esforço na luta pela existência** dessa forma, a **fraude seria "de todos os tempos**" (Santos, 2024).

De volta à Teoria Geral do Direito e ao "Novo Fato Social", que por sua vez demanda atuação policial e só então ocorre o apelo aos representantes para a mudança legislativa e, o último passo se dá com o treinamento e aperfeiçoamento policial pautado na alteração legislativa, é fundamental para identificar e desmantelar redes de fraude a capacitação contínua dos policiais, principalmente para acompanhar as novas tecnologias e os métodos utilizados pelos criminosos, bem como realizar o que já vêm sendo feito, no caso da cooperação com outras agências e o esclarecimento dos riscos para a comunidade por meio das cartilhas. No entanto, não se trata de desmerecer as propostas de treinamento de pessoal, mas de incrementar a atuação da gestão, pois a complexidade das fraudes exige uma abordagem multifacetada, perpassando a proteção preventiva das vítimas e a punição adequada dos infratores para diminuição da sensação de impunibilidade, de modo que estes deveriam ser objetivos centrais das políticas de segurança pública no contexto atual.

Quanto ao treinamento para atuação policial em si, atualmente, no enfrentamento ao estelionato, é sobremaneira desafiadora, ainda após a alteração legislativa, devido à natureza sofisticada e variada das fraudes envolvidas. As técnicas de investigação precisam ser apuradas e adaptadas às diferentes modalidades de estelionato, que podem envolver desde golpes simples, como falsas promessas de emprego, até complexos esquemas financeiros, ocorre que a vultuosidade de ocorrência dos delitos não é plausível de absorvição pela estrutura atual investigativa, o que carece de atenção gestacional ao fenômeno, que pode ter como hipótese de solução a presença preventiva do guardião no ambiente virtual.

Se o Direito Penal percebeu em 1955 o que atualmente é denominada Teoria da Migração ou da Escolha Racional do Delito, o tratamento jurídico-normativo do delito de estelionato também foi identificado como de conceito amplo de fraude, como a bem citada criatividade e mudança racional do criminoso percebida por Hungria. Tais abordagens, embora esclarecedoras da história cíclica, não são suficientes para os ditames da sua configuração da atividade policial no mundo complexo e em rede do século XXI, em que organizações criminosas especializam-se em delitos cibernéticos e em golpes virtuais, praticam delitos desterritorializados, rompem fronteiras e arquitetam impunidade pelos limites da burocracia formal de atuação policial, que precisa passar a ser presente no ambiente digital se objetiva a manutenção do estado contratualista.

3.2 Engenharia social e o delito de estelionato digital

O conceito de Engenharia Social refere-se à utilização de manipulação intencional de indivíduos em conflito com as leis e éticas sociais para obter vantagens indevidas, dados ou informações, conforme a Secretaria de Gestão e Ensino em Segurança Pública do Ministério da Justiça (Brasil, 2020, p. 15). Afirma a Secretaria que a Engenharia Social ocorre tanto em contextos cibernéticos quanto físicos, por meio do engano e ocultação dos objetivos reais. Tal situação se assemelha, mas não deve se confundir, com o delito de estelionato em si, que possui fim específico previsto no artigo 171 de obtenção de vantagem patrimonial indevida,

de modo que o patrimônio é implícito ao objeto jurído tutelado pelo tipo e capítulo do Código Penal, pois o tipo apenas cita vantagem ilícita:

> Art. 171 - **Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento**: Pena - reclusão, de um a cinco anos, e multa, de quinhentos mil réis a dez contos de réis (Brasil, 1940; Grifo nosso).

No campo da cibersegurança, a Engenharia Social é definida como o uso de truques psicológicos por *hackers* para obter informações necessárias para acessar sistemas de computador. No entanto, percebe-se que a prática de enganar pelos meios digitais com contato direto e não pelos sistemas, seja por telefone, sites, redes sociais diversas e plataformas de vendas, tem demonstrado atingir os mesmos efeitos e até mais gravosos que o uso isolado de vulnerabilidades de sistemas de computação, pois neste último a intenção comum é violar a segurança, enquanto no fenômeno atual observa-se a a clara intenção de obtenção de vantagem patrimonial. Ainda sobre o conceito de Engenharia Social, o site tratado na introdução, Kaspersky, define que:

> **A Engenharia Social é uma técnica de manipulação que explora erros humanos para obter informações privadas, acessos ou coisas de valor**. No crime cibernético, esses **golpes de "hacking humano"** tendem a atrair usuários desavisados para expor dados, espalhar infecções por malware ou dar acesso a sistemas restritos. Os ataques podem acontecer on-line, em pessoa e por outros meios de interação. Os golpes promovidos com base em Engenharia Social são feitos a **partir de como as pessoas pensam e agem**. Sendo assim, os ataques de Engenharia Social são especialmente úteis para **manipular o comportamento de um usuário**. Quando um invasor entende o que motiva as ações de um usuário, ele pode enganar e manipular o usuário de forma eficaz.
>
> Além disso, os *hackers* tentam explorar a **falta de conhecimento do usuário**. Graças à velocidade da tecnologia, muitos consumidores e funcionários não **reconhecem certas ameaças** como os downloads automáticos. Os usuários podem também não perceber a verdadeiro **valor dos dados pessoais**, como o seu número do telefone, por exemplo. Por isso, muitos usuários não sabem exatamente como proteger a si mesmo e seus dados.
>
> Em geral, os invasores de Engenharia Social têm um dos seguintes objetivos:
>
> 1. Sabotagem: interrupção ou corrupção de dados para causar danos ou incômodos.
> 2. Roubo: obtenção de objetos de valor, como informações, acesso ou dinheiro[12].

O termo "Engenharia Social" tem sido utilizado então para descrever técnicas de golpe no âmbito da tecnologia, sendo uma intrusão não técnica e que depende da interação humana.

12 - Disponível em: https://www.kaspersky.com.br/resource-center/definitions/what-is-social-engineering, acesso em 10Jul2024.

De acordo com Mitnick e Simon (2003), no livro "A Arte de Enganar", destacam que engenheiros sociais induzem pessoas a violar procedimentos normais de segurança para obter credenciais e informações sigilosas para fins ilícitos. Esses criminosos são de perfis diversos, dentre os quais cita-se os estelionatários, ex-funcionários descontentes, terroristas ou iniciantes no *hacking*, motivados por interesses financeiros, poder, ideologia, vingança, curiosidade ou maldade. No presente enfoque, torna-se mais relevante os indivíduos motivados por interesses financeiros.

Na prática, os ataques de Engenharia Social podem ser realizados de muitas maneiras, tanto tecnológicas quanto humanas, mas, especificamente nos que envolvem tecnologia, o usuário acredita que interage com um sistema ou um pessoal real, e divulga informações confidenciais. Seria semelhante ao erro de tipo estudado pelo Direito, no que tange à uma falsa percepção da realidade, mas nesse caso não pelo autor, mas sim pela vítima. Conclui-se o que se pode chamar de erro de tipo às avessas, termo produto dessa pesquisa e possível análise pelo legislativo no que tange à possível alteração do tipo, orientada pelo Direito Penal com enfoque na vítima e que poderia, como forma de tutela em processo criminal, declarar o erro de tipo em um delito que não se tem a identidade do autor sem demorada investigação, além de ser esta investigação condicionada à representação da vítima (representar contra quem?), e sem disponibilidade das agências de atender tamanha demanda dos atos investigativos. O novo inciso, após acurado estudo, deveria declarar de imediato o vício de percepção de realidade da vítima, anular o negócio jurídico, bloquear e cancelar de imediato todas as transações financeiras realizadas pela vítima e esse ato processual liminar seria aplicado já pela autoridade policial, para além das burocracias clássicas dos imites de competência e de acordo com as novas vertentes de sociedade em rede e problemas complexos, sem prejuízo da análise definitiva judicial.

A despeito do estudo de Hungria e a diferenciação do dolo e do erro no negócio jurídico e do dolo para o estelionato, sabe-se que o Processo Civil prevê tais institutos de tutela antecipada de urgência e emergência, mas que, devido ao acesso à justiça, ainda que haja a ampliação da atuação dos órgãos garantidores, não seria tão fácil atender aos bloqueios das contas com celeridade a tempo de salvaguardar a não transferência ou saque dos valores até a tutela. Os poucos casos em que são alcançados tais bloqueios se dão por escritórios de

advocacia especializados e de alto valor de pagamento de honorários, o que também não garante o acesso do serviço para sociedade.

Na abordagem humana, presencial ou não, os ataques exploram respostas previsíveis a gatilhos psicológicos. A extensão desses ataques é limitada apenas pela criatividade do *hacker* ou dos golpistas, portanto, há a necessidade de novas estratégias de segurança para mitigar esses riscos.

Se, no contexto das fraudes eletrônicas, a Engenharia Social é uma ferramenta utilizada por criminosos para explorar vulnerabilidades humanas e tecnológicas, as agências carecem de aperfeiçoar as estratégias de prevenção e mitigação pensadas especificamente para o fenômeno ora desmistificado.

Nesse ínterim, a obra sobre Detecção de Fraudes Eletrônicas em Período de Crise aduz diversos conceitos, casos práticos e as estratégias usadas pelos criminosos para explorar as vítimas (Brasil, 2020, p. 22). Sobre os conceitos, fez-se necessário estruturar objetivamente para detalhar os diferentes tipos de fraudes eletrônicas, bem como tradução livre para fins de melhor entendimento:

Quadro 2 - Tipos de fraudes eletrônicas

Classificação	**Descrição**
1. *Phishing* (Fraude Eletrônica)	Método comum onde o atacante se passa por uma entidade confiável para enganar a vítima e obter informações sensíveis, como senhas e dados bancários.
2. *Spear Phishing* (Fraude Eletrônica Direcionada)	Forma mais sofisticada de phishing, onde o ataque é direcionado a um indivíduo ou organização específica, utilizando informações personalizadas para aumentar a eficácia do golpe.
3. *Pretexting* (Pretextação)	Envolve a criação de um cenário falso (pretexto) para enganar a vítima e induzi-la a fornecer informações confidenciais. Um exemplo clássico é um atacante que se passa por um funcionário do suporte técnico.

4. *Baiting* (Isca)	Utiliza uma isca, como um dispositivo de armazenamento infectado ou um anúncio atrativo, para enganar a vítima e induzi-la a comprometer seu sistema ou informações pessoais.
5. *Quid Pro* Quo (Troca)	Oferece algo em troca de informações, como um serviço técnico gratuito em troca de acesso ao sistema da vítima, mantendo em erro a vítima.

Fonte: Produzidos pela autora

Ao contrário dos ataques técnicos que exploram falhas em sistemas computacionais, como já citado a respeito dos *downloads* com vulnerabilidades, como os cavalos de tróia, a Engenharia Social foca nas fraquezas humanas, como a curiosidade, a confiança e o medo, então pode-se concluir que precisam da interação com o ser humano, e essa é a principal característica diferencial entre o crime cibernético essencial e o acidental, que se utiliza de meios digitais. O pouco que se pode pesquisar sobre o perfil dos autores, em decorrência da limitação da informação dos autores nos registros policiais por causa da desterritorialização e da anonimidade, provém das afirmações do Ministério da Justiça (Brasil, 2020, p. 15):

> Aos criminosos, que usam técnicas de Engenharia Social para obtenção de credenciais personalíssimas e informações sigilosas para fins ilícitos, é dado o nome "engenheiros sociais". **O perfil deste tipo de delinquente é variante, afastando-se o estereótipo de que se trata sempre de profissionais da tecnologia mal-intencionados.**
>
> O que se deve levar em conta nesta seara, é que a atuação de um indivíduo no universo criminológico cibernético resulta de motivações diversas, as quais podem ser arroladas como: **interesse financeiro, poder, ideologia, instinto de vingança, curiosidade e até a pura maldade. Admite-se, assim, que engenheiros sociais podem ser estelionatários**, ex-funcionários descontentes de uma organização, terroristas, fanáticos de toda natureza ou iniciantes do mundo hacking (Grifo nosso).

Identificado o problema, torna-se essencial implementar estratégias de prevenção e mitigação que abordem tanto a dimensão técnica quanto a humana da segurança. As campanhas de conscientização e treinamentos regulares podem aumentar a resistência às tentativas de fraude, mas sozinhas não atingem os resultados pretendidos. Estabelecer e reforçar políticas de segurança claras que regulam o uso de sistemas de informação e a manipulação de dados sensíveis, tal qual o fez a Lei Geral de Proteção de Dados, pode reduzir a exposição aos riscos. No Brasil, o site Cert.br cuida e monitora dessas diretrizes para verificar a autenticidade de solicitações e a utilização de procedimentos seguros, mas, no que tange à aplicabilidade para as agências, na atuação preventiva é incentivar aos

cidadãos implementarem tecnologias simples como filtros de e-mail, autenticação multifatorial e sistemas de detecção de intrusão, que podem ajudar a identificar e bloquear tentativas de Engenharia Social ciber, mas não especificamente as humanas. A esse respeito, o Ministério da Justiça (Brasil, 2020, p. 16-17):

> Em grande parte desses ataques praticados por *hackers* contam com **vulnerabilidades deixadas nos sistemas alvo**. Estruturas lógicas de bancos de dados e soluções de plataformas desenvolvidas pelas corporações podem deixar falhas quando programadas. É evidente que já se detecta neste contexto a **falibilidade humana**, que pode ser de toda uma equipe de desenvolvimento, mas extensível a outras relacionadas a **qualidade de *software* e até segurança,** considerando a interdependência dessas áreas nos modelos atuais.
>
> Mas o que se chama a atenção no contexto deste capítulo é a **participação humana nos incidentes de segurança como usuário**. Assim como ocorre no exemplo da segurança predial, no ambiente digital, a contribuição das pessoas para a ocorrência de sinistros é extremamente relevante, razão pela qual sempre são estabelecidos regras e protocolos a ser observados. **Historicamente, a maioria das técnicas desenvolvidas para combater os ataques à segurança concentrava-se em colocar "barricadas virtuais" em torno dos sistemas**, tentando impedir que um indivíduo indesejado obtivesse acesso aos recursos. **Porém, verificou-se que tamanho investimento não surtia efeitos, pois os elos mais fracos de todas as defesas de segurança das organizações, na maioria das vezes, foram seus funcionários**.
>
> De fato, o ideal da segurança impenetrável nunca pôde ser alcançado, muito menos quando **se tenta impedir ataques em um nível técnico e não se preocupando com o nível físico-social**. A ignorância desse elemento social vital sempre forneceu aos *hackers* um método fácil para obter acesso a um sistema privado.
>
> Em suma, toda a preocupação ora apresentada com o **usuário** serve para demonstrar o quão este é classificado **como ponto de preocupação em qualquer sistema.** Isto se explica por causa de seu c**omportamento previsível e outros aspectos psicológicos**, o que acaba sendo **frequentemente explorado por pretensos invasores** (Grifo nosso).

De igual modo, o Ministério da Justiça e Segurança Pública trabalha tal exploração das vulnerabilidades humanas, resumidas no contexto da Engenharia Social como a capacidade dos autores de explorar as vulnerabilidades humanas, e que podem ser categorizadas em três principais áreas:

Quadro 3 - Áreas de vulnerabilidade

Área de Vulnerabilidade	**Descrição**
1. Confiança e Autoridade	Criminosos frequentemente se passam por figuras de autoridade ou entidades confiáveis para induzir a vítima a obedecer a suas instruções sem questionamento.

2. Curiosidade e Medo	A curiosidade humana e o medo são emoções poderosas que podem ser exploradas. Mensagens que despertam curiosidade (por exemplo, um e-mail com um assunto intrigante) ou medo (como uma suposta violação de segurança) são eficazes para induzir a vítima a agir impulsivamente.
3. Urgência e Pressão	Criar um senso de urgência ou pressão pode levar a vítima a tomar decisões precipitadas. Mensagens que exigem uma ação imediata para evitar consequências negativas são comuns em ataques de Engenharia Social.

Fonte: Produzidos pela autora

Conclui-se que o tema Engenharia Social ainda é pouco trabalhada pelo Direito e pela Tecnologia da Informação, mas ainda sim representa notável diferenciação dentro do universo de delitos cibernéticos, e um desafio significativo para a segurança pública da informação, se é que se pode assim defini-la após o artigo 5º inserir no rol de direitos fundamentais a proteção de dados, principalmente porque pela Engenharia Social ocorre a capacidade de explorar as fraquezas humanas e as digitais simultaneamente. A combinação de educação, políticas robustas e tecnologias avançadas mitiga os riscos, bem como a conscientização, mas no que tange ao psicológico humano, não há ainda solução prática ou simples identificada como plausível defesa contra as técnicas sofisticadas de Engenharia Social na sociedade em rede.

3.3 Métodos policiais de análise criminal: polícia preditiva e novas premissas para o delito desterritorializado

As técnicas de análise preditiva utilizadas pela polícia incluem a análise de dados históricos, como registros de crimes anteriores, dados demográficos, informações sobre infraestrutura urbana e outras variáveis relevantes. Esses dados são alimentados em algoritmos, que usam técnicas estatísticas e de aprendizado de máquina para identificar padrões e tendências. Por exemplo, por meio da análise de gráficos produzidos neste trabalho poder-se-ia concluir que o maior número de delitos ocorre nas capitais possivelmente devido ao maior fluxo de pessoas, movimentações financeiras digitais e maior uso de aparelhos celulares e sinais, mas, com o fenômeno da cidade sem muros, não se pode predizer que permanecerão nesses locais, pois os autores de tais crimes podem estar em qualquer lugar do globo terrestre.

Se não forem utilizadas técnicas de rastreamentos – como já utilizam as Delegacias Ciber e os Grupos de Inteligência de Órgãos Investigativos Policiais ou Ministeriais, nada efetivo poderá ser feito e carece de reiteração que o efetivo e investimento nesses órgãos é infinitamente menor que nos demais. Com o crime transeunte e materialístico, parece mais lógico que com base nas análises realizadas, a polícia possa implementar estratégias proativas, como o aumento do patrulhamento em áreas identificadas como de alto risco, a alocação de recursos em determinados locais e horários, e a implementação de programas de prevenção do crime direcionados. Essas ações têm como objetivo prevenir a ocorrência de crimes, bem como melhorar a resposta e a eficiência das forças policiais, mas com os crimes instranseuntes, ou seja, que não deixam vestígios, ou com os imateriais, formais ou de mera conduta, sem resultado físico no mundo real, não se torna tão oportuno o lançamento de policiamento ou técnicas de investigação tradicionais. A despeito da ideia de anonimato, agora fortalecida:

> Jacobs em 1961 destacava os ecossistemas urbanos compostos por processos físicos, econômicos e éticos, em que a diversidade e a interdependência cumpririam a função de revitalização e controle. O problema da segurança nas grandes cidades estaria diretamente relacionado ao enfraquecimento dos mecanismos habituais de controle exercidos naturalmente pelas pessoas que vivem nos espaços urbanos. A partir daí, perspectivas de intervenção ambiental passaram a incorporar conceitos como o de "espaço defensivo" (Newman, 1972) ou de "prevenção de crime através do design ambiental" (Jeffery, 1971). A ideia de espaço defensivo relaciona-se a soluções arquitetônicas de recuperação de moradias públicas nos Estados Unidos, obrigando seus moradores a exercer seus naturais instintos de "territorialidade". Este instinto é perdido quando se constroem grandes prédios de habitação coletiva, em que os moradores mal se conhecem, e onde existe uma variedade enorme de acessos não supervisionados que facilitam a atividade de predadores. A ideia é reduzir esse anonimato não apenas pelo incremento da vigilância natural, mas também diminuindo as vias de escape para potenciais ofensores (Beato *et al*, 2004).

