REVISTA DCS
FUNDADA EN 2000

PROATIVIDADE EM CIBERCRIME NA PF (2023–2025): PARA CADA PRISÃO, 2–3 MANDADOS DE BUSCA E APREENSÃO

PROACTIVITY IN CYBERCRIME AT THE FEDERAL POLICE (2023–2025): FOR EVERY ARREST, 2–3 SEARCH AND SEIZURE WARRANTS

PROACTIVIDAD EN CIBERCRIMEN EN LA PF (2023–2025): POR CADA ARRESTO, 2–3 ÓRDENES DE REGISTRO Y ALLANAMIENTO

Edinaldo Inocêncio Ferreira Junior[1], Mayara Magna Oliveira Tavares[2], Maria Cristina Ferreira Marques[3], Cesar Mauricio de Abreu Mello[4], Raylene Rodrigues de Sena[5]

DOI: 10.54899/dcs.v22i85.3640
Recibido: 23/10/2025 | Aceptado: 24/10/2025 | Publicación en línea: 04/12/2025.

RESUMO

O estudo analisa a eficiência operacional da Polícia Federal no enfrentamento ao crime cibernético no Brasil, com base na proporção entre mandados de busca e apreensão e prisões (flagrantes, preventivas e temporárias) realizadas entre 2023 e 2025, com foco na Região Norte e no estado do Amazonas. A pesquisa parte da justificativa de compreender como a atuação estratégica da instituição reflete sua capacidade de resposta em um cenário de crescente complexidade tecnológica e risco informacional. O problema de pesquisa centra-se na ausência de métricas consolidadas para avaliar a maturidade das ações de inteligência cibernética no país. Fundamentado nas abordagens de intelligence-led policing, na teoria da sociedade de risco e nos modelos de governança pública em contextos periféricos, o estudo adota uma metodologia quantitativa e descritiva, baseada em dados públicos consolidados da Polícia Federal, tratados por meio de estatística descritiva e projeção linear. Os resultados revelam que, para cada prisão, foram expedidos de dois a três mandados de busca e apreensão, evidenciando uma atuação predominantemente proativa e orientada por inteligência. Observam-se, contudo, desigualdades regionais marcantes no Amazonas, associadas à limitação tecnológica e à ausência de delegacias especializadas. Conclui-se que o indicador MBAs/Prisões constitui uma métrica inovadora de desempenho, capaz de subsidiar políticas públicas voltadas à cibersegurança e à governança digital.

Palavras-chave: Forense Digital. Governança Cibernética. Indicadores de Desempenho. Inteligência Policial. Medidas Cautelares.

[1] Mestrando em Segurança Pública, Cidadania e Direitos Humanos, Universidade do Estado do Amazonas (UEA), Manaus, Amazonas, Brasil. E-mail: edinaldoferreira.adv@gmail.com Orcid: https://orcid.org/0009-0003-5675-8398
[2] Mestrando em Segurança Pública, Cidadania e Direitos Humanos, Universidade do Estado do Amazonas (UEA), Manaus, Amazonas, Brasil. E-mail: mayaramagna@yahoo.com.br Orcid: https://orcid.org/0009-0007-6743-1322
[3] Mestrando em Segurança Pública, Cidadania e Direitos Humanos, Universidade do Estado do Amazonas (UEA), Manaus, Amazonas, Brasil. E-mail: mcfm.msp25@uea.edu.br Orcid: https://orcid.org/0009-0009-0268-4315
[4] Doutor em Desenvolvimento Sustentável do Trópico Úmido, Universidade Federal do Pará (UFPA), Manaus, Amazonas, Brasil. E-mail: mello.cesar@gmail.com Orcid: https://orcid.org/0000-0003-3086-2624
[5] Doutora em Administração, Universidade Federal de Minas Gerais (UFMG), Manaus, Amazonas, Brasil. E-mail: rsena@uea.edu.br Orcid: https://orcid.org/0000-0001-5263-6981