A função preditiva da polícia tradicional advém da ideia de policiamento de *hotspots*, adiante tratado, mas, no presente trabalho o que se propõe por intermédio do uso da IA levanta questões éticas e de privacidade, como o uso de grandes bancos de dados pessoais, o potencial de discriminação e preconceito nos algoritmos e a necessidade de garantir a transparência e a responsabilidade no uso dessas tecnologias, sem afetar o sigilo no que for imprescindível à ordem pública (Faria, Michalick, 2024, p. 79-80).

> Várias técnicas de mapeamento diferentes são usadas para identificar **pontos críticos de crime** - mapeamento de pontos, mapeamento temático de áreas geográficas, elipses espaciais, mapeamento temático de grade e estimativa de densidade do kernel. Vários estudos de pesquisa discutiram o uso desses métodos para **identificar focos de crime**, geralmente com base em sua facilidade de uso e capacidade de interpretar espacialmente a localização, tamanho, forma e orientação de grupos de incidentes de crime.
>
> Identificar os hot spots é o primeiro passo que uma agência de policiamento precisa dar ao discernir onde melhor priorizar seus recursos. A tentativa de fazer isso por meio de mapeamento de pontos tornou-se desatualizada desde a proliferação do *software* de Sistemas de Informação Geográfica (SIG) e a crescente sofisticação das técnicas de mapeamento (Chainey;Tompson;Uhlig,2008).

O mapeamento criminal se fundamenta, até então, nos pontos quentes críticos de crime, na compreensão de que o crime possui uma natureza intrinsecamente geográfica e não ocorre de maneira aleatória no espaço, percebido também pelas teorias da criminologia da escolha racial e as ambientais. Ocorre que, por longos anos, foi possível se entender a dinâmica criminal em um contexto social, pois revelava-se por meio da interpretação dos dados pelos analistas como o ambiente, as condições locais e a interação dos indivíduos com o espaço influenciavam na ocorrência de delitos. Reconhecer a importância da localização e do espaço no fenômeno criminal permite que políticas públicas sejam melhor direcionadas, aumentando a eficácia das intervenções, desde a colocação de uma viatura em local estratégico de repetitivos índices, como nas investigações de grupos interligados de regiões diversas.

Como bem citado por Faria e Michalick (2024, p. 80), o fenômeno criminal é composto por quatro dimensões fundamentais: a lei, o ofensor, o alvo e o lugar. Esses elementos são interdependentes, e, na perspectiva do mundo físico, a ausência de qualquer um deles inviabiliza a ocorrência de um crime. A lei é o primeiro elemento, pois sem ela não há como definir um ato como criminoso. O ofensor, por sua vez, é o indivíduo primeiramente motivado e que, ao violar a lei, se torna o autor do crime. O alvo é a pessoa ou propriedade que sofre a violação, sendo essencial para que o crime se concretize. Finalmente, o lugar é o espaço físico onde o crime ocorre, e sua importância reside na forma como ele pode facilitar ou dificultar a ação criminosa, mas, na perspectiva do mundo virtual, a ausência do espaço físico não inviabiliza a ocorrência do crime, o que induz a algumas diferenciações sobre o espaço.

O lugar tradicional do policiamento de *hot spots* era definido como uma área muito pequena, como uma esquina, um endereço específico, ou mesmo um segmento de rua, e era representado por um mapa físico e alfinetes vermelhos eram demarcados acima do local do crime, indicando um ponto quente, literalmente um *hot spot*, mas, com o passar dos anos os programas de geoprocessamento já faziam de forma mais aprimorada. Importa dizer que a delimitação do local do crime é crucial para o entendimento da geografia do crime no policiamento tradicional de *hot spots*, quando agora sequer pode-se marcar o local do delito com precisão, pois a vítima, o alvo, o autor e o resultado estão em locais não coincidentes, o que torna a análise complexa e exigente de rastreamento.

No transcorrer do crime tradicional, os pequenos ambientes, inseridos em contextos sociais mais amplos, são os locais onde a interação entre o ofensor e o alvo se acontece. Ao mapear essas localidades, é possível identificar padrões de ocorrência e concentrar esforços de prevenção e controle nas áreas mais vulneráveis. O que não deixará de existir é a efetividade desse tipo de análise e policiamento para os delitos de mundo físico, pois o mapeamento criminal não apenas revela onde os crimes ocorrem, mas também fornece subsídios para a criação de ambientes mais seguros e resilientes, no entanto, as alternativas para os delitos desterritorializados devem ser de imediato pensadas pelas agências de acordo com Faria e Michalick (2024, p. 176).

> Assim, os resultados da análise criminal são promissores para a implementação da estratégia de **Policiamento de Hot Spots**, pois poderíamos focar em um número reduzido de locais, os quais tem potencial em contribuir com maior possibilidade de **redução das taxas gerais de crimes**.
>
> Outra previsão teórica que se confirmou foi a **estabilidade dos hot spots**. Em Belo Horizonte os dados indicaram que houve uma **estabilidade de manutenção do status em termos de concentração crimina**l entre o período de análise (2018 a 2021) acima de 70% para ambos os crimes analisados, o que demonstra que, apesar de diminuição geral nas taxas criminais durante o período, os hot spots permaneceram quentes. Esta constatação além de fornecer melhor subsídio para a implementação do Policiamento de Hot Spots também robustece a ideia de que a análise para elaboração de cartões-programa deve ser por períodos acima de um ano, já que no período de quatro anos não houve mudanças substanciais na distribuição dos crimes ao longo do tecido urbano.
>
> Em termos da distribuição temporal dos crimes violentos e de furtos, observou-se que houve uma certa coincidência na distribuição por dias da semana, mas um **comportamento peculiar para cada tipologia por faixa horária**. Em termos de concentração, destacou-se o período entre 14h e 23h59min com taxas de ocorrência acima de 50% do total de eventos ocorridos nos anos de 2018 a 2021 (52% no caso dos furtos e 57% para os crimes violentos).

> Um aspecto que merece relevo no momento de conclusão deste livro é que não se identificou na literatura outros estudos nacionais que tivesse o foco nos microespaços e suas possibilidades de emprego operacional dedicado.

O último aspecto que os autores consideraram de relevo que não se identificou na literatura outros estudos nacionais com o foco nos microespaços e suas possibilidades de emprego operacional tem razão específica de ser. A aplicação da análise preditiva pela polícia se estruturou ao longo dos anos de forma restrita e responsável, em consideração aos princípios éticos e aos direitos dos cidadãos, mas tratava-se de análises e gestão de dados por humanos. Verifica-se relevante e admissível a preocupação das repartições de Inteligência ou tecnologia em restringir por longos anos o acesso aos dados e ao conhecimento de como realizar tais investigações, pois é importante garantir que a tecnologia seja usada para melhorar a segurança pública de forma justa, imparcial e transparente.

O que não se pode ignorar é que o mundo passa por acelerada mudança e o cenário de crimes mudou drasticamente, de maneira que não investir ou expandir tais conhecimentos pode implicar no enfraquecimento do próprio Estado como figura detentora do monopólio de segurança pública ou de uso de força policial, ora percebida como a autorização legítima em prol da proteção do bem comum. O uso da IA torna-se inevitável e a solução tangencia supervisão adequada, regulamentação para manutenção e possibilidade de permanência responsável da função preditiva pela polícia.

Enquanto a luta pela implementação de proteção por meio da rede comunitária permanece nos dias atuais, o tão assustador anonimato das metrópoles já fora superado pelas infinitas possibilidades de atuação anônima em um território virtual, sem (ou com muito pouca) vigilância social e estatal, o que resulta em um território propício e seguro para a prática de crimes. Percebe-se grande dificuldade da geração nascida antes do século XXI, atualmente ativos e em atividades de poder, em perceber e se adaptar às rápidas mudanças geracionais posteriores ao Século XXI.

Aparentemente, estudam, pesquisam e trabalham projetos para o presente, sem observar o fato de que o mundo geracional teve o indivíduo aculturado em outros ambientes e numa outra forma de comunidade/cidade, por conseguinte, também mudará a forma de suas

práticas delitivas e seus bens juridicamente tutelados. O que interessava ao Direito proteger, não mais está sequer ao seu alcance sem adaptações de teorias puras, ainda que em um lapso temporal dos últimos 20 anos. A tecnologia ao qual esse indivíduo que é gestor, legislador, jurista, e atores de segurança se adaptou, já é intrínseca à geração a qual está sendo entregue papeis sociais com espaços de exercício de poder, para tanto, os métodos policiais de análise criminal por intermédio da polícia preditiva precisam de novas premissas como a inteligência artificial para alcançar o delito desterritorializado e rastrear os infratores.

3.4 Percepção do ciberespaço e as novas premissas para o delito desterritorializado

Em 2005, o sociólogo francês Robert Castel (1933-2013) após estudar a sociedade "superprotetora e securitária" publicou no Brasil o livro "A Insegurança Social: o que é ser protegido?" Para o autor, a insegurança moderna não seria a falta de proteção, mas ao contrário, um universo projetado em torno de uma busca sem fim de proteções ou de uma busca tresloucada de segurança.

O que é ser protegido nessas condições? Não é viver na certeza de poder controlar todos os riscos da vida, mas, sobretudo, viver cercado de sistemas de segurança que são construções complexas e frágeis ao mesmo tempo e que trazem em si mesmas o risco de falhar em sua tarefa e decepcionar as expectativas que elas suscitaram.

Para Castel (2005), a busca de proteção cria insegurança. Um exemplo disso no mundo virtual são os antivírus que podem ser a própria vulnerabilidade em si, bem como o indivíduo que prefere não se colocar em risco e negar a utilizar tecnologias de aplicativos ou navegações e finda desinserido e marginalizado diante na nova sociedade e mercado de trabalho.

Castel (2005) trabalhou implicitamente os conceitos constitucionais conhecidos pelos juristas como a segurança expressa no art. 5º da CRFB (liberdade individual) e a segurança expressa no artigo 6º (direito coletivo), ao dizer que as sociedades modernas são construídas sobre o terreno da insegurança, porque são sociedades de indivíduos que

encontram em seu entorno imediato a capacidade de assegurar sua proteção (individual). Essas sociedades promovem o indivíduo, mas também promovem sua vulnerabilidade e produzem certa frustração securitária – os programas de proteção jamais podem ser completamente cumpridos, o que gera decepção e ressentimento.

As intepretações de Castel (2005) dialogam com Bauman (2009) no sentido de que a segurança jamais é outorgada, nem mesmo conquistada, porque, à medida que se atingem objetivos, novos se criam. Quanto à proteção social, há certa proliferação contemporânea de uma aversão ao risco que faz com que o indivíduo nunca se sinta em segurança, pois para isso teria que conseguir controlar todos os imprevistos. Uma possível solução seria enfrentar os fatores de dissociação social que estão na origem da insegurança civil.

Parte-se do pressuposto de a "sociedade do risco" está a ocupar territórios muitas vezes fictos, numa nova dinâmica das interações sociais marcadas pela fluidez, volatilidade e rapidez, disponíveis ao simples toque dos dedos, num espaço cibernético de infinitas possibilidades de insegurança.

Ao tratar da relação entre crime, oportunidade e vitimização, Beato Filho, Peixoto e Andrade (2004) afirmam:

> Fatores que mais influenciam o risco de vitimização dos indivíduos são: exposição, proximidade da vítima ao agressor, capacidade de proteção, atrativos das vítimas e natureza dos delitos. A exposição é definida pela quantidade de tempo que os indivíduos frequentam locais públicos, estabelecendo contatos e interações sociais. O estilo de vida de cada indivíduo determina em que intensidade os demais fatores estão presentes na sua vida. Assim, determina em que medida **os** indivíduos se expõem ao frequentar lugares públicos, qual a sua capacidade de proteção, seus atrativos e a proximidade com os agressores [...]. **A ideia um tanto óbvia de que ofensores e vítimas devem convergir no tempo e no espaço deu origem a estudos que visam a identificar as dinâmicas pelas quais os indivíduos proporcionam oportunidades para vitimização** (Grifos nosso).

Os autores destacam variáveis importantes, tais como: exposição, capacidade de proteção, atrativos das vítimas e natureza dos delitos, e em especial a convergência entre ofensores e vítimas num mesmo tempo e espaço, mas que não são mais ideias tão óbvias, conforme se compreendia.

As metamorfoses das cidades se deram ao longo da história de forma física, mas até então não havia a expansão virtual. Nesse sentido, Tereza Pires (2000) em “Cidade de Muros” - nomenclatura utilizada na Antiguidade e Idade Média e nos dias atuais aplicada aos condomínios - não representa mais proteção ao patrimônio de forma real, pois pode-se retirar todos os ativos de um morador desses enclaves fortificados estando a quilômetros de distância.

Da mesma forma, os indivíduos menos informados – não necessariamente os integrantes de classes sociais economicamente vulneráveis – são os mais suscetíveis a sofrerem ataques em seu patrimônio “líquido”, já que o mundo é “líquido”, tal como conceituado por Bauman (2014) e a Engenharia Social se utilizará do comportamento do usuário da tecnologia que desconhece ou não desconfia de parte do funcionamento ou da proteção de dados e, por conseguinte, patrimônio.

Castel (2005) refuta que os autores de crimes patrimoniais advêm exclusivamente das classes baixas, e defende que certas formas de mendicância não interferem ou envolvem-se em delitos, demonstrada em sua obra pelos institutos de assistência que conseguem assegurar minimamente uma estabilidade e responsabilidade social a indivíduos que se situam abaixo do patamar da pobreza, qualquer que seja a forma de mensuração.

Outros grupos de “vagabundos” estudados por Bauman (1999), que outrora não eram nem mais nem menos “pobres”, recebiam um tratamento totalmente diferente e eram completamente estigmatizados, de forma que havia na França em determinado período uma classe média alta que era considerada socialmente “perigosa”. Essa afirmação coaduna com a percepção de Castel (1997, p. 24) de que “o nível de recursos econômicos constitui apenas um elemento para caracterizar as situações marginais”.

Como alguns fenômenos sociais possuem a tendência de se repetir, algo não mudou nesse cenário: As cidades permaneceram no risco e não tomaram medidas para evitar a instauração da desordem num ambiente novo e desconhecido, sem regras e, diferentemente de como se

formaram os aglomerados, sem limites territoriais. Tais considerações permitem inferir que o fenômeno social do crime patrimonial cibernético não mais permite a afirmação de que se trata de um crime de classe baixa contra classes altas, dados os requintes de técnicas de colarinho branco, há registros de esquemas de golpes engendrados por escritórios inteiros montados para tal finalidade, como também há registros de golpes aplicados via celulares em presídios ou aglomerados.

Conclui-se que não há classe estigmatizada para a nova modalidade de crime patrimonial, bem como a teoria criminológica aplicável de melhor linha é a ambiental, devido à facilidade do ambiente que conta com a ausência de guardião e tem influenciado para a motivação do autor, que encontra suas vítimas em potencial.

3.5 Complexidade e multidimensionalidade do fenômeno criminal em ambientes virtuais

Essa reflexão parte do Paradigma da Complexidade, proposto por Edgar Morin (2003), que defende uma abordagem holística e integradora do conhecimento. De acordo com Morin (2003), esse paradigma abrange diversas áreas de estudo e enfatiza a interconexão entre elas, na busca de uma compreensão mais completa e menos fragmentada do mundo, de modo que verifica uma visão ampla e inclusiva, essencial para enfrentar os desafios complexos do século XX.

Tal paradigma desafia os métodos tradicionais e incentiva uma reflexão mais aprofundada sobre como o conhecimento é construído e aplicado na solução dos problemas. Morin sugere que apenas por meio de uma compreensão mais profunda e conectada dos fenômenos pode-se encontrar soluções eficazes para os problemas persistentes. A adoção de uma abordagem baseada na Complexidade é, portanto, uma questão acadêmica e necessidade urgente para o progresso e bem-estar da sociedade global (Priuli, 2023).

A Teoria da Complexidade oferece uma perspectiva inovadora para entender a dinâmica social, rompendo com abordagens tradicionais como o reducionismo, o holismo e o hierarquismo. Propõe uma visão onde os sistemas não são simplesmente partes isoladas ou um todo homogêneo, mas uma interação complexa de elementos que são complementares, concorrentes e antagônicos. Essa reelaboração permite entender as relações sociais como uma rede de interdependências, onde a causa e o efeito são circulares e recíprocos, fomentando a auto-organização e o dinamismo do sistema (Santos, Pelosi, Oliveira, 2012; Quirino Júnior, Cotta, 2023; Silva, 2024).

A complexidade e a multidimensionalidade do fenômeno criminal em ambientes virtuais, como o estelionato digital, exigem uma reflexão profunda sobre a relação entre informação, conhecimento e sabedoria, conforme discutido por Edgar Morin em sua obra “Introdução ao pensamento complexo” (2005, p. 110). Na obra, Morin problematiza a diferença entre esses conceitos, afirmando que a sabedoria é reflexiva, o conhecimento é organizador, e a informação se apresenta como unidades designável. Essa distinção é crucial para entender como as Ciências Policiais devem abordar o fenômeno criminal no ciberespaço e evitar o medo para com a substituição do ser humano pela IA.

No contexto da criminalidade digital, a informação por si só não basta; é necessário processá-la, organizá-la e transformá-la em conhecimento aplicável, o que pode ser feito pela inteligência artificial. Morin (2005) sugere que a informação é extraída da natureza e transformada em signos, o que implica que, no âmbito das investigações criminais, a coleta de dados (informação) deve ser seguida por um processamento rigoroso (conhecimento) para que se obtenha uma compreensão profunda e reflexiva (sabedoria) das dinâmicas criminosas. Significa dizer que para atingir real conhecimento e sabedoria da situação prática, será necessária a gestão pelo policial humano da ferramenta, sob o risco de deduções erradas pela falta de conhecimento do todo.

No caso dos crimes virtuais, como o estelionato digital, a complexidade aumenta devido à desterritorialização e à rapidez com que as informações são geradas e disseminadas, de modo que o conhecimento sobre esses crimes exige não apenas a interpretação dos dados digitais, mas também uma compreensão das interações humanas que ocorrem inicialmente no âmbito

da Engenharia Social e posteriormente no ambiente virtual. É nesse ponto que a computação, como descrita por Morin (2005), desempenha um papel fundamental ao permitir que as forças de segurança extraiam padrões significativos do vasto "ruído" de dados presentes na internet, e por mais que a IA possa gerir a big data, esse conhecimento não conhece a si próprio:

> A informação supõe a computação viva. Além disso, devo fazer esta precisão: a computação não se resume de modo algum ao tratamento das informações. A computação viva comporta aos meus olhos uma dimensão não digital. A vida é uma organização computacional que, por isso mesmo, comporta uma dimensão cognitiva indiferenciada em si mesma. **Esse conhecimento não se conhece a si próprio**. **A bactéria não conhece o que ela conhece, e ela não sabe que sabe**. O aparelho cerebral dos animais constitui um aparelho diferenciado do conhecimento. Ele não computa diretamente os estímulos selecionados e codificados pelos receptores sensoriais; ele computa as computações que fazem seus neurônios (Morin, 2005, p. 110; Grifo nosso).

Morin (2005) também ressalta que o conhecimento supõe uma separação interna e externa, refletindo a complexidade do fenômeno criminal que não se limita apenas ao mundo exterior, mas também envolve uma profunda introspecção sobre as próprias capacidades e limitações das forças policiais. Ao reconhecer que a mente, por mais capacitada que seja, ignora muitos aspectos do próprio corpo, podemos traçar um paralelo com a necessidade das agências de segurança de se autoavaliar e ajustar continuamente suas estratégias de combate ao crime em ambientes virtuais. É latente segurança pública no Brasil possui certa fragilidade na Gestão da Segurança Pública ainda amparada nos resquícios da burocracia e do patrimonialismo, de forma que qualquer proposição de mudança aparenta ameaça institucional e não é vista como boa mudança em prol do resultado social.

De forma que coaduna com a teoria de Morin que não percebe o conhecimento estanque metodológico, mas interligado em níveis micro e macro, a cultura do trabalho policial brasileiro e das organizações permeia toda e qualquer proposta interventiva técnica que é feita. Fácil é deduzir que se precisa alocar mais recursos para treinamento e especialização em crimes cibernéticos em ambas as polícias e que estas devem oferecer treinamento contínuo para atualizar as habilidades dos agentes diante da rápida evolução tecnológica e que a colaboração entre as polícias e entre as agências brasileiras deve ser fortalecida para promover uma abordagem unificada. Difícil é perceber as nuances do jogo de poder que se

estabelece entre as instituições e todos os acordos e regras do jogo que não estão escritos nos manuais técnicos policiais e nas diretrizes de cada instituição.

Sobre as “regras do jogo”, e ainda na esteira da interseção entre a complexidade intrínseca do conhecimento, conforme discutido por Edgar Morin, os desafios enfrentados pelas Ciências Policiais na era digital são apontados por Morin de forma que a organização do conhecimento tradicional é um processo seletivo que separa, distingue e hierarquiza dados, mas essa separação pode resultar em um entendimento mutilado e incompleto da realidade (Morin, 2005, p. 10). Esse conceito é altamente relevante para a compreensão dos crimes cibernéticos, onde a fragmentação do conhecimento e a ausência de uma abordagem holística sobre a realidade da atividade policial, pelo o que investiga as Ciências Policiais, podem levar a respostas ineficazes ao fenômeno criminal.

O governo que segue o pensamento liberalista, focado na política de não intervenção de mercado e desenvolvimento desse, sempre terá ótimas soluções e modelos que promovam parcerias com o setor privado, universidades e especialistas em cibersegurança para compartilhar conhecimentos e recursos. O governo legalista, mais voltado para a burocracia, sempre dirá que a Legislação não está atualizada e por isso não é possível agir pois o Brasil precisa revisar e atualizar a legislação relacionada aos crimes cibernéticos para cobrir novas ameaças e táticas. O governo paternalista, de imediato focado na segurança do cidadão, por vezes não percebe o problema iminente pois não percebe os resultados naturalísticos imediatos e não avalia medir o aumento da desigualdade em médio prazo. As instituições policiais, por sua vez, se veem muitas vezes tecnicamente sem meios para identificar os criminosos golpistas ou sem conhecimento para atuar e findam por fazer o que podem, ao propor a conscientização pública, a educação e conscientização pública sobre cibersegurança e indicar medidas como cartilhas, que passam a ser apresentadas como prioridade de atuação que foca apenas em reduzir a vulnerabilidade dos cidadãos.

Em resumo, o modelo de atuação da polícia brasileira em crimes cibernéticos precisa de melhorias significativas em termos de recursos, treinamento, colaboração e legislação, mas principalmente em relação a gestão e a cultura das organizações policiais, muito além do que

está escrito e muito diferente do que se consegue medir em números e resultados com índices escolhidos para controlar a criminalidade.

Assim, ao lidar com a criminalidade em ambientes virtuais, é fundamental que as agências policiais não apenas coletem e processem informações, mas que também desenvolvam um conhecimento reflexivo que permita a compreensão das causas profundas desses crimes e a formulação de estratégias eficazes. Essa abordagem multidimensional é essencial para enfrentar a complexidade do fenômeno criminal em um mundo cada vez mais digitalizado. É fato que a aplicação de tecnologia avançada é essencial para enfrentar os golpes, especialmente no contexto digital, mas a análise de dados, a mineração de dados e as ferramentas de cibersegurança que podem ser usadas para identificar atividades suspeitas, rastrear transações e coletar evidências digitais só poderão ser efetivamente implementadas após a percepção do problema da e pela gestão policial.

Para além da complexidade das questões de Estado e de Governo, a definição do que é ambiente virtual e desterritorializado é, por si só, não pacífica e correlacionada a um emaranhado de circunstâncias. No que tange a micro dimensão proposta por Morin, o desenvolvimento de ferramentas tecnológicas tem sido fomentado dentro da realidade de cada agência policial em Minas Gerais, aqui especificada na PMMG e na PCMG. Aquela possui centro próprio de desenvolvimento em tecnologia e sistemas e esta possui os meios adequados e legais para a investigação de tais delitos complexos. Mas, ao buscar soluções, deve-se considerar que, conforme trabalhado adiante, investir em tecnologia avançada, como ferramentas de análise de dados e Inteligência Artificial, pode fortalecer a capacidade de identificar atividades suspeitas e antecipar possíveis golpes. Essas ferramentas podem ajudar a analisar grandes volumes de dados para identificar padrões e anomalias.

> As diferentes opiniões sobre o que deve ser considerado um crime de informática e, é claro, a dificuldade em mensurar qualquer tipo de atividade ilegal têm levado a estimativas bastante variadas dos valores envolvidos nesse tipo de crime. No ponto mais baixo, está o Nation Center for Computer Crime Data (Centro Nacional de Dados sobre Crimes da Informática), cujos números totalizam 550 milhões de dólares por ano nos EUA. Enquanto isso, a empresa de segurança em computação Inter-Pact aponta cifras 30 vezes maiores: 15 bilhões de dólares." O que sabemos, com certeza, independentemente de sua definição, é que os crimes de informática estão aumentando rapidamente. Em 1986, quando entrevistados responderam se achavam que suas empresas estavam sendo vítimas de crimes de informática,

> apenas 7% responderam que sim. Sete anos mais tarde, uma outra pesquisa mostrou que 70% das mais de 400 empresas pesquisadas acreditavam terem sido vítimas de crimes de informática no último ano. Dois anos depois, em 1995, 148 das 150 empresas pesquisadas disseram ter sido vítimas de atos criminosos da área de informática.
>
> Do ponto de vista legal, **a maioria dos crimes de informática entra em uma das três categorias seguintes. Em primeiro lugar, existem os furtos e as fraudes que envolvem o uso da internet e de outras tecnologias da computação para enganar o público,** praticamente da mesma forma como era feito anteriormente sem o apoio dessas tecnologias. Mas outro alvo cada vez mais comum são informações: acordos secretos, listas de mala direta, números de cartões de crédito. Mais próximos da imagem que o grande público faz do criminoso de informática estão os *hackers*, que cometem atos de vandalismo: destroem arquivos, desorganizam negócios, invadem computadores só pelo prazer e pela emoção (Coleman, 2005, p. 35; Grifo nosso).

Ao considerar a cooperação interestadual e a criação de unidades policiais especializadas, deve-se antes perceber que os crimes cibernéticos são fenômenos multidimensionais que não podem ser compreendidos ou enfrentados eficazmente com abordagens simplificadas ou unidimensionais. Morin sugere que a complexidade deve ser abordada como um tecido de eventos, ações, interações e incertezas. Da mesma forma, para enfrentar crimes como o estelionato digital, as agências de segurança pública precisam adotar uma visão que vá além da simples coleta de dados ou da aplicação de leis. É necessário integrar diversas disciplinas e conhecimentos, indo além da fragmentação imposta por abordagens tradicionais.

Os desafios descritos por Morin, como a cegueira gerada pela simplificação excessiva e a incapacidade de conceber a complexidade do real, são diretamente aplicáveis ao contexto dos crimes cibernéticos. A fragmentação do conhecimento e a ausência de cooperação eficaz entre diferentes estados e nações podem resultar em uma incapacidade de enfrentar a criminalidade digital de forma abrangente. Assim, a criação de unidades especializadas e a promoção da cooperação internacional não devem ser vistas como soluções isoladas, mas como partes de um esforço mais amplo para reestruturar a forma como o conhecimento e a prática policial abordam a complexidade dos crimes virtuais.

> Vivemos sob o império dos princípios de disjunção, de redução e de abstração, cujo conjunto constitui o que chamo de o "**paradigma de simplificação**". Descartes formulou este paradigma essencial do Ocidente, ao separar o sujeito pensante (ego cogitans) e a coisa entendida (res extensa), isto é, filosofia e ciência, e ao colocar como princípio de verdade as **ideias "claras e distintas**", ou seja, o próprio **pensamento disjuntivo**. Esse paradigma, que controla a aventura do

> pensamento ocidental desde o século XVII, sem dúvida permitiu os maiores progressos ao conhecimento científico e à reflexão filo-sófica; **suas consequências nocivas últimas só começam a se revelar no século XX.**
>
> **Tal disjunção, rareando as comunicações entre o conhecimento científico e a reflexão filosófica**, devia finalmente privar a ciência de qualquer possibilidade de ela conhecer a si própria, de refletir sobre si própria, e mesmo de se conceber cientificamente.
>
> Mais ainda, o princípio de disjunção isolou radicalmente uns dos outros três grandes campos do conhecimento científico: a física, a biologia e a ciência do homem.
>
> **A única maneira de remediar essa disjunção foi uma outra simplificação: a redução do complexo ao simples** (redução do biológico ao físico, do humano ao biológico). Uma hiperespecialização devia, além disso, despedaçar e fragmentar o tecido complexo das realidades, e fazer crer que o corte arbitrário operado no real era o próprio real. Ao mesmo tempo, o ideal do conhecimento científico clássico era descobrir, atrás da complexidade aparente dos fenô-menos, uma Ordem perfeita legiferando uma máquina perpétua (o cosmos), ela própria feita de microelementos (os átomos) reunidos de diferentes modos em objetos e sistemas.
>
> Tal conhecimento, necessariamente, baseava seu rigor e sua operacionalidade na medida e no cálculo; mas, cada vez mais, a matematização e a formalização desintegraram os seres e os entes para só considerar como únicas realidades as fórmulas e equações que governam as entidades quantificadas. Enfim, **o pensamento simplificador é incapaz de conceber a conjunção do uno e do múltiplo (unitat multiplex). Ou ele unifica abstratamente ao anular a diversidade, ou, ao contrário, justapõe a diversidade sem conceber a unidade.**
>
> Assim, chega-se à inteligência cega. **A inteligência cega destrói os conjuntos e as totalidades, isola todos os seus objetos do seu meio ambiente**. **Ela não pode conceber o elo inseparável entre o observador e a coisa observada**. As realidades-chave são desintegradas. Elas passam por entre as fendas que separam as disciplinas. As disciplinas das ciências humanas não têm mais necessidade da noção de homem. E os pedantes cegos concluem então que o homem não tem existência, a não ser ilusória. Enquanto que **as mídias produzem a baixa cretinização, a Universidade produz a alta cretinização**. A metodologia dominante produz um **obscurantismo acrescido**, já que **não há mais associação entre os elementos disjuntos do saber, não há possibilidade de registrá-los e de refleti-los** (Morin, 2005; Grifo nosso).

Essa reestruturação exige uma superação do "paradigma de simplificação" que Morin critica, em favor de uma abordagem que reconheça e enfrente a complexidade em todas as suas dimensões. Isso implica não apenas a integração de diferentes disciplinas e técnicas, mas também uma revisão crítica dos próprios paradigmas que guiam a ação policial, a fim de evitar que a prática investigativa se torne cega às realidades complexas e interconectadas do mundo digital.

4 METODOLOGIA

4.1 Base de dados sobre estelionato digital do estado de minas gerais

A metodologia da pesquisa proposta para o trabalho relaciona-se à análise criminal e teve início com a aquisição dos dados provenientes dos registros de ocorrências policiais referentes aos crimes de estelionato registrados no Estado de Minas Gerais no período compreendido entre os anos de 2018 a 2022. Na análise de dados criminais, deve-se compreender a origem e as características dos dados utilizados para garantir a validade das conclusões e a possível eficácia das políticas públicas a serem sugeridas e que são e serão baseadas neles. A fonte dos dados abrange dimensões como a origem, o método de coleta e a confiabilidade dos dados (Souza, 2020).

Conforme exposto por Souza (2020), a origem dos dados pode variar entre diferentes entidades, como agências governamentais, forças policiais ou organizações terceirizadas, para tanto, preferiu-se não trabalhar com os dados do cert.br, site interessante do Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil, que é uma organização que faz parte do NIC.br (Núcleo de Informação e Coordenação do Ponto BR). Brevemente, um dos principais serviços do CERT.br é a coleta, análise e divulgação de estatísticas relacionadas a incidentes de segurança na Internet no Brasil, mas são estatísticas que são atualizadas diariamente ou mensalmente, como o Kasyper já citado, e, a depender do tipo de dado, estão disponíveis para consulta pública, ou seja, trata-se do gestor brasileiro da internet, de fonte aberta, mas que ora justifica-se sua não utilização devido à impossibilidade de cruzamento de dados específicos do estado percebidos como crimes, já que o Cert.br trabalha e analisa incidentes, de forma mais abrangente. Em suma, nem todo incidente cibernético é crime[13].

13 - Disponível em: https://stats.cert.br/.

Saber de onde os dados provêm permite avaliar sua legitimidade e adequação ao objetivo da pesquisa. Tais dados são essenciais para a construção de uma análise sólida e fundamentada, vez que, na situação presente, refletem informações coletadas por instituições responsáveis pela segurança pública. Nesse modelo de análise criminal, deve-se considerar, além da fonte de produção, a confiabilidade inerente à coleta de dados criminais, que são de acesso restrito. Por certo que a subnotificação de alguns crimes pode gerar uma distorção na percepção da criminalidade real, uma vez que nem todos os delitos são reportados às autoridades e, por conseguinte, registrados. Essa subnotificação, conhecida como "cifra negra", representa uma limitação significativa, que deve ser cuidadosamente considerada para evitar conclusões equivocadas, mas serão tratadas adiante em subitem específico.

Os dados ora tratados são provenientes do Armazém de Informações do Sistema Integrado de Defesa Social (SIDS), e tal banco de dados, de onde foram extraídas as informações, é alimentado pelos dos Registros de Eventos de Defesa Social (REDS), fonte humana de registro, que consiste nos boletins de ocorrências policiais informatizados que são confeccionados por agentes da segurança pública do Estado de Minas Gerais.

Tais dados foram extraídos do Armazém de Informações do Sistema Integrado de Defesa Social (SIDS), que tem a função principal de integrar a base de informações produzidas pela Polícia Militar, Polícia Civil, Corpos de Bombeiro Militar e Sistema Prisional do Estado de Minas Gerais. Essa base é gerenciada pelo Centro Integrado de Informações de Defesa Social (CINDS) da Polícia Militar de Minas Gerais, que possui a finalidade de produzir as estatísticas, diagnósticos e relatórios sobre a criminalidade no Estado de Minas Gerais e tem como fonte de informações os bancos de dados do sistema integrado de defesa social e das respectivas instituições que o compõem. Atualmente a CINDS incorporou o Centro de Gestão de Análise de Dados Estatísticos (CGA).

O Armazém de dados possui acesso restrito, dessa forma, foi solicitado por meio de mensagem eletrônica enviada pelo canal de comunicação interna, denominado Painel Administrativo da PMMG, ao Centro Integrado de Informações de Defesa Social, (CINDS). Após a solicitação do acesso aos dados, houve a autorização e foi iniciada a análise e divulgação no presente trabalho, amparado na Resolução nº 4320/14 – CG c/c item 4.1 do

14 - Disponível em: https://www.revistaaec.com/index.php/revistaaec/article/view/1219.

Memorando nº 011/2022 – CINDS/DOP, que dispõe sobre a concessão de acesso e a análise dos pedidos de acesso à informação (relatórios estatísticos) ao público externo. A autorização para extração, utilização e divulgação dos dados foi concedida pelo Chefe do CINDS, por meio de mensagem enviada pelo Painel Administrativo da PMMG, registrado com protocolo de envio nº 202207056358361-2207.

Após a extração dos dados, estes foram trabalhados por meio do uso de planilhas e gráficos trabalhados no *Software* de edição de planilhas Microsoft Excel o que possibilitou a elaboração de gráficos e tabelas, permitindo a análise por ano, mês e dia da semana do fato, local do fato, modalidade e perfil das vítimas. Para a plotagem de mapas de localização dos delitos foi utilizado o Sistema de Gestão de Operacional (SIGOP) aplicativo da PMMG que utiliza os dados do Armazém para a produção de informações ao público interno, com acesso através do sistema Intranet da PMMG.

A análise temporal foi delimitada em cinco anos específicos em decorrência do período pandêmico, de modo a analisar um ano antes, o período propriamente dito e um não depois, sem desconsiderar que o registro inclui o exame do momento em que os crimes foram reportados e não quando exatamente ocorreram, mas pode revelar padrões sazonais ou tendências ao longo do tempo. Isso porque certos tipos de crimes podem ter picos em determinadas épocas do ano, influenciados por fatores como clima, feriados ou condições econômicas, o que pode ser verificado na análise dos resultados, mas cabe a inferência de que a identificação dessas tendências temporais é essencial para a implementação de medidas preventivas e para a alocação eficiente de recursos de segurança, não apenas colocação física de viaturas, como já exposto.

Em suma, a validação dos dados e da metodologia envolve uma compreensão detalhada da fonte, da categorização e dos padrões temporais dos dados criminais, para fins de elaboração de uma análise equânime que contribua para a formulação de políticas públicas eficazes e para a melhoria das estratégias de segurança pública.

Após a aquisição dos dados, foi realizado o trabalho de escritório, que consistiu no levantamento e leitura de várias obras de autores renomados que tratam do assunto, bem

como documentos da PMMG, com objetivo do conhecimento das teorias da criminalidade, bem como análise criminal.

A principal característica do trabalho consistiu, portanto no emprego de dados quantitativos, coleta e tratamento destes, e método de análise inferencial lógico-indutivo na descrição das possíveis causas pelas quais acontecem, bem como, na análise das teorias que corroboram com o fenômeno estudado.

4.2 Descrição dos procedimentos metodológicos para o desenvolvimento da pesquisa

Não menos relevante, a categorização dos crimes é outro aspecto concorrente à delimitação do objeto de estudo e também crucial à análise de dados criminais. Os crimes podem ser classificados de várias formas, como crimes violentos, crimes contra o patrimônio, crimes cibernéticos, entre outros. A categorização adequada pelas agências permite uma análise mais direcionada e eficaz, e tal situação é feita pela chamada “natureza do delito”, que é encontrada em forma de campo parametrizado no REDS e possibilita, por meio da chamada DIAO (diretriz que discrimina as naturezas desses registros) a identificação de padrões específicos e a formulação de estratégias de preenchimento mais adequado ao fato.