ABSTRACT

This study analyzes the operational efficiency of the Brazilian Federal Police in combating cybercrime, based on the ratio between search and seizure warrants and arrests (in flagrante, preventive, and temporary) carried out between 2023 and 2025, focusing on the Northern Region and the state of Amazonas. The research aims to understand how the institution's strategic performance reflects its responsiveness within an increasingly complex technological and informational risk environment. The problem lies in the lack of consolidated metrics to assess the maturity of cyber intelligence actions in Brazil. Grounded in the approaches of intelligence-led policing, risk society theory, and public governance models in peripheral contexts, the study adopts a quantitative and descriptive methodology, using consolidated public data from the Federal Police, analyzed through descriptive statistics and linear projection. Results show that for each arrest, two to three search and seizure warrants were issued, revealing a predominantly proactive and intelligence-driven operational pattern. However, regional disparities persist in Amazonas due to limited technology and the absence of specialized units. It is concluded that the MBAs/Arrests ratio constitutes an innovative performance indicator capable of guiding public policies for cybersecurity and digital governance.

Keywords: Cyber Governance. Digital Forensics. Performance Indicators. Police Intelligence. Precautionary Measures.

RESUMEN

El estudio analiza la eficiencia operativa de la Policía Federal de Brasil en el combate al ciberdelito, con base en la proporción entre órdenes de registro e incautación y detenciones (en flagrancia, preventivas y temporales) realizadas entre 2023 y 2025, con énfasis en la Región Norte y el estado de Amazonas. La investigación busca comprender cómo el desempeño estratégico de la institución refleja su capacidad de respuesta ante un entorno de creciente complejidad tecnológica y riesgo informacional. El problema de investigación se centra en la ausencia de métricas consolidadas para evaluar la madurez de las acciones de inteligencia cibernética en el país. Basado en los enfoques de intelligence-led policing, la teoría de la sociedad del riesgo y los modelos de gobernanza pública en contextos periféricos, el estudio adopta una metodología cuantitativa y descriptiva, utilizando datos públicos consolidados de la Policía Federal, tratados mediante estadística descriptiva y proyección lineal. Los resultados muestran que por cada detención se emitieron entre dos y tres órdenes de registro e incautación, revelando un perfil operativo predominantemente proactivo y orientado por la inteligencia. No obstante, se observan desigualdades regionales significativas en Amazonas, vinculadas a la limitación tecnológica y a la falta de unidades especializadas. Se concluye que el indicador Órdenes/Detenciones constituye una métrica innovadora de desempeño, capaz de apoyar políticas públicas en ciberseguridad y gobernanza digital.

Palabras clave: Gobernanza Cibernética. Indicadores de Desempeño. Informática Forense. Inteligencia Policial. Medidas Cautelares.

INTRODUÇÃO

O avanço da sociedade digital trouxe ganhos econômicos e sociais inegáveis, mas também favoreceu o surgimento de novas modalidades criminosas. Entre elas, os crimes cibernéticos destacam-se pelo caráter transnacional, pela sofisticação técnica e pela capacidade de gerar impactos expressivos. Segundo a Organização Internacional de Polícia Criminal (ICPO-Interpol, 2022), a criminalidade virtual figura entre as maiores ameaças contemporâneas, com prejuízos financeiros comparáveis aos do tráfico internacional de drogas. No Brasil, o cenário reflete a fragilidade da governança digital, com altos índices de ataques e limitada capacidade estatal de resposta (Cruz; Rodrigues, 2018). A Polícia Federal (PF), responsável pela repressão a crimes de alta complexidade, assume protagonismo no combate ao cibercrime, mas há escassez de estudos empíricos que avaliem a eficiência operacional de suas ações. A literatura tem privilegiado análises normativas e jurídicas, como as discussões sobre impunidade (Cruz; Rodrigues, 2018), tensões entre vigilância e privacidade (Moreira; Razzolini Filho; Adrião, 2023) e limites da investigação preliminar (Colli, 2009), carecendo de métricas que relacionem mandados de busca e apreensão (MBAs) e prisões em operações digitais.