As fórmulas de cálculo estatístico são ferramentas fundamentais para a interpretação e síntese de dados, e foram utilizadas por meio de *software* Excel que já produz a planilha dinâmica e gera gráfico com base na análise dos dados que nele são inseridos, mas cabe ao analista correlaciona-los de maneira correta e saber o que deseja investigar. Foi utilizada a fórmula de aumento percentual automática, de modo que essa função faz o cálculo e permite identificar o crescimento relativo de um evento em comparação com o período anterior.

Do modo manual, não seria possível gerir bigdata, mas, para fins de explicação, considerando-se um cenário onde ocorrem 100 roubos em um ano e 110 no ano seguinte, o aumento percentual é de 10%. Esse valor é obtido de forma automática após inserida a

fórmula ou o filtro na planilha dinâmica do Excel, mas pela estatística básica do exemplo o resultado é atingido subtraindo-se o número inicial (100) do número final (110), resultando em 10; em seguida, divide-se esse aumento pelo valor inicial (100) e multiplica-se por 100, resultando em um aumento percentual de 10%. Essa metodologia é amplamente utilizada em estudos de criminalidade para quantificar e analisar tendências ao longo do tempo, e bem empregada pode tornar mais clara a visão sobre a evolução de determinados fenômenos criminais.

A fórmula supra é conhecida como fórmula de aumento percentual ou taxa de crescimento percentual e serve para medir o crescimento ou a diminuição de um valor em relação ao seu valor anterior em termos percentuais, basicamente calculada pela diferença entre o valor novo e o valor antigo, dividida pelo valor antigo, e o resultado é multiplicado por 100 para expressar o crescimento ou diminuição em porcentagem. Quanto a escolha do que seria analisa, o delito de Estelionato, tipificado de maneira geral no art. 171 do Código Penal Brasileiro, foi dividido, para efeito deste estudo, em dois grupos, de acordo com o campo parametrizado do REDS que discrimina o meio utilizado na ação, sendo delimitado o campo que contém os praticados por Meio Eletrônico (Internet ou SMS) como foco deste trabalho, e os demais registros de estelionato, que não marcaram o campo parametrizado do registro o meio eletrônico, foram demonstrados em quantitativo e percentual de aumento, mas não investigados em profundidade.

O Armazém de Informações constitui-se em um *software* com funcionamento *online* que tem a função de extrair os dados através do REDS, e é preenchido pelo policial no ato do registro da ocorrência do fato criminal. Este registro, em formato de formulário eletrônico e acessado online, possui diversos campos de preenchimento obrigatório e campos facultativos complementares. A extração desses dados é feita pelo Armazém, após a finalização do registro, e disponibilizada para consulta em planilhas eletrônicas com coordenadas geográficas atribuídas ao endereço do fato.

Para efeito desta pesquisa foi utilizado um filtro no Armazém dentro do universo de ocorrências policiais, com o objetivo de extrair todas as ocorrências registradas conforme as naturezas abaixo no estado de Minas Gerais no período de 2018 a 2022. Os dados englobam

14 - Disponível em: https://www.revistaaec.com/index.php/revistaaec/article/view/1219.

informações sobre as características socioeconômicas, hábitos e as características de residência e vizinhança das vítimas, mas não dos autores. A pesquisa inicialmente abarcou uma amostra muito grande de dados, mas em decorrência da delimitação do objeto as análises foram restritas, tornando-se uma pesquisa de vitimização, pois não conseguiu alcançar dados suficientes dos autores, tendo como local todo o estado de Minas Gerais e foram consideradas inicialmente as seguintes categorias de crime:

1 - "Fraude eletrônica" - 171 §2º-A;

2 - "Invasão de dispositivo informático" - 154-A E B;

3 - "Furto eletrônico" - 155§4º-B;

4 - "Interromper serviço telefônico" – 266;

5 - "Inserção de dados falsos em sistema" 313-A e B

Como mencionado, não foi possível a análise detalhada de todo o universo retirado dos Armazéns, embora autorizados para a pesquisa, tendo sido selecionado apenas o universo do estelionato. A pesquisa contém informações sobre todos os acontecimentos criminais que foram registrados pelos órgãos de Segurança Pública de Minas Gerais e permitiu análise dos danos sofridos pelos indivíduos, sobre a quantidade e o tipo de perda incorrida e, raras vezes e por desconsideradas, sobre as características dos criminosos, o que indica o fenômeno da desterritorialização em que não é coincidente o local de vítima, autor e resultado. Logo, os dados apresentados nesta seção são provenientes do que se denominou pesquisa de vitimização realizada por meio dos Registros de Eventos de Defesa Social (Armazém SIDS), para o período compreendido entre 2018 e 2022.

4.3 Limitações na contabilização pautada exclusivamente no banco de dados dos boletins de ocorrência

A análise dos crimes de estelionato, especialmente em seu formato digital, apresenta limites significativos devido à forma como os dados são registrados e coletados. A primeira distinção está entre crimes reportados e não reportados, porque as estatísticas oficiais

14 - Disponível em: https://www.revistaaec.com/index.php/revistaaec/article/view/1219.

incluem apenas os crimes que chegam ao conhecimento das autoridades, o que exclui da análise aqueles que, por diversas razões, não foram comunicados pelas vítimas. Esse fenômeno é conhecido como "cifra oculta" e esconde uma parte substancial da criminalidade, além de ser o principal limite de compreensão da realidade por estatística, já que esta última não mostra toda a extensão do problema.

O segundo limite mais evidente são os erros e inconsistências nos registros, como falhas na entrada de dados ou mudanças na DIAO ao longo do período da amostra (metodologia que direciona a confecção/inserção da natureza no relatório), mas, embora diminuta em comparação à cifra negra (na qual não se pode obrigar o cidadão a realizar o registro) pode também comprometer a análise e distorcer a compreensão do fenômeno criminal por ser um fato registrado com codificação diversa.

O evento de estelionato não é amplamente utilizado como indicador de criminalidade devido à sua menor gravidade percebida e à antiga baixa taxa de notificação junto aos órgãos públicos, então o impacto da subnotificação é menor, mas deve-se considerar que algumas vítimas não relatam o ocorrido, seja pelo baixo valor dos bens envolvidos, seja pela descrença no processo investigativo após vários registros ao longo dos anos, no entanto o que pode ser de notável fator motivacional para o registro é o resguardo do destino dos ativos e bloqueio de transações. Contudo, a subnotificação afeta sim a precisão dos dados pois inviabiliza a contagem exata dos eventos criminais.

Em resumo, as principais limitações identificadas na metodologia em vigor são as circunstâncias fáticas que dificultam o registro adequado antes de ser inserida a alteração da legislação no sistema, as falhas no preenchimento dos boletins de ocorrência e a subnotificação provocada por erros ou omissões nos registros. As estatísticas oficiais, por si só, não fornecem um retrato completo do fenômeno, em que pese ser o objetivo de ouro das instituições que imaginam que se controlam todos os dados terão todas as respostas, para tanto, têm se aumentado os mecanismos de poder e controle que influenciam a qualidade e a precisão das informações registradas, mas há possibilidades mais eficientes sugeridas ao final deste trabalho.

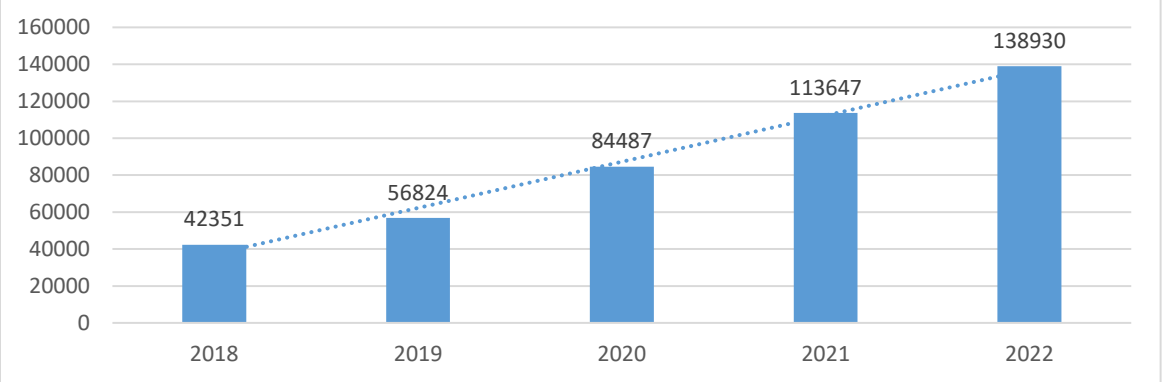
A compreensão dessas limitações é fundamental para evitar conclusões precipitadas e para promover uma análise mais sólida e contextualizada dos crimes de estelionato, especialmente em um cenário de criminalidade digitalizada e dispersa geograficamente.

5 RESULTADOS E DISCUSSÃO

5.1 Análise quantitativa dos resultados e tendências dos crimes de estelionato

Em suma, a análise propriamente dita para delimitação do objeto foi relativa ao estelionato e a sua subespécie fraude eletrônica. Os dados coletados foram condensados em forma de tabelas, gráficos e mapas de calor, evolução dos hotspots citados. Inicialmente, para análise e interpretação dos dados sobre estelionato, o quantitativo geral das ocorrências no período foi demonstrado abaixo em gráfico de barras, para fins de melhor visualização da linha de crescimento (GRAF. 1).

Gráfico 1 - Evolução dos crimes de estelionato registrados por ano, período: 2018 a 2022



Fonte: Produzidos por meio de dados dos Armazéns de Segurança Pública de Minas Gerais 2023.

Significa dizer que, em um contexto geral dos crimes físicos e virtuais, não houve aumento apenas do delito de fraude eletrônica, mas do estelionato como um todo. Nos últimos anos, especialmente durante a pandemia de Covid-19, o número de ocorrências registradas dessa natureza cresceu exponencialmente em Minas Gerais. Isso reflete uma tendência e um indício de que a digitalização de serviços e a maior conectividade da população têm sido acompanhadas por um aumento significativo de crimes cibernéticos. Se em 2018 o número

14 - Disponível em: https://www.revistaaec.com/index.php/revistaaec/article/view/1219.

de registros total ao final do ano foi de 42.351, em 2019 esse número sobe para 56.824, e em 2020 a quantidade dobra em relação ao ano base parâmetro, qual seja, 2018 e atinge 84.487 registros em todo o estado. Em 2021 o quantitativo permanece subindo para 11.3647 e em 2022 a quantidade se mantém na linha crescente e encerra o ano com 13.8930. Dentro desse imenso universo, algumas separações foram paulatinamente destrinchadas, a saber, do quantitativo de delitos tentados e consumados demonstrados no Quadro 4:

Quadro 4 - Crimes de estelionato registrados por ano

Crimes estelionato registrados por ano			
Ano	**Crimes de estelionato**	**Consumado**	**Tentado**
2018	42351	40278	2073
2019	56824	53472	3352
2020	84487	78970	5517
2021	113647	104983	8664
2022	138930	130435	8495

Fonte: Armazéns de Segurança Pública de Minas Gerais, 2023.

Tendo em vista que a análise de dados criminais é uma ferramenta que utiliza da estatística e trabalha com a coleta de informações sobre crimes e essas informações podem ser usadas para entender padrões de como, quando e onde os crimes mais acontecem, dentro do último universo de registros realizados por ano, fez-se uma seleção dos dados em planilhas e foi aplicado o filtro de “consumado” e “tentado”, um dos campos parametrizados obrigatórios do REDS, e o quantitativo da soma destes eventos devem equivaler ao quantitativo anterior apontado.

Foi identificado que os crimes de estelionato registrados entre 2018 e 2022 revelam uma tendência crescente e preocupante na criminalidade relacionada a fraudes no Brasil. Em 2018, foram registrados 42.351 casos, dos quais 40.278 foram consumados e 2.073 tentados. Esse número aumentou significativamente ao longo dos anos, atingindo 138.930 casos em 2022, com 130.435 crimes consumados e 8.495 tentados. O crescimento exponencial, especialmente evidente a partir de 2020, como já exposto, pode estar associado ao aumento

14 - Disponível em: https://www.revistaaec.com/index.php/revistaaec/article/view/1219.

da digitalização e à maior dependência de transações online durante a pandemia de Covid-19, que ampliou as oportunidades para atividades fraudulentas.

Quanto ao aumento percentual anual de estelionato, foi calculado e representado conforme os números acima e estruturados no Quadro 5 que perfazem mais claras as demonstrações das tendências, conforme:

Quadro 5 – Crimes de estelionato por modalidade consumado e tentado

CRIMES DE ESTELIONATO POR MODALIDADE CONSUMADO E TENTADO					
ANO	CRIMES DE ESTELIONATO	CONSUMADO	%	TENTADO	% TENTADO
2018	42351	40278	95,11%	2073	4,89%
2019	56824	53472	94,10%	3352	5,90%
2020	84487	78970	93,47%	5517	6,53%
2021	113647	104983	92,38%	8664	7,62%
2022	138930	130435	93,89%	8495	6,11%

Fonte: Produzidos por meio de dados dos Armazéns de Segurança Pública de Minas Gerais, 2023.

O percentual indicado acima indica o valor que representa naquele ano em relação ao quantitativo de crimes cometidos. A análise dos dados sobre crimes de estelionato consumados e tentados entre 2018 e 2022, específico conforme o quadro 5 acima apresentada, demonstra uma persistente alta taxa de sucesso nas ações fraudulentas. Em 2018, 95,11% dos crimes de estelionato foram consumados, percentual que, embora tenha variado ligeiramente ao longo dos anos, se manteve elevado, e atingido 93,98% em 2022.

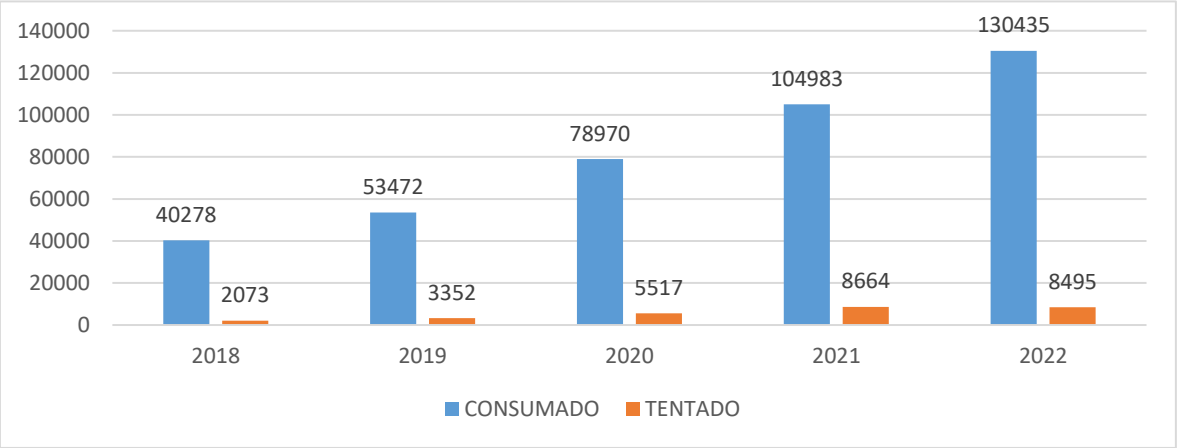
A pequena variação na taxa de sucesso desses crimes sugere que, apesar de um aumento significativo no número total de casos, a eficiência dos criminosos em concretizar suas fraudes permanece alta, no entanto, há que se considerar que os agentes que registram podem entender que, por não haver a efetiva transferência de valores ou situação similar, o crime não se concretizou, situação jurídica controversa. Ocorre que os números evidenciam uma lacuna na capacidade de prevenção e resposta imediata por parte das vítimas e das agências. O crescimento dos crimes tentados, que passou de 4,89% em 2018 para 7,62% em 2021, seguido por uma leve redução para 6,11% em 2022, que indica uma possível maior conscientização ou resistência das vítimas, embora ainda insuficiente para reverter a tendência geral, mas também podem indicar que os agentes que registram passaram a

perceber que os golpes que possuem a capacidade de engodo da vítima se consumam independente da vantagem econômica em caráter definitivo em poder do autor.

Em números gerais, quanto ao Gráfico 1, o aumento percentual de casos de estelionato (sem especificar meio ou se foi consumado ou tentado) ano a ano, sempre conforme o ano anterior, equivale aproximadamente a 33,75% de 2018 para 2019. De 2019 para 2020, o aumento foi ainda mais expressivo, aproximadamente 48,68%. De 2020 para 2021, o aumento foi de 34,45%. Finalmente, de 2021 para 2022, houve um crescimento de 22,26%. Esses números evidenciam uma escalada significativa na incidência de estelionato ao longo dos anos.

Baseado nos dados extraídos, obteve-se as seguintes informações sobre o delito de estelionato ao longo dos anos da amostra, por meio dos números de casos consumados e tentados e representados no Gráfico 2:

Gráfico 2 - Evolução das modalidades consumado e tentado nos registros dos crimes de estelionato por ano, Minas Gerais (2018 a 2022)



Fonte: Produzidos por meio de dados dos Armazéns de Segurança Pública de Minas Gerais, 2023.

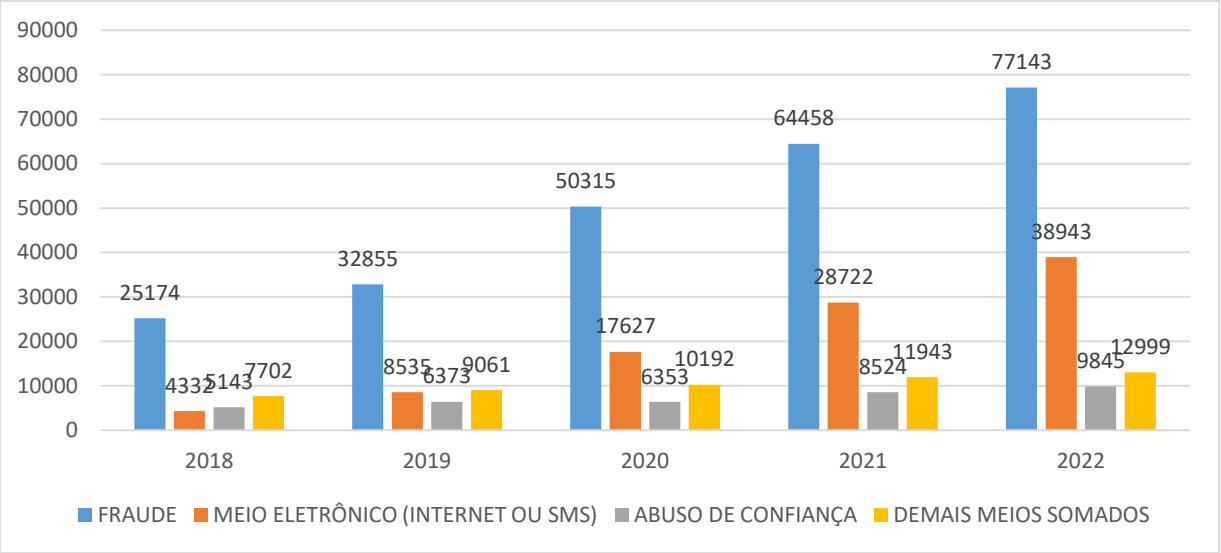
O Gráfico 2 divide os crimes de estelionato em duas categorias: os que foram consumados (ou seja, a fraude foi bem-sucedida) e os que foram tentados (a fraude foi iniciada, mas não teve sucesso em decorrência de circunstâncias alheias à vontade do agente). Em 2018, foram consumados 3.992 crimes, enquanto em 2022 esse número chegou a 35.714. Por outro lado, o número de crimes tentados, embora também tenha aumentado, é significativamente menor

14 - Disponível em: https://www.revistaaec.com/index.php/revistaaec/article/view/1219.

do que o de crimes consumados, isso demonstra que a maioria dos crimes de estelionato praticados por meio eletrônico resulta em sucesso para os criminosos, ou que a percepção dos registradores é de que a empreitada foi bem sucedida.