Diante desse contexto, o problema de pesquisa busca responder: qual é a proporção entre MBAs e prisões expedidas nas operações da PF contra o crime cibernético no Brasil, entre 2023 e 2025, e o que essa proporção revela sobre a maturidade estratégica da atuação policial, especialmente na Região Norte e no Amazonas? O objetivo geral é analisar o perfil da resposta policial no enfrentamento ao cibercrime, a partir dessa proporção. Especificamente, pretende-se: (i) calcular a proporção MBAs/Prisões por unidade federativa; (ii) examinar sua evolução e variações regionais; (iii) destacar o Amazonas, dada sua vulnerabilidade digital; e (iv) discutir implicações para eficiência operacional e políticas de segurança pública.

A relevância científica reside em preencher lacunas sobre mensuração de eficiência no combate ao cibercrime. Dalal e Gorab (2016) indicam que o comportamento criminoso digital decorre também de percepções de impunidade, enquanto De Andrade (2024) ressalta o papel da forense digital e Aragão (2015) discute a tensão entre eficiência e garantias processuais. Socialmente, o tema é urgente: os cibercrimes atingem empresas e cidadãos em todo o país, agravando a vulnerabilidade digital, sobretudo na Amazônia, onde limitações estruturais e tecnológicas se somam à incidência de delitos associados, como crimes ambientais e exploração sexual infantil (Leão et al., 2021). Assim, este estudo propõe uma análise empírica inédita,

articulando teoria e prática para aferir se a atuação da PF é predominantemente reativa ou proativa, contribuindo para o debate sobre a maturidade estratégica do Brasil no enfrentamento ao crime cibernético (Ulrich, 1998; Castells, 2003; Ratcliffe, 2016).

REFERENCIAL TEÓRICO

Eficiência Operacional em Segurança Pública

O conceito de eficiência operacional em segurança pública é amplamente debatido nas políticas criminais contemporâneas e refere-se à capacidade institucional de converter recursos limitados em resultados efetivos. Essa eficiência não se mede apenas pelo número de prisões ou operações, mas pela capacidade de reduzir riscos, prevenir crimes e proteger direitos fundamentais. Ratcliffe (2016) define a eficiência como a habilidade institucional de antecipar ameaças e neutralizá-las, distinguindo ações reativas, como prisões em flagrante, de ações proativas baseadas em inteligência e monitoramento digital. De forma complementar, Weber (2004) defende que a burocracia deve operar com racionalidade formal, alinhando meios e fins de modo mensurável. Bayley (2005) amplia essa visão ao afirmar que uma polícia eficiente é a que inspira confiança social e reduz riscos, não apenas a que gera estatísticas repressivas.

Beck (1998), em sua teoria da sociedade de risco, observa que a modernidade produz ameaças difusas e globais, como os crimes cibernéticos, cuja natureza transnacional desafia métricas tradicionais. Castells (2003) complementa que tais delitos decorrem da própria lógica da sociedade em rede, em que fluxos informacionais são apropriados por atores ilícitos com rapidez e alto potencial de dano. No Brasil, Cruz e Rodrigues (2018) destacam que, apesar da intensificação das operações da Polícia Federal (PF) contra o cibercrime, faltam parâmetros objetivos de eficiência. Essa lacuna é agravada pelo predomínio de abordagens normativas, que negligenciam a análise empírica da eficácia investigativa.

A relação entre mandados de busca e apreensão (MBAs) e prisões (flagrantes, temporárias e preventivas) surge como inovação metodológica capaz de mensurar a maturidade estratégica da PF. Colli (2009) demonstra que a ausência de parâmetros claros compromete a persecução penal e a legitimidade institucional. Cerqueira e Rocha (2013) reforçam esse ponto ao abordar o desafio de equilibrar eficiência e garantias fundamentais em investigações de fraudes eletrônicas. De Andrade (2024) acrescenta que a forense digital é essencial para garantir provas válidas e

responsabilização efetiva, evitando ações meramente midiáticas.

No contexto amazônico, Leão et al. (2021) e Cerqueira e Rocha (2013) apontam que a carência de infraestrutura e de delegacias especializadas compromete a efetividade estatal, reforçando a importância de estratégias de inteligência. Para Wall (2024) e Holt e Seigfried-Spellar (2022), a eficiência contra o cibercrime depende da cooperação internacional e do uso de tecnologias avançadas. A Europol (2024) sustenta que a medição da eficiência deve incluir não apenas outputs (prisões, operações), mas outcomes (redução de riscos e proteção de vítimas).

Assim, compreender a eficiência operacional como constructo multidimensional, racionalidade (Weber, 2004), gestão de riscos (Beck, 1998; Ratcliffe, 2016), capacidade tecnológica (De Andrade, 2024) e atenção às desigualdades regionais (Leão et al., 2021), permite situar o indicador MBAs/Prisões como instrumento inovador de análise da maturidade estratégica da segurança pública brasileira.

Ações Reativas e Proativas no Ciberespaço

O enfrentamento aos crimes cibernéticos representa um dos maiores desafios da segurança pública contemporânea. Diferentemente da criminalidade tradicional, os delitos digitais são desterritorializados, velozes e transnacionais. Diante disso, as agências de segurança precisam equilibrar duas posturas complementares: ações reativas e ações proativas.

As ações reativas concentram-se na responsabilização do infrator após a ocorrência do delito, manifestando-se em prisões (flagrantes, temporárias e preventivas), inquéritos e persecução penal. Embora essenciais para a efetividade do sistema de justiça, elas dependem da materialização prévia do crime e enfrentam barreiras técnicas, como o anonimato, a criptografia e o uso de redes de anonimização (TOR, VPNs). Cruz e Rodrigues (2018) observam que tais limitações alimentam a sensação de impunidade, mesmo diante de avanços legais no combate ao cibercrime. Em contrapartida, as ações proativas priorizam a antecipação e a prevenção, englobando atividades de inteligência, execução de mandados de busca e apreensão (MBAs), análise de grandes volumes de dados e uso da forense digital. De Andrade (2024) ressalta que esta é indispensável para assegurar a validade jurídica das provas e a responsabilização efetiva, garantindo rigor técnico nas etapas de coleta, preservação, análise e apresentação de evidências.

Dalal e Gorab (2016) ampliam o debate ao demonstrar que a motivação criminal também decorre de fatores organizacionais, como percepções de injustiça e ausência de políticas

preventivas. Assim, ações proativas devem incluir medidas de gestão interna, compliance e promoção da justiça organizacional, fortalecendo a integridade institucional.

Na literatura internacional, Wall (2024) distingue os cyber-dependent crimes (crimes que só existem no ambiente digital) dos cyber-enabled crimes (crimes tradicionais potencializados pela internet). Essa diferenciação tem implicações práticas: os primeiros exigem capacidade técnica elevada, enquanto os segundos demandam políticas integradas de repressão e inclusão digital. Holt e Seigfried-Spellar (2022) defendem que a eficácia institucional depende da integração entre capacidades técnicas, infraestrutura, perícia e centros de resposta, e sociais, como cooperação internacional e educação digital.

A Europol (2024) e a ICPO-Interpol (2022) reforçam que a eficiência no ciberespaço depende de ações multilaterais e do compartilhamento de informações em tempo real, priorizando outcomes (redução de riscos e desarticulação de redes) em vez de simples outputs (número de prisões). No Brasil, a PF vem ampliando o uso de MBAs e da perícia digital, sinalizando amadurecimento estratégico. Contudo, Colli (2009) e Cerqueira e Rocha (2013) destacam o desafio de compatibilizar eficiência com garantias constitucionais, dado o caráter intrusivo de certas medidas.

Assim, a maturidade institucional no combate ao cibercrime não se mede apenas por prisões, mas pela capacidade de antecipar, investigar e neutralizar ameaças, dimensão que torna a proporção entre MBAs e prisões um indicador empírico de eficiência estratégica.

Polícia Federal, Vigilância e o Papel Estratégico no Combate ao Cibercrime no Brasil

O combate ao crime cibernético no Brasil reflete um campo de tensão entre eficiência investigativa, limites constitucionais e dilemas éticos ligados à privacidade. A Polícia Federal (PF) ocupa posição central nesse cenário, sendo a principal responsável por investigar crimes de alta complexidade e interesse nacional. Entre as tipologias mais recorrentes destacam-se lavagem de dinheiro, exploração sexual infantil, fraudes bancárias e ataques a infraestruturas críticas — manifestações de uma criminalidade desterritorializada que se expande