Quanto aos meios utilizados no cometimento dos crimes de estelionato entre 2018 e 2022, foi realizado novo filtro nas planilhas, possibilitado pelo preenchimento dos campos parametrizados, e o resultado foi a produção do Gráfico 3 apresentado abaixo.

Gráfico 3 - Evolução dos meios utilizados no cometimento dos crimes de estelionato por ano, Minas Gerais (2018 a 2022)



Fonte: Produzidos por meio de dados dos Armazéns de Segurança Pública de Minas Gerais, 2023.

Observa-se que a prática do estelionato comum, ou seja, aplicação de fraudes tradicionais, permaneceu como a categoria predominante ao longo do período e aumentou de 25.174 casos em 2018 para 77.143 em 2022. No entanto, percebe-se também o crescimento significativo dos crimes de estelionato praticados por meio eletrônico (Internet ou SMS), que passaram de 4.332 casos em 2018 para 38.943 em 2022, o que reflete uma mudança também na percepção de quem registra para com o modus operandi dos criminosos. Este aumento, particularmente acentuado durante a pandemia de Covid-19, reforça o raciocínio indutivo de correlação com o período histórico da população mundial. O abuso de confiança e os demais meios somados tiveram um crescimento mais modesto, mas consistente, o que pode indicar

14 - Disponível em: https://www.revistaaec.com/index.php/revistaaec/article/view/1219.

que as fraudes se diversificam em suas formas de execução, possivelmente utilizando o Stelio, no sentido de camuflagem do camaleão, e adaptando-se ao conhecimento do público ao se aproveitar das mudanças tecnológicas e sociais

Ao diminuir mais a amostra, obteve-se as seguintes informações sobre o delito de estelionato utilizando meio eletrônico por modalidade tentado e consumado ao longo dos anos da amostra, Quadro 6:

Quadro 6 – Crimes de estelionato utilizando meio eletrônico (internet ou SMS) por modalidade consumado e tentado, Minas Gerais (2018 a 2022)

CRIMES DE ESTELIONATO UTILIZANDO MEIO ELETRONICO (INTERNET OU SMS) POR MODALIDADE CONSUMADO E TENTADO					
ANO	CRIMES POR MEIO ELETRONICO	CONSUMADO	%	TENTADO	%
2018	4332	3992	92,15%	340	7,85%
2019	8535	7691	90,11%	844	9,89%
2020	17627	15827	89,79%	1800	10,21%
2021	28722	25525	88,87%	3197	11,13%
2022	38943	35714	91,71%	3229	8,29%

Fonte: Produzidos por meio de dados dos Armazéns de Segurança Pública de Minas Gerais, 2023.

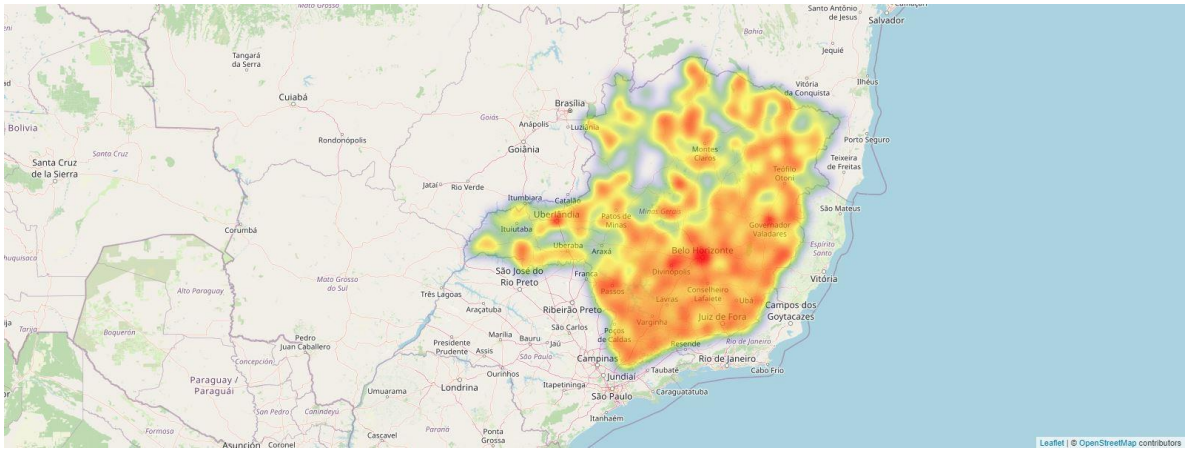
O Quadro 6 indica os crimes de estelionato utilizando meio eletrônico (Internet ou SMS) por modalidade consumada e tentada, no período de 2018 a 2022, e revela novamente as tendências de crescimento e de efetividade positiva dessas práticas criminosas. Em 2018, dos 4.332 crimes reportados, 92,15% foram consumados, o que perfaz a conclusão de que os indivíduos autores obtiveram alta eficácia na empreitada das fraudes eletrônicas.

O padrão se manteve elevado nos anos subsequentes, com pequenas variações, como em 2020, em que 89,79% dos crimes foram consumados. No entanto, observa-se um aumento na taxa de crimes tentados, que subiu de 7,85% em 2018 para 11,13% em 2021, antes de cair levemente para 8,28% em 2022. Os dados sugerem que, embora a maioria das fraudes eletrônicas seja bem-sucedida, há um crescimento nas tentativas, que não chegam a ser concretizadas possivelmente devido a uma maior conscientização das vítimas, pois as cartilhas já estavam sendo divulgadas pelas agências de segurança pública, e também foram divulgadas massivamente à época às melhorias nas medidas de segurança digitais, como a autenticação em dois fatores. Ainda assim, a alta taxa de sucesso dos crimes consumados

indica uma necessidade de manutenção das políticas de prevenção e na educação digital dos usuários para reduzir tanto a incidência quanto a concretização da fraude eletrônica.

O Mapa 1, por sua vez, também advém da ideia de hotspots e mapa de calor, produzido por meio do SIGOP com os dados do REDS, e ilustra a incidência dos crimes de estelionato utilizando meio eletrônico (Internet ou SMS) em MG durante o ano de 2022.

Mapa 1- Incidência dos crimes de estelionato utilizando meio eletrônico (Internet ou SMS) em Minas Gerais em 2022



Fonte: Dados dos Armazéns de Segurança Pública de Minas Gerais, 2023.

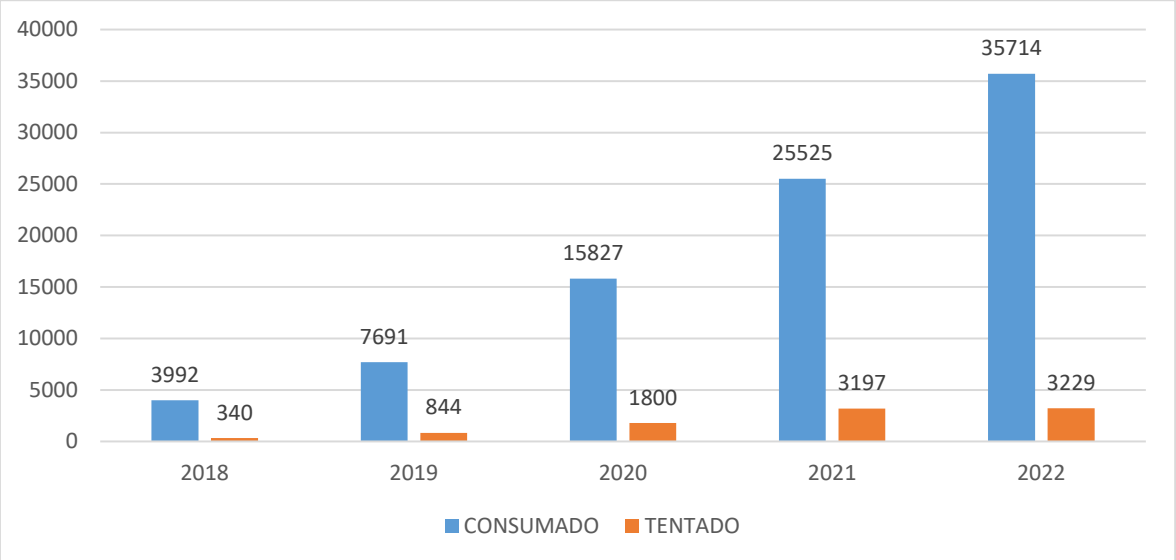
A representação de calor, vermelho dos pontos quentes (hotspots) no mapa, indica as áreas com maior concentração de ocorrências e mostra que as regiões mais afetadas estão nas proximidades de grandes centros urbanos como Belo Horizonte e outras cidades satélites do sul e sudeste do estado. As cores mais quentes, como vermelho e laranja, significam um número elevado de crimes e indicam que essas áreas urbanizadas e densamente povoadas são os principais alvos das atividades criminosas, ou que as áreas rurais não recorrem tanto aos registros. A hipótese de acessibilidade para o registro não pode ser descartada, mas é diminuta, e a associação da concentração desses crimes nas regiões metropolitanas pode ser melhor associada à maior penetração da internet e à maior atividade econômica nessas áreas, que proporcionam um ambiente fértil para os golpes, ou seja, as fraudes eletrônicas, especialmente nas regiões com alta densidade populacional e maior acesso a tecnologias digitais.

14 - Disponível em: https://www.revistaaec.com/index.php/revistaaec/article/view/1219.

Quanto à acessibilidade a área rural para os registros, no ano de 2023 e 2024 houve massivo engajamento em técnicas de aproximação e presença policial em tais lugares, por meio do fortalecimento das políticas públicas direcionadas às patrulhas rurais, e o resultado dessa aproximação pode ser medido em pesquisa futura que analise o aumento dos registros nessas localidades ou não, de modo a discernir se houve saneamento das localizações georrefenciadas que não são localizadas e por vezes obrigam o forçamento do endereço na sede do registro, bem como se a população rural está registrando mais ou se realmente o fato não ocorre nas regiões rurais.

Ainda na esteira de detalhar os dados, foi realizada nova subdivisão vista no Gráfico 4 para destrinchamento da análise:

Gráfico 4 - Evolução das modalidades consumado e tentado nos registros dos crimes de estelionato praticados utilizando meio eletrônico (Internet ou SMS) por ano, Minas Gerais (2018 a 2022)



Fonte: Produzidos por meio de dados dos Armazéns de Segurança Pública de Minas Gerais, 2023.

14 - Disponível em: https://www.revistaaec.com/index.php/revistaaec/article/view/1219.

O Gráfico 4, por sua vez, mostra a evolução das modalidades consumado e tentado nos registros dos crimes de estelionato praticados utilizando meio eletrônico (Internet ou SMS) entre 2018 e 2022. Observa-se novamente que o número de crimes consumados aumentou significativamente ao longo do período, passando de 3.992 em 2018 para 35.714 em 2022. Esse crescimento acentuado indica, além da eficácia crescente das fraudes eletrônicas, a percepção complexa de quem registra, pois se já não é claro para o operador do REDS o delito físico ser consumado ou tentado, quiçá o desterritorializado, concluindo-se, pois, que o operador passa a preferir e entender também a consumação efetivada na maioria dos casos.

Paralelamente, os crimes tentados também apresentaram aumento de 340 casos em 2018 para 3.229 em 2022, o que sugere um aumento no registro das tentativas também, embora a taxa de sucesso ainda seja bem mais alta. Em resumo, os dados destacam a urgência de aprimorar as medidas de segurança digital e a conscientização dos usuários para prevenir tanto as tentativas quanto os crimes consumados, bem como expedir normatização interna das agências que recomende em certos casos a demarcação do item consumado e tentado, mas tal normatização e trabalho de orientar cada agente para registro pode ser substituído pelo desenvolvimento da IA que reclassifique conforme histórico, tal qual o faz os analistas em delitos selecionados e verificadas as inconsistências de natureza.

Quadro 7 - Municípios mineiros de maior incidência dos crimes de estelionato utilizando meio eletrônico (Internet ou SMS) (2018 a 2022)

Municípios Mineiros De Maior Incidência Dos Crimes De Estelionato Utilizando Meio Eletrônico (Internet Ou Sms)										
Município	**Ano**									
	2018	**%**	**2019**	**%**	**2020**	**%**	**2021**	**%**	**2022**	**%**
Belo Horizonte	1262	29,13%	2500	29,29%	4536	25,73%	7227	25,16%	8411	21,60%
Contagem	170	3,92%	392	4,59%	885	5,02%	1298	4,52%	1584	4,07%
Uberlândia	166	3,83%	355	4,16%	810	4,60%	1044	3,63%	1331	3,42%
Betim	93	2,15%	199	2,33%	366	2,08%	699	2,43%	1015	2,61%
Juiz De Fora	169	3,90%	446	5,23%	560	3,18%	679	2,36%	907	2,33%
Uberaba	80	1,85%	192	2,25%	325	1,84%	575	2,00%	743	1,91%
Divinópolis	71	1,64%	126	1,48%	163	0,92%	413	1,44%	668	1,72%

14 - Disponível em: https://www.revistaaec.com/index.php/revistaaec/article/view/1219.

Municípios Mineiros De Maior Incidência Dos Crimes De Estelionato Utilizando Meio Eletrônico (Internet Ou Sms)										
Ribeirão Das Neves	54	1,25%	89	1,04%	262	1,49%	523	1,82%	621	1,59%
Montes Claros	110	2,54%	185	2,17%	248	1,41%	329	1,15%	527	1,35%
Santa Luzia	38	0,88%	105	1,23%	214	1,24%	356	1,24%	488	1,25%
Demais Municípios Somados	2119	48,91%	3946	46,23%	9258	52,52%	15579	54,24%	22648	58,15%
Total	4332	100%	8535	100%	17627	100%	28722	100%	38943	100%

Fonte: Produzidos por meio de dados dos Armazéns de Segurança Pública de Minas Gerais, 2023.

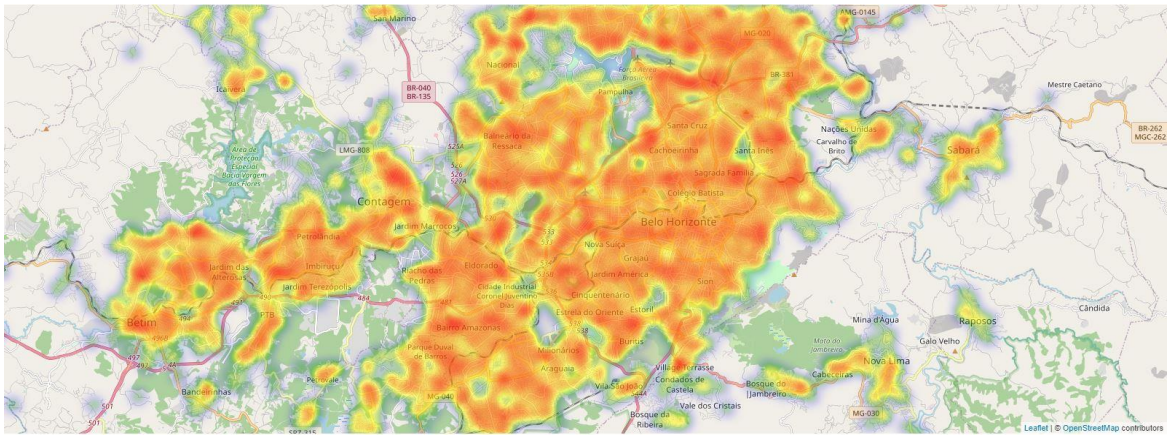
Os números de registro por ano do Quadro 7 apresentam-se na coluna do ano (2018, 2019, 2020, 2021, 2022), e a coluna de Frequência Acumulada (FAC), é indicada pela porcentagem, e significa quantos por cento aquele total de registros representa no ano de referência, que aqui utilizou por base a coluna anterior. Nota-se que a capital lidera, seguida pelas cidades satélites, e o maior fator de percentual somado está, na verdade, pulverizado nas demais cidades, o que permite inferir que os alvos/vítimas não são específicos, e os autores, por possuírem a vantagem do crime à distância e a facilidade de não ter imediatamente revelado, sem investigação, o lugar de onde praticam, atingem, precipuamente, locais com maior concentração de eletrônicos ou renda per capita maior, que permite tal acessibilidade; além de ter que se considerar o fator de que as Regiões Metropolitanas, capitais e cidades satélites detém o maior número de pessoas por espaço e necessitam da tecnologia para os serviços e funcionamento transacionais financeiros da sociedade.

Quanto à análise criminal propriamente dita dos municípios mineiros com maior incidência de crimes de estelionato utilizando meio eletrônico (Internet ou SMS), como dito, revela uma concentração significativa das ocorrências em grandes centros urbanos, com as mesmas considerações supra em relação à area rural. Belo Horizonte destaca-se como a cidade com o maior número de registros em todo o período, representando 29,13% dos casos em 2018 e, apesar de ser visível uma ligeira queda percentual, ainda lidera em 2022 com 21,60%.

Contagem e Uberlândia seguem como os próximos municípios com maior incidência, sendo que a primeira faz parte da região metropolitana de BH e a segunda é cidade satélite na região do triângulo mineiro. Ambas mantiveram consistência nos registros ao longo dos anos, embora em proporções menores que a capital. A análise temporal demonstra um crescimento contínuo no número absoluto de casos em quase todos os municípios listados, com destaque para o aumento expressivo nos demais municípios somados, que passam a representar 58,15% dos casos em 2022, que torna perceptível uma dispersão desse tipo de crime para além dos grandes centros, possivelmente relacionado à expansão do acesso à internet forçado pela impossibilidade das relações presencias à época, bem como muitos iniciantes na utilização de tecnologias em regiões mais distantes do estado e a maior vulnerabilidade dessas populações às fraudes digitais.

Em continuidade ao destrinchamento da análise, chamou atenção o ponto vermelho no Mapa 1 e os índices da Quadro 6 da região metropolitana de BH, e optou-se por demonstrar sua visualização mais aproximada no ano de 2022, ano selecionado como amostra dentro do universo para detalhamento, em decorrência de ser o último ano da análise, período de encerramento da pandemia e ter o lapso temporal mais próximo ao presente momento que os demais:

Mapa 2 - Incidência dos crimes de estelionato utilizando meio eletrônico (Internet ou SMS) na região metropolitana de Minas Gerais em 2022

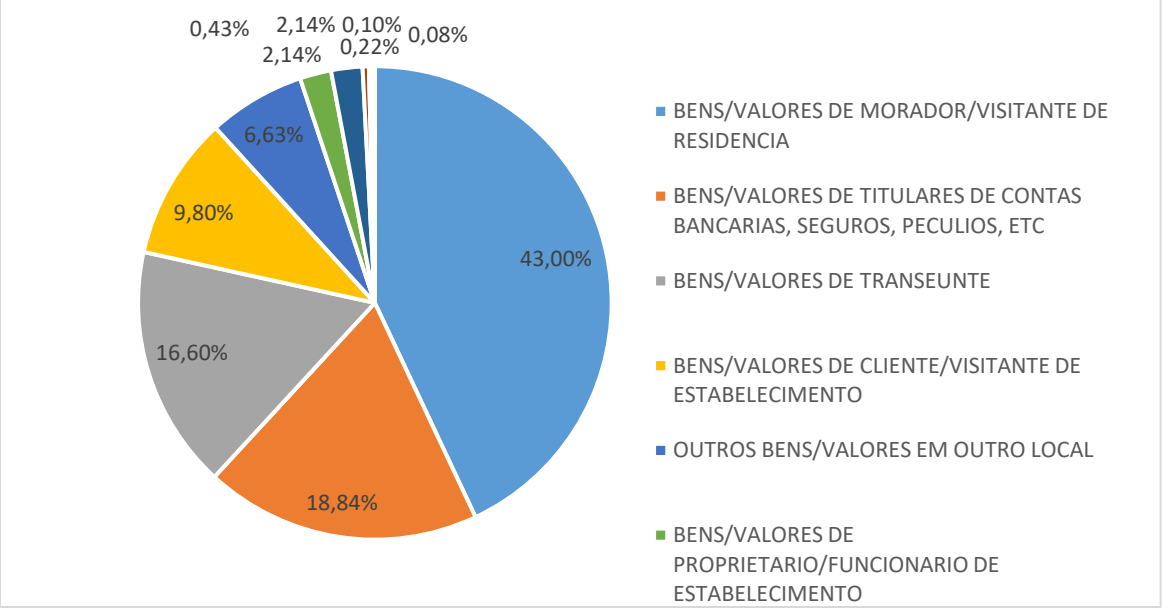


Fonte: Produzidos por meio de dados dos Armazéns de Segurança Pública de Minas Gerais, 2023.

A análise geográfica desses crimes permite identificar áreas de maior risco apenas, e é um indício de desterritorialização na distribuição da criminalidade. O mapa 2 amplia e mostra a identificação das principais localidades afetadas pelo estelionato, especialmente utilizando meios eletrônicos, de modo que áreas urbanas e densamente povoadas, como grandes centros urbanos, são as mais impactadas. No entanto, ressalta-se que correlação não implica causalidade, pois embora haja uma correlação entre altos índices de criminalidade e fatores como densidade populacional e acesso à tecnologia, isso não significa necessariamente que um fator causa o outro. Fatores socioeconômicos como desemprego, nível educacional e características demográficas (quantidade de habitantes) também desempenham um papel significativo nas taxas de criminalidade, potencialmente aumenta a vulnerabilidade de certas regiões.

A despeito do local, o Gráfico 5 foi produzido para detalhar os principais alvos dos crimes de estelionato eletrônico do mesmo ano de 2022. Ele categoriza as vítimas com base em diferentes situações, como 'morador/visitante de residência', 'titulares de contas bancárias', 'transeuntes', entre outros, conforme:

Gráfico 5 - Principais Alvos dos Crimes de Estelionato Praticados Com Uso de Meio Eletrônico (Internet ou SMS) em 2022



Fonte: Produzidos por meio de dados dos Armazéns de Segurança Pública de Minas Gerais, 2023.

14 - Disponível em: https://www.revistaaec.com/index.php/revistaaec/article/view/1219.

O Gráfico 5 foi proveniente de mais um filtro dentro do ano de todas as ocorrências de estelionato do ano de 2022, após o filtro de “meio eletrônico”, pesquisou-se novo filtro referente aos principais alvos dos crimes de estelionato, dentro do universo dos praticados com uso de meio eletrônico (Internet ou SMS) em 2022, ou seja, novo subgrupo.

Percebe-se que os bens e valores de moradores ou visitantes de residência foram os bens juridicamente tutelados mais atingidos, representando 43,00% dos casos, de modo que, por ser crime à distância, o fenômeno confirma que as pessoas estavam em suas casas e utilizando-se dos meios digitais, e não que o criminoso foi até o endereço e teve algum contato com a vítima, restando crimes e registros sem características de autores, de modo que não foi sequer possível essa análise. Em seguida, os titulares de contas bancárias, seguros e pecúlios constituíram 18,84% dos alvos, o que destaca não a vulnerabilidade financeira e a confiança que os criminosos depositam na eficácia de suas técnicas para acessar informações bancárias e valores segurados, pois esse seria o aumento do delito furto eletrônico e não da fraude eletrônica, mas sim que a Engenharia Social trabalhou ara fazer com que o próprio dono dos ativos bancários lhe fizesse ou transferisse valores sem saber que se tratava de fundo falso, pirâmides, aquisição e transações financeiras falsas, o que gera linha tênue com o furto eletrônico, mas perpassa o engano e aqui restaram registardas como fraude.

Bens e valores de transeuntes e clientes de estabelecimentos também figuram como alvos frequentes, representaram 16,60% e 9,80% respectivamente, de modo que o terceiro mais afetado pode indicar não que a exposição pública e as interações comerciais continuam sendo cenários propícios para fraudes, pois esse viés fora demonstrado pelo gráfico e tabela 1, mas sim que o item bens e valores de transeunte pode ser uma alternativa de inserção para quando não se pode determinar a correlação da vítima, espaço e autor, nem determinar que o bem atingido era de morador porque não fez referência com a moradia, e uma possível inconsistencia no registro causada pela complexidade da compreensão dos agentes, de modo que o bem juridicamente afetado, qual seja, o objeto sob o qual recai a conduta do agente, se confunde com quem foi afetado.

14 - Disponível em: https://www.revistaaec.com/index.php/revistaaec/article/view/1219.

Em números, o Gráfico 4 corresponde ao Quadro 8 representado abaixo na coluna do ano de 2022:

Quadro 8 - Crimes de estelionato utilizando meio eletrônico (Internet ou SMS), por alvos do evento

CRIMES DE ESTELIONATO UTILIZANDO O MEIO ELETRÔNICO (INTERNET OU SMS), POR ALVO DO EVENTO										
ALVO DO EVENTO	2018	%	2019	%	2020	%	2021	%	2022	%
BENS/VALORES DE MORADOR/VISITANTE DE RESIDENCIA	1340	30,93%	3114	36,49%	7048	39,98%	12461	43,38%	16746	43,00%
BENS/VALORES DE TITULARES DE CONTAS BANCARIAS, SEGUROS, PECULIOS, ETC	593	13,69%	1095	12,83%	2687	15,24%	4893	17,04%	7335	18,84%
BENS/VALORES DE TRANSEUNTE	722	16,67%	1365	15,99%	2447	13,88%	4148	14,44%	6465	16,60%
BENS/VALORES DE CLIENTE/VISITANTE DE ESTABELECIMENTO	628	14,50%	1217	14,26%	2687	15,24%	3399	11,83%	3816	9,80%
OUTROS BENS/VALORES EM OUTRO LOCAL	588	13,57%	1082	12,68%	1577	8,95%	2038	7,10%	2583	6,63%
BENS/VALORES DE PROPRIETARIO/FUNCIONARIO DE ESTABELECIMENTO	138	3,19%	210	2,46%	397	2,25%	778	2,71%	835	2,14%
BENS/VALORES DE ESTABELECIMENTO/PESSOA JURIDICA	253	5,84%	299	3,50%	519	2,94%	691	2,41%	834	2,14%
VEICULO OU EMBARCACAO	37	0,85%	79	0,93%	147	0,83%	136	0,47%	169	0,43%
BENS/VALORES DE MOTORISTA/PASSAGEIRO DE VEICULO PARTICULAR	16	0,37%	42	0,49%	46	0,26%	91	0,32%	87	0,22%
BENS/VALORES DE MORADOR DE RUA	6	0,14%	26	0,30%	46	0,26%	63	0,22%	39	0,10%
DEMAIS ALVOS SOMADOS	11	0,25%	6	0,70%	26	0,14%	24	0,08%	34	0,08%
TOTAL	4332	100%	8535	100%	17627	100%	28722	100%	38943	100%

Fonte: Produzidos por meio de dados dos Armazéns de Segurança Pública de Minas Gerais, 2023.

De forma mais ampla que o Gráfico 4, o Quadro 8 demonstra a evolução dos crimes de estelionato utilizando meio eletrônico (Internet ou SMS) em Minas Gerais de todos os anos da seleção, categorizados por diferentes alvos de delito. Como no ano de 2022, em geral os bens e valores de moradores/visitantes de residência foram os mais afetados e consistentemente apareceram como o alvo mais frequente, representando 43,00% dos casos em 2022 como detalhado no gráfico pizza. Em seguida, a análise por amostragem do ano de 2022 é confirmada e figuram os titulares de contas bancárias, seguros, pecúlios em segundo lugar, mas mostram-se diminuídas em 2022, ou seja, foram maiores nos anos anteriores propriamente pandêmicos. Apesar de uma leve redução percentual ao longo dos anos, ainda constituem uma parcela significativa, com 18,84% dos casos em 2022.

De forma peculiar, são identificados bens e valores de moradores de rua, de forma possível a indicar o fenômeno da digitalização ainda que com o indivíduo que se encontra às margens da sociedade. Notavelmente o terceiro lugar é também fenômeno social diferente pois indica o aumento contínuo na categoria de bens/valores de transeunte, que em 2022 representou 16,60% dos casos, conforme supracitado sobre a figura do transeunte. A análise desses dados reforça a necessidade de uma atenção especial a essas categorias de transeuntes e moradores

de rua, os bens de transeuntes porque se são indefinidos e confundidos com a pessoa, e os moradores de rua porque mostraram mais vulneráveis a esse tipo de crime no ápice da pandemia e ao longo do tempo diminuíram os registros.

Quadro 9 - Causa presumida dos crimes de estelionato utilizando meio eletrônico (Internet ou SMS)

CAUSA PRESUMIDA DOS CRIMES DE ESTELIONATO UTILIZANDO MEIO ELETRONICO (INTERNET OU SMS)										
CAUSA PRESUMIDA	ANO									
	2018	%	2019	%	2020	%	2021	%	2022	%
VANTAGEM ECONOMICA	4010	92,57%	8023	94,00%	16663	94,53%	27467	95,63%	37280	95,73%
OUTRAS MOTIVAÇÕES/CAUSAS	257	5,93%	407	4,77%	706	4,01%	909	3,16%	1246	3,20%
AÇÃO DE GANGUES/FACÇÕES CRIMINOSAS	36	0,83%	81	0,95%	215	1,22%	293	1,02%	342	0,88%
AUTOR COM OUTRAS DÍVIDAS	11	0,25%	11	0,13%	35	0,20%	42	0,15%	62	0,16%
NÃO INFORMADO	16	0,37%	12	0,14%	7	0,04%	7	0,02%	9	0,02%
ENVOLVIMENTO COM DROGAS	2	0,05%	1	0,01%	1	0,01%	4	0,01%	4	0,01%
TOTAL	4332	100%	8535	100%	17627	100%	28722	100%	38943	100%

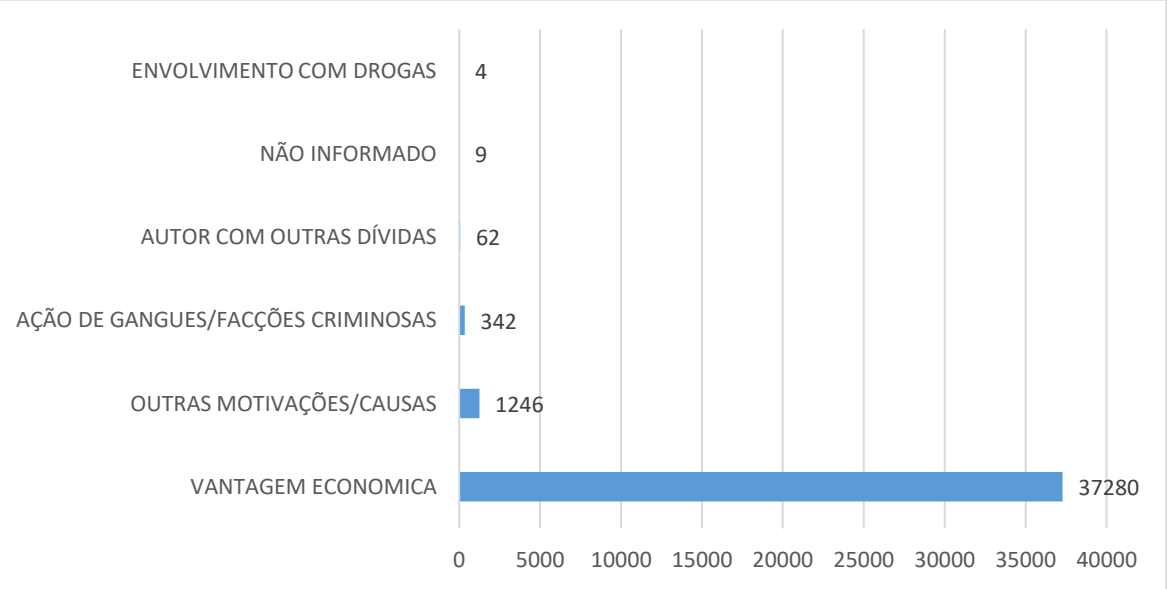
Fonte: Produzidos por meio de dados dos Armazéns de Segurança Pública de Minas Gerais, 2023.

Quanto à causa do crime, correlacionou-se com o objeto jurídico tutelado pelo Direito Penal no Título do crime tipificado no 171, qual seja, contra a propriedade. Dessa forma, o Quadro 9 detalha as causas presumidas dos crimes de estelionato utilizando meio eletrônico (Internet ou SMS) de todos o universo de registros selecionados. A vantagem econômica foi indicada como a motivação predominante, responsável por mais de 90% dos casos em todos os anos analisados e com um percentual de 91,75% em 2022. Se a maioria dos crimes é motivada por ganhos financeiros, é nítido o interesse dos criminosos em explorar a Engenharia Social para gerar mais vulnerabilidades econômicas das vítimas em potencial.

Outras motivações, incluindo ação de gangues ou facções criminosas e autor com outras dívidas, embora representem uma porcentagem muito menor, mostram que não há unanimidade e a diversidade de contextos e motivações existe. A categoria não informado apresenta números baixos, o que sugere que os campo parametrizado nesse item ter se tornado de preenchimento obrigatório resultou em uma coleta de dados mais eficaz sobre as motivações dos crimes.

Importa dizer que esses dados perfazem a necessidade de estratégias não somente preventivas, como as focadas em proteger as vítimas potenciais de explorações financeiras, mas da necessidade de criar medidas voltadas para identificar e mitigar a influência de organizações criminosas nesses delitos, conforme exposto nos capítulos anteriores, sobre a necessidade de se investigar porque as organizações criminosas estão aumentando a investida nesse meio e o que pode ser feito em contramedida. O gráfico 6 foi estruturado em barras na horizontal para fins de melhor visualização apenas do ano de 2022:

Gráfico 6 - Causa Presumida no Cometimento dos Crimes de Estelionato Praticados Por Meio Eletrônico (Internet ou SMS) em 2022



Fonte: Produzidos por meio de dados dos Armazéns de Segurança Pública de Minas Gerais, 2023.

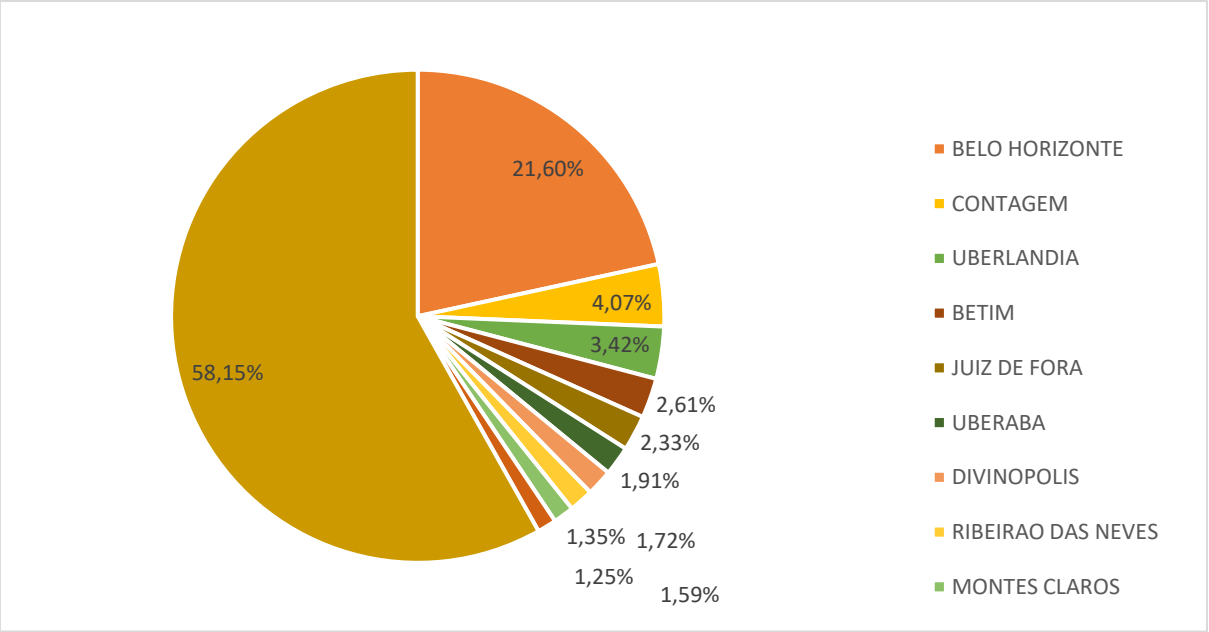
Há que se considerar também que as ações de gangues e facções podem representar um número muito maior, mas que sem investigação não é possível identificar e marcar no campo parametrizado do REDS no ato do registro. Pela amostra dos anos, essa seleção de 2022 representa e vai de acordo com os dados do Quadro 6, em que a vantagem econômica é a causa predominante, com 37.280 casos, e significa a motivação principal por trás da maioria desses crimes. Outras causas, como outras motivações/causas (1.246 casos) e ação de gangues/facções criminosas (342 casos) apareceram com menor frequência. Já autor com outras dívidas, não informado e envolvimento com drogas são causas menos comuns, com

14 - Disponível em: https://www.revistaaec.com/index.php/revistaaec/article/view/1219.

números infimamente menores, o que só reforça a predominância da busca por ganho econômico como o principal fator motivador dos crimes de estelionato eletrônico.

Por fim, com intuito de demonstrar a hipótese da desterritorialização e o atual limite da análise de hotspots nesses delitos, optou-se pelas representações mais claras referentes às localidades, de modo que o Gráfico 7 representa o Quadro 6 e deve ser observado em conjunto com o Mapa 3 de calor, pois trata-se de um Mapa intermediário entre o 1 e o 2.

Gráfico 7 - Municípios Mineiros de Maior Incidência de Crimes de Estelionato Praticados Utilizando Meio Eletrônico (Internet ou SMS) em 2022



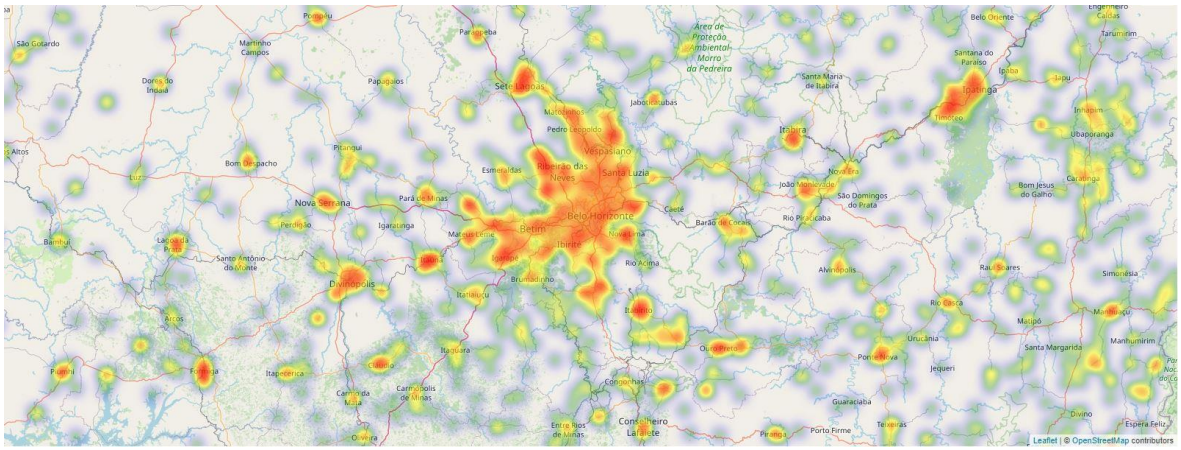
Fonte: Produzidos por meio de dados dos Armazéns de Segurança Pública de Minas Gerais, 2023.

Os 58,15% significam as demais localidades afetadas, somadas para além das cidades satélites, de modo a demonstrar a dispersão dos crimes para além dos grandes centros urbanos em 2022 e possível maior digitalização das cidades menores, mas a crescente vulnerabilidade de regiões diversas, possivelmente devido à maior conectividade e à disseminação da internet em áreas anteriormente menos expostas a esse tipo de delito, não permite inferir que os autores ali estão atuando, pois sequer estão nessas cidades de forma obrigatória. Caso trata-se de delito presencial comum, os dados poderiam sim sugerir que as estratégias de prevenção e combate ao estelionato (que fosse físico e não eletrônico) seria

14 - Disponível em: https://www.revistaaec.com/index.php/revistaaec/article/view/1219.

maior presença policial tanto nas grandes cidades quanto nas localidades menores, que agora também se encontram mais vitimadas, mas como assim não é, novas estratégias de análise e de prevenção carecem de serem desenvolvidas.

Mapa 3 - Incidência dos crimes de estelionato utilizando meio eletrônico (Internet ou SMS) em 2022



Fonte: Produzidos por meio de dados dos Armazéns de Segurança Pública de Minas Gerais, 2023.

A presença de várias manchas de calor espalhadas pelo Mapa 3 no estado confirma uma dispersão significativa dos crimes, com focos em outras cidades menores e áreas suburbanas. Ocorre que a análise geoespacial dessas incidências não é mais crucial para direcionar os esforços de prevenção e resposta ao estelionato eletrônico de maneira eficaz e localizada, pois a colocação de viaturas nessas localidades não impactará diretamente na diminuição ou na prevenção da não ocorrência de novos delitos dessa natureza.

5.2 Proposição de melhoria ao sistema REDS do estado de Minas Gerais: possibilidade de diminuição da cifra oculta por meio de inteligência artificial

Deve-se considerar que os conjuntos indicados nos gráficos respectivos às análises podem ser na realidade bem maior, em decorrência do preenchimento de forma diversa do campo parametrizado “meio utilizado” do REDS, sem considerar a cifra oculta de indivíduos que não registraram por motivos diversos. As cidades satélites indicam maior concentração de

14 - Disponível em: https://www.revistaaec.com/index.php/revistaaec/article/view/1219.

registros, não se pode determinar se as pessoas das demais localidades não quiseram deslocar até às unidades policiais para registro, o que possivelmente será diminuído com o fortalecimento das patrulhas rurais atual e estreitamento de laços com a comunidade rural no interior de Minas.

Quanto às análises de dados, a realidade presente indica que o que antes era serviço despendido por vários agentes, atualmente pode ser feito pela IA. Para demonstrar tamanha complexidade das análises, cita-se como foi realizado na pesquisa de Herculano (2022) pelo CINDS, atualmente integrado ao Centro de Gestão de Análises, quando da análise dos registros de estelionato de um mês específico selecionado para amostra em julho de 2021 em Minas Gerais:

> Dentre as mencionadas pesquisas, no âmbito da PMMG, o Centro Integrado de Defesa Social realizou a estratificação de 8.414 ocorrências de estelionato (FIGURA 3). Este número representa o total de ocorrências registradas pelas já mencionadas instituições através do sistema REDS no mês de junho de 2021 em todo o Estado. Conforme dados da entrevista detalhada na Subseção 7.2.2, **as ocorrências foram analisadas e classificadas por sete militares que executaram a tarefa, em cerca de nove dias em dedicação exclusiva** (Herculano, 2022).

A pesquisa à época obteve resultados práticos proveitosos ao perceber e analisar que o estelionato, em que pese o aumento, não era o maior índice do estado, pois estava em segundo lugar, sendo que em primeiro lugar dos delitos patrimoniais identificou o furto, medida tal que incentivou a análise pelo alto comando, que incluiu como meta de gestão de desempenho operacional em 2024 a redução dos delitos de furto. Para além da demonstração do problema social, a pesquisa motivou resultados práticos na gestão de um dos órgãos de segurança pública e impactou na vida da sociedade mineira, tal qual sua relevância casuística.

O Mestre em Ciências da Computação pela Universidade Federal de Minas Gerais e perito criminal federal Arnaldo Gomes dos Santos Júnior é especialista em inteligência artificial (IA) e sugere que esta seja mais que uma ferramenta interessante para gerir bigdata, mas também apresenta infinitas possibilidades, na visão de futuro, no que tange ao treinamento de um time de Bots (robôs virtuais com IA), pensamento tal que para o tema em questão

14 - Disponível em: https://www.revistaaec.com/index.php/revistaaec/article/view/1219.

adapta-se às possibilidades da criação de um Batalhão especialistas em áreas restritas, para resolver o que eles sejam programados. Tal projeto fora desenvolvido por Santos Júnior na Interpol, e é utilizada no âmbito das agências federais. Quanto a sua aplicabilidade nos estados, é iminente e apresenta-se em amplo desenvolvimento, sendo de interesse restrito e para tal não referenciados (Santos Júnior, Mayrink, Andrade, 2007).

Importa dizer que não se trata de substituir pessoas por IA's, mas de aperfeiçoar o serviço policial com a gestão de bigdata com a utilização de tal tecnologia, de modo que haja a interpretação única e o comandamento via conhecimento da realidade social pelo cérebro humano somado à utilização da outrora memória externa e atual interpretativa inteligência artificial. Trata-se de tecnologias tão novas que não há referências acadêmicas e importam em restrito arcabouço teórico.

Quanto às dúvidas que surgem no uso das novas ferramentas pelas agências, cita-se o trabalho publicado pela Revista de Direito Administrativo e Constitucional já em 2020, que se propôs a realizar uma breve análise acerca das potencialidades e riscos inerentes à utilização de inteligência artificial pelo Poder Público já predizia a aplicação na segurança pública e no Judiciário, bem como apresentou uma sugestão de solução para a questão com controle contínuo, por meio de uma agência ou comitê permanente a ser criado no âmbito da Administração Pública para monitorar essa matéria.

> Algumas dificuldades já enfrentadas envolvem, por exemplo, a utilização dos algoritmos para estabelecer condições de fiança e determinar o desfecho de sentenças penais. A ideia é que os algoritmos possam realizar prognósticos acerca do futuro comportamento do acusado, levando em conta o histórico de violência ou a probabilidade de cometimento de outro crime. Na formação dessa análise, o algoritmo é programado para considerar fatores demográficos, tais como idade, sexo e raça e fatores comportamentais históricos, como a idade do início do comportamento criminoso e a natureza das prisões anteriores, além de outros fatores sociais.
>
> Um caso que ensejou um debate concreto em um processo judicial ocorreu no Estado de Wisconsin (State vs. Loomis), nos Estados Unidos. A sentença de primeiro grau foi proferida com a utilização de uma ferramenta de gerenciamento de risco baseada em inteligência artificial (Correctional Offender Management Profiling for Alternative Sanctions – COMPAS) para condenar um acusado de envolvimento numa troca de tiros. A defesa alegou que, em virtude de a decisão condenatória ter utilizado um mecanismo de **inteligência artificial** para construir as razões que levaram à condenação, ela não teve acesso as razões que embasaram

14 - Disponível em: https://www.revistaaec.com/index.php/revistaaec/article/view/1219.

> essa análise, o que acarretaria uma violação à garantia do due process of law. A Suprema Corte local confirmou a condenação, mas entendeu que a utilização do mecanismo comportaria aprimoramentos.As ponderações da Suprema Corte do Estado de Wisconsin, nesse caso de utilização do COMPAS, foram feitas no sentido de reconhecer algumas limitações do sistema, tais como: a) **o desconhecimento total acerca dos fatores de risco exatos utilizados;** b) a identificação de grupos de alto risco, sem que seja possível traçar informações precisas sobre indivíduos específicos; c) alguns resultados sugerem que o sistema pode ser racialmente tendencioso; d) o sistema não havia sido validado ou regulamentado a partir de amostragem em Wisconsin; e e) o sistema não havia sido desenvolvido para uso em sentenças condenatórias criminais.
>
> Assim, como se vê, esse debate, que parece extraído de um filme de ficção científica, já faz parte da realidade vivenciada em outros países, e **é razoável acreditar que pode ser, em alguma medida, incorporada, dentro de pouco tempo, à rotina de segurança pública brasileira** e à função jurisdicional no país (Grifo nosso)[14].

Os autores expõem que primeiro passo para a mitigação dos riscos é a identificação, pelo próprio Poder Público, dos principais riscos inerentes à utilização de inteligência artificial (De Araujo; Zullo; Torres, 2020, p. 257), de modo que a fiscalização deve ser por um órgão estatal, como a Autoridade Nacional de Proteção de Dados, instituída pela Lei nº 13.853/2019, ou por uma instituição de natureza fiscalizatória, como o Ministério Público ou o Tribunal de Contas. Ademais, foi dito que monitoramento da formulação de métricas que assegurem a qualidade dos dados utilizados, para realmente atingir o resultado prático das políticas implementadas por meio da utilização de inteligência artificial. Por fim, também citam a observância de parâmetros que assegurem proteção à privacidade dos cidadãos a partir dos princípios elencados na Lei Geral de Proteção de Dados (Lei nº 13.709/2018) (De Araujo; Zullo; Torres, 2020, p. 258)

Em que pese a adiantada preocupação já em 2020, os autores foram assertivos no trabalho e todas as propostas carecem de ser observadas quando da gestão de bigdata pelas agências, trabalho que é feito hodiernamente pelas repartições específicas de cada órgão, seja PM, PC ou PF, tendo em vista a relevância das informações geridas. De igual modo, sugere-se que seja implementada a inteligência artificial na melhoria do REDS, para além das análises nas quais já tem sido aplicada, em *software* que busque nos históricos a verdadeira natureza ou reclassificação e classificação segundo a DIAO pelo contido no histórico, sem tampouco forçar o usuário do sistema que registra, mas permitindo a sugestão da natureza, haja vista

14 - Disponível em: https://www.revistaaec.com/index.php/revistaaec/article/view/1219.

que a IA já têm sido utilizadas como ferramenta de análise de dados, seria proveitoso pensar em ferramenta de implementação *bots*, como explicitado por Santos Júnior.

6 CONSIDERAÇÕES FINAIS

A Inteligência Artificial (IA) surge como uma ferramenta revolucionária, com potencial para transformar a maneira como as instituições de segurança pública operam, porque a gestão de dados por *bots* e algoritmos de IA otimizam a coleta, o processamento e a análise de grandes volumes de informações, com uma resposta mais rápida e precisa às ameaças. A automação de registros e atendimentos virtuais é tema mais polêmico, porque envolve aparente substituição do homem pela máquina, mas não se trata de retirar o contato humano, mas oportunizar que o próprio policial utilize ao gerir o sistema e realizar os registros, além de que a proposta oferece mais acessibilidade e eficiência aos serviços prestados à população, especialmente em regiões remotas, cujo paradoxo foi identificado.

A análise preditiva que atualmente já é realizada pelos analistas e *softwares*, se viabilizada pela IA, possibilita que as forças de segurança antecipem e previnam crimes com maior eficácia, já que a atual não se aplica aos delitos desterritorializados, por óbvio que permanecerão ajustadas as estratégias de empenho de acordo com as tendências identificadas nos dados históricos, mas será bem mais avançada e até rastreável por IP, com serviço de "investigação" preliminar baseada em parâmetros de atuação. No entanto, a adoção dessas tecnologias deve ser acompanhada de um planejamento cuidadoso e de considerações éticas, para assegurar que os benefícios sejam maximizados sem comprometer direitos individuais ou criar novos riscos sobre o tratamento de dados por tais bots. Em resumo, devem ser de criação e desenvolvimento próprios para maior segurança.

As conclusões deste estudo apontam para a necessidade de as agências policiais desenvolverem uma compreensão profunda do fenômeno do estelionato digital como ponto inicial de teste de novas tecnologias, como as tecnologias avançadas de IA para melhorar suas operações. A continuidade da análise nos anos seguintes será crucial para confirmar as

tendências observadas e para ajustar as abordagens de combate ao estelionato em ambiente virtual, de modo que a segurança pública não perca espaço virtual e evolua de forma integrada e eficiente em resposta a esse novo cenário criminal.

Os resultados obtidos permitem avaliar que o aumento dos registros do crime de estelionato digital indica um fenômeno criminal significativo e exponencial, no sentido de indicar, por meio da técnica da análise preditiva, considerável possibilidade de aumento sequencial nos anos vindouros, tal qual observado nos índices também de 2023, mas não destrinchados nessa pesquisa, que delimitou o período de 2018 a 2022.

Atualmente a base de dados de segurança pública em Minas Gerais é composta por um grande Big Data integrado pelas polícias e órgão de segurança pública e defesa civil. Os sistemas seguem em pleno desenvolvimento pelos centros de tecnologia próprio dos órgãos, e permitem avalições cada vez mais precisas , posto que a análise criminal ainda este ano de 2024 passou a ter centro próprio na PMMG denominado como Centro de Gestão de Análises (CGA), o que implica em profissionais capacitados trabalhando em conjunto com a tecnologia, de forma que pesquisas anteriores que necessitavam de informações que estavam em bancos de dados diversos e despendiam diversos profissionais para mineração dos dados registro por registro, agora podem ser executadas por *softwares* e inteligência artificial de forma imediata. O resultado observado indica um grande avanço no que tange à análise preditiva no e para o serviço policial, e que indica possíveis caminhos a serem percorridos quando da estipulação de novas estratégias de atuação contra os cibercrimes, especificamente no que tange ao estelionato.

A criação dos centros de análise produzem a antiga ideia de gestão administrativa tayloriana de especialidade do serviço e facilitam o contínuo monitoramento das agências, ainda que mantidas as ordenações da burocracia de atuação conjunta com as demais entidades da federação, a especialidade e a ação integrada dentro da perspectiva de administração em rede (de modo que todos os órgãos de segurança pública do Estado de Minas consigam se comunicar e agir em conjunto com as demandas da sociedade), e a liberação do SIGOP Estatística (sistema de gestão operacional) para os policiais, fortalece as agências e resulta em avanços de desenvolvimento de tecnologias específicas para as demandas sociais, pois é

realizada a análise com mais rapidez e a percepção do problema social pelos registros possibilita propor soluções para a demanda social presente.

Quando do projeto dessa pesquisa em 2022, uma das possíveis hipóteses era a integração dos diversos sistemas de segurança pública que não dialogavam, e ao término dessa etapa de análise de resultados, identifica-se a criação da Base Integrada de Segurança pública (BISP) como maior avanço de informações em rede, que aumentam a comunicação, fiscalização e a gestão entre Polícias e Judiciário, por meio do acesso à informação.

Quanto à metodologia da estrutura científica, após exposição dos dados em diálogo com o arcabouço teórico, retoma-se o problema inicial proposto para este artigo: como as agências policiais podem enfrentar os desafios apresentados pelo "fenômeno social complexo" do estelionato em ambiente virtual? Inicialmente buscou-se caracterizar o contexto de emergência dos crimes cibernéticos por meio de uma breve contextualização que levou em consideração as preocupações internacionais, nacionais e normativas para tratar do fenômeno.

Ao realizar a exposição dos dados percebeu-se que somente é possível identificar as vítimas de estelionato digital, uma vez que autor e vítima não estão no mesmo local físico durante a consumação do delito. Isso apresenta uma variável importante em termos de como o geoprocessamento é realizado para esse tipo de delito. As vulnerabilidades de segurança digital, presentes devido à rápida adoção de tecnologias cibernéticas, se constitui variável importante no aumento do estelionato em ambiente virtual. A incapacidade de garantir a proteção adequada das informações pessoais e financeiras cria oportunidades para criminosos explorarem essas brechas, realizando atividades fraudulentas que podem resultar em ganhos ilícitos.

A natureza globalizada do crime cibernético, permitida pelo mundo digital conectado, faz com que o estelionato em ambiente virtual ultrapasse fronteiras e torne-se um desafio difícil para a repressão qualificada. As especificidades de cada organização policial brasileira e a relação entre elas são variáveis importantes na elaboração de propostas de enfrentamento desse novo fenômeno criminal complexo. Há necessidade de estabelecer um sistema

eficiente, eficaz e efetivo, que respeitando as *expertises* das agências policiais, atue pautado em protocolos integrados, com definição clara de rotinas e fluxo. Uma atuação sinergética baseada em compartilhamento de dados específicos.

Junta-se a essa dinâmica procedimental, a alocação de recursos para capacitação em crimes cibernéticos para as policiais, de acordo com seus diplomas legais. Os treinamentos devem ser contínuos de forma a criar competências necessárias aos policiais diante das rápidas transformações tecnológicas. A gestão pública deve buscar soluções e modelos que promovam parcerias com o setor privado, universidades e especialistas em cibersegurança para compartilhar conhecimentos e recursos.

As agências policiais responsáveis pela investigação dos delitos necessitam aprimorar tecnicamente suas rotinas de forma a identificar cirbercriminosos para uma atuação segura. Em resumo, o modelo de atuação da polícia brasileira em crimes cibernéticos precisa de melhorias significativas em termos de recursos, treinamento, colaboração e legislação, mas principalmente em relação a gestão e a cultura entre as agências.

A aplicação de tecnologia avançada é essencial para reprimir os golpes que tem se utilizado de técnicas de colarinho branco, especialmente no contexto digital. A análise de dados, a mineração de dados e as ferramentas de cibersegurança são usadas para identificar atividades suspeitas, rastrear transações e coletar evidências digitais. Em última análise, o enfrentamento eficaz aos crimes supracitados requer uma abordagem multidisciplinar e colaborativa, pois envolve conhecimento técnico, investigativo e legal para desvendar práticas ilícitas complexas e garantir a prestação de serviços policiais à sociedade.

O presente estudo buscou abordar o complexo fenômeno do estelionato digital inserido no contexto mais amplo dos crimes cibernéticos com foco específico na aplicação das Ciências Policiais. Em um cenário em que a digitalização acelerada das interações sociais e econômicas trouxe novos desafios para as agências policiais, foi crucial entender como o estelionato, particularmente aquele praticado por meio eletrônico, se manifestou durante e após o período da pandemia de Covid-19.

A análise quantitativa dos dados revelou um crescimento significativo dos crimes de estelionato em Minas Gerais pela migração das práticas criminosas do ambiente físico para o virtual. Este fenômeno foi acompanhado por uma dispersão geográfica dos crimes, com grande parte das ocorrências agora se distribuindo entre várias localidades menores, além dos grandes centros urbanos. Esses resultados permitiram a elaboração de sugestões práticas que perfizeram a necessidade de as Ciências Policiais desenvolverem novas metodologias com a utilização de inteligência artificial para fins de melhorar a eficácia na elucidação dos crimes e reduzir a cifra oculta.

Com a sugestão de implementação de melhoria de sistema, foi possível, após a revisão bibliográfica e a análise criminal, responder à questão central: como as agências policiais podem enfrentar os desafios apresentados pelo "fenômeno social complexo" do estelionato em ambiente virtual. A hipótese levantada foi a necessidade de, primeiramente, conhecer esse fenômeno invisível em sua multidimensionalidade e complexidade. Em conclusão, destacou-se a importância de criar rotinas e protocolos integrados entre agências policiais, instituições públicas e privadas e, para muito além do que combater esse tipo de cibercrime patrimonial, manutenir o estado como força pública legítima e atuante. Por fim, a capacitação dos envolvidos para o desenvolvimento de competências necessárias já era considerada essencial, mas foi sugerida solução econômica de gestão de tempo, efetividade e resultado.

Com base nessa problemática e na hipótese apresentada, o objetivo geral atingido foi refletir sobre o "fenômeno criminal complexo" do estelionato em ambiente virtual, entendido como uma modalidade de cibercrime patrimonial. Os objetivos específicos foram: analisar teoricamente a multidimensionalidade dessa modalidade criminosa e apresentar dados quantitativos que esclarecessem esse complexo fenômeno criminal em Minas Gerais.

Quanto aos gráficos, representaram a análise estatística e o filtro dos registros anuais e demonstraram um aumento significativo na incidência de crimes de estelionato a partir do início da pandemia do Covid-19, comprovado especialmente o crescimento nas categorias de fraudes e crimes cometidos por meio eletrônico (Internet ou SMS). Esses dados indicaram que, enquanto o universo dos crimes patrimoniais em Minas Gerais aumentou como um todo,

houve uma migração notável do ambiente físico para o virtual, como inclusive figurava do projeto inicial de pesquisa, e que ao tempo do início da pesquisa não foi localizado o termo teoria da migração em outras fontes para menção, ao qual se atribui autoria, mas durante o transcorrer dos trabalhos e após submissões diversas, localizou-se o termo/teoria atualmente já citado e demonstrado pelo Fórum Brasileiro de Segurança Pública[15].

Foi realizado recorte para delimitação do objeto, conforme visto no Gráfico 2, ao focar especificamente nos delitos de estelionato que utilizam meios eletrônicos, e foi possível demonstrar um crescimento exponencial anual dos crimes que alcançaram recordes de registros no período da amostra 2022, que também foram mais detalhados. A pesquisa contínua realizada ainda em 2023 corrobora com essa tendência e confirma que o estelionato por meios eletrônicos se consolidou como um fenômeno criminal predominante e a análise dos resultados foi detalhada nos gráficos apresentados ao longo daquele capítulo, de modo que confirmou uma evolução significativa dos crimes de estelionato em Minas Gerais, particularmente no período de 2018 a 2022.

Os gráficos indicam que o número total de crimes de estelionato aumentou em todo o estado, mas que Belo Horizonte permanece como o epicentro, seguido por outras cidades como Contagem e Uberlândia. Contudo, em 2022 a análise também aponta para uma dispersão dos crimes para municípios menores, sugerindo uma expansão da vulnerabilidade em áreas fora dos grandes centros urbanos, estabelecido o paradoxo de grandes capitais e/ou pulverização no interior.

Outro aspecto antes esperado e ora demonstrado pelos números foi a predominância da vantagem econômica como a motivação principal por trás desses delitos. Em suma, os dados não apenas indicam um aumento quantitativo dos crimes de estelionato, mas também uma transformação qualitativa no modus operandi dos criminosos, que agora exploram mais intensamente as plataformas digitais, confirmando a migração, que compara esse índice com os delitos patrimoniais físicos, não tendo sido mais objeto desse trabalho após as publicações diversas.

15 - Disponível em: https://fontesegura.forumseguranca.org.br/migracao-dos-crimes-violentos-de-rua-para-crimes-digitais/.

Mesmo com a hipótese de que a pandemia de Covid-19 pudesse ser um *outlier* na análise estatística, os dados permitem inferir que o aumento não foi um evento isolado, mas pode ser sim o marco de um novo padrão criminal, cuja continuidade no ambiente virtual persistiu após o término da pandemia. Isso porque o aumento dos registros se repete ano a ano, e não foi identificado medida variável de desvio considerável ao longo da análise. Pressupõe-se na estatística que o período de Covid-19 signifique um *outlier* (ponto fora da curva), mas o que se pode inferir é que os aumentos coincidem com o início o período pandêmico e permanecem com seu término, de forma que a análise de 2024 será igualmente importante para a demonstração da continuidade delitiva no ambiente virtual mesmo após o término da Pandemia, o que significa não um outlier, mas um marco inicial de um novo fenômeno criminal.

Portanto, a análise temporal não deixou de ser essencial para identificar dessas tendências e compreensão se a criminalidade digital continuará em ascensão ou passará por declínio, como em 1955 ocorreu com a geração conforme publicado por Hungria, de modo que fomentou a época novas abordagens de combate e prevenção aos delitos patrimoniais, mas nova onda de criminalidade física despontou nos anos seguintes. Se se trata de um ciclo histórico de criminalidade migratória ou definitiva mudança pelos ditames da globalização, apenas a manutenção da pesquisa no decurso do tempo poderá responder. A continuidade do monitoramento pelas agências em anos futuros será crucial para confirmar se essas tendências se mantêm e para desenvolver novas abordagens que possam mitigar os impactos desse fenômeno criminal em constante migração e evolução.

Diante das descobertas, propõe-se que o sistema REDS do Estado de Minas Gerais seja aprimorado, ao incorporar ferramentas de inteligência artificial para auxiliar na categorização e análise dos boletins de ocorrência no momento da confecção. Tal medida pode potencialmente reduzir a cifra oculta decorrente de naturezas erradas, mas também facilitar o registro online pelo atendiemento IA 190 bots, o que contribui para melhor atendimento ao público pela facilidade e também para as análises estatísticas no que tange à uma melhor compreensão da realidade criminal e por conseguinte a elaboração de estratégias mais eficazes de prevenção e combate ao estelionato digital. Além disso, a integração de dados entre diferentes instituições e a capacitação contínua dos profissionais envolvidos são

imperativos para enfrentar os desafios impostos por esse novo paradigma de criminalidade patrimonial.

Por fim, a respeito da Engenharia Social e o delito de estelionato digital percebeu-se que na prática, os golpes podem ser realizados de muitas maneiras, tanto tecnológicas quanto humanas, mas especificamente nos que envolvem tecnologia, o usuário acredita que interage com um sistema ou uma pessoa real, e por isso divulga informações confidenciais. Seria semelhante ao erro de tipo estudado pelo Direito, no que tange à uma falsa percepção da realidade, mas nesse caso não pelo autor, mas sim pela vítima.

Conclui-se o que se pode chamar de erro de tipo às avessas, termo produto dessa pesquisa e possível análise pelo legislativo no que tange à possível alteração do tipo, orientada pelo Direito Penal com enfoque na vítima e que poderia, como forma de tutela em processo criminal, declarar o erro de tipo em um delito que não se tem a identidade do autor sem demorada investigação, além de ser esta investigação condicionada à representação da vítima (representar contra quem?), e sem disponibilidade das agências de atender tamanha demanda dos atos investigativos. O novo inciso, após acurado estudo, deveria declarar de imediato o vício de percepção de realidade da vítima, anular o negócio jurídico, bloquear e cancelar de imediato todas as transações financeiras realizadas pela vítima e esse ato processual liminar seria aplicado já pela autoridade policial, para além das burocracias clássicas dos imites de competência e de acordo com as novas vertentes de sociedade em rede e problemas complexos, sem prejuízo da análise definitiva judicial.

Sabe-se que, a despeito da separação das esferas para proteção do stellius já trabalhado por Hungria no século passado, o Direito Civil prevê tais institutos de tutela antecipada de urgência e emergência, mas que devido ao acesso à justiça, ainda que com a ampliação dos órgãos garantidores, não conseguiria atender aos bloqueios com celeridade a tempo de salvaguardar a não transferência ou saque dos valores até a tutela. Os poucos casos em que são alcançados tais bloqueios se dão por escritórios de advocacia especializados e de alto valor de pagamento de honorários, o que também não garante o acesso do serviço para sociedade. Na abordagem humana, os ataques exploram respostas previsíveis a gatilhos psicológicos e a extensão desses ataques é limitada apenas pela criatividade do hacker, de

modo que confirma a necessidade de novas estratégias de políticas públicas de segurança para mitigar esses riscos.

Por fim, os policiais do futuro - quase presente - precisarão ser mais que decoradores de leis e gestores de sistemas. Passarão a ser o ponto de pensamento e reflexão sobre os problemas sociais que se apresentarão e terão que desenvolver a criatividade para criar soluções bots eficientes para cada realidade social, já que a linguagem de sistemas fora decodificada e os comandos serão diretos, sem esquecer, por óbvio, dos problemas do mundo físico latente e da dignidade da pessoa humana, da dificuldade e da nobreza de tratar e lidar pessoalmente com o ser humano nos mais diversos desafios sociais, que apenas mudam e migram de cenário de tempos em tempos.

REFERÊNCIAS

BARRETO, A. G.; FONSECA, R. M. T. **Curso Detecção de Fraudes Eletrônicas em Períodos de Crise.** Ministério da Justiça e Segurança Pública, Secretaria de Gestão e Ensino em Segurança Pública, Diretoria de Ensino e Pesquisa, Coordenação-Geral de Ensino, Coordenação de Ensino a Distância.

BAUMAN, Zygmunt. **As consequências humanas da globalização.** Rio de Janeiro: Zahar, 1999.

BAUMAN, Zygmunt. **Confiança e medo na cidade.** Rio de Janeiro: Zahar, 2009.

BAUMAN, Zygmunt; LYON, David. **Vigilância líquida.** Rio de Janeiro: Zahar, 2014.

BEATO, Cláudio; PEIXOTO, Betânia Totino; ANDRADE, Mônica Viegas. **Crime, oportunidade e vitimização.** Revista Brasileira de Ciências Sociais, v. 19, n. 55, São Paulo, 2004.

BECK, Ulrich. **Sociedade do risco: rumo a uma outra modernidade.** São Paulo: ED. 34, 2010.

BITTNER, Egon. **Aspectos do trabalho policial.** 2. ed. São Paulo: Edusp, 2003. 254 p.

BRASIL. **Decreto-Lei n.º 2.848, de 7 de dezembro de 1940. Código Penal.** Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 12 abr. 2024.

BRASIL. **Decreto-Lei n.º 3.689, de 3 de outubro de 1941. Código de Processo Penal.** Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm. Acesso em: 12 abr. 2024.

BRASIL. **Decreto n.º 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.** Disponível em: http://www.planalto.gov.br/CCIVIL_03/_Ato2011-2014/2014/Lei/L12965.htm. Acesso em: 12 abr. 2024.

BRASIL. **Ministério da Justiça e Segurança. Curso de crimes cibernéticos.** Brasília: Secretaria de Gestão e Ensino em Segurança Pública, 2020.

BRASIL. **Ministério da Justiça e Segurança Pública. Detecção de fraudes eletrônicas em período de crise.** Brasília: Secretaria de Gestão e Ensino em Segurança Pública, 2020.

BRASIL. **Ministério Público Federal. Manual prático de investigação de crimes cibernéticos.** São Paulo: Comitê Gestor da Internet no Brasil, 2006.

CALDEIRA, Teresa Pires. **Cidade de muros. Crime, segregação e cidadania em São Paulo.** São Paulo: Ed. 34 / Edusp, 2000.

CASTEL, Robert. **A dinâmica dos processos de marginalização: da vulnerabilidade à "desfiliação".** In: Caderno CRH, Salvador, nº. 26/27, p. 19-40, jan./dez. 1997.

CASTEL, Robert. **A insegurança social: o que é ser protegido?** Petrópolis: Vozes, 2005.

CERT.br – Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. **Estatísticas.** Disponível em: https://stats.cert.br/. Acesso em: 31 jul. 2024.

COHEN, Lawrence; FELSON, Marcus. Social change and crime rate trends: a routine approach. American Sociological Review, 44: 588-608, 1979.

COLEMAN, James William. **A elite do crime - para entender o crime do colarinho branco.** São Paulo: Ed. 5 / Manole, 2005.

DE ARAUJO, Valter Shuenquener; ZULLO, Bruno Almeida; TORRES, Maurílio. **Big Data, algoritmos e inteligência artificial na administração pública: reflexões para a sua utilização em um ambiente democrático.** A&C-Revista de Direito Administrativo & Constitucional, v. 20, n. 80, p. 241-261, 2020. Disponível em: https://www.revistaaec.com/index.php/revistaaec/article/view/1219. Acesso em: 31 jul. 2024.

FARIA, Antônio Hot Pereira de; MICHALICK, Miller França. **Policiamento de Hot Spots: teoria e prática.** Belo Horizonte: Academia do Prado Mineiro, 2024. 200 p.

FARIA, Thiago Rodrigues de. **A teoria do domínio do fato de Claus Roxin: e sua aplicabilidade ao Direito Penal Econômico.** Belo Horizonte, MG: Dialética, 2024. E-book. Disponível em: https://plataforma.bvirtual.com.br. Acesso em: 08 jul. 2024.

GARTNER, Inc. **Gartner Announces the Top Government Technology Trends for 2024.** Sydney, Australia: Gartner, 16 abr. 2024. Disponível em: https://www.gartner.com/en/newsroom/press-releases/2024-04-16-gartner-announces-the-top-government-technology-trends-for-2024. Acesso em: 4 ago. 2024.

HAMADA, Hélio Hiroshi; MOREIRA, Renato Pires [Orgs.]. **Inteligência de segurança pública e cenários prospectivos da criminalidade.** Série inteligência, estratégia e defesa social. Belo Horizonte: Editora D'Plácido, 2016.

HERCULANO, Alexandre Junqueira. **Os impactos da internet para a prática do crime de estelionato.** Belo Horizonte, 2022.

HUNGRIA, Nélson; DOTTI, René Ariel. **Comentários ao código penal: dec.-lei n. 2.848, de 7 de dezembro de 1940; lei n. 7.209, de 11 de julho de 1984.** Rio de Janeiro, RJ: GZ, 2017. E-book. Disponível em: https://plataforma.bvirtual.com.br. Acesso em: 08 jul. 2024.

KAHN, Túlio. Migração dos crimes violentos de rua para crimes digitais. Fontes Segura. Disponível em: https://fontesegura.forumseguranca.org.br/migracao-dos-crimes-violentos-de-rua-para-crimes-digitais/. Acesso em: 31 jul. 2024.

KASPERSKY. **Cybermap Stats.** Disponível em: https://cybermap.kaspersky.com/pt/stats. Acesso em: 15 jul. 2024.

KASPERSKY. **What is an IP address?** Disponível em: https://www.kaspersky.com.br/resource-center/definitions/what-is-an-ip-address. Acesso em: 10 jul. 2024.

KASPERSKY. **What is social engineering?** Disponível em: https://www.kaspersky.com.br/resource-center/definitions/what-is-social-engineering. Acesso em: 15 jul. 2024.

LEAL, Gabriel Rodrigues. **Fundamentos das ciências policiais: da barbárie à segurança pública.** Curitiba: CRV, 2016. 360 p.

LEITE, Ricardo Gonçalves Pessoa. **A Polícia Militar de Minas Gerais na era dos crimes cibernéticos: diretrizes para uma proposta de estratégia preventiva e protocolo de atuação.** Monografia para Especialização em Gestão Estratégica de Segurança Pública – CEGESP. Academia de Polícia Militar de Minas Gerais e Fundação João Pinheiro. Belo Horizonte, 2018.

LOIOLA, Luciano da Silva [et al.]. **Tópicos especiais em ciências policiais.** Brasília, DF: Ultima Ratio, 2022. 320 p.

MACHADO JUNIOR, Renato Quirino; COTTA, Francis Albert. **Olhares da complexidade no Aglomerado da Serra em Belo Horizonte: notas autoetnográficas sobre o mundo do crime e sua gramática moral iconográfica.** O Alferes, Belo Horizonte, v. 32, n. 81, p. 140-182, jan./jun. 2022.

MARTINS, Alexander Dias. **A atuação da PMMG na prevenção e repressão aos crimes cibernéticos.** Belo Horizonte: Fundação João Pinheiro, 2010.

MITNICK, Kevin D.; SIMON, William L. **A arte de enganar.** São Paulo: Pearson, 2003.

MORIN, Edgar. **Introdução ao pensamento complexo.** Tradução Eliane Lisboa. Porto Alegre: Sulina, 2015. 120 p.

MOURA, Grégore Moreira de. **Curso de direito penal informático.** Belo Horizonte: Editora D'Plácido, 2021.

NAZARENO, Marcineiro (org.). **Ciências policiais, conceito, objeto e método da investigação científica.** São José do Rio Preto, SP: HN, 2023.

POLÍCIA CIVIL DO ESTADO DE MINAS GERAIS. **Cartilha de golpes.** Belo Horizonte: PCMG, 2022. 25 p. Disponível em: https://www.policiacivil.mg.gov.br/pagina/servico-cartilhas-pcmg. Acesso em: 06 jul. 2024.

PRIULI, R. M. **A abordagem hermenêutico-fenomenológica e a epistemologia da complexidade.** Revista Letra Magna, v. 19, n. 34, p. 1-18, 2023. Disponível em: https://ojs.ifsp.edu.br/index.php/magna/article/view/2398. Acesso em: 6 maio. 2024.

SANTOS, Luis Miguel Luzio dos; PELOSI, Edna Marta; OLIVEIRA, Bernardo Carlos Spaulonci Chiachia Matos de. **Teoria da complexidade e as múltiplas abordagens para compreender a realidade social.** Serviço Social Revista, Londrina, v. 14, n. 2, p. 47-72, jan./jun. 2012.

SANTOS, Luciano Cirino dos. **A fraude como elemento essencial para a configuração da tipicidade objetiva dos crimes contra a ordem tributária praticados por particulares.** Belo Horizonte, MG: Dialética, 2024. E-book. Disponível em: https://plataforma.bvirtual.com.br. Acesso em: 08 jul. 2024.

SAWAYA, Márcia Regina. **Dicionário de informática e internet.** São Paulo: Nobel, 1999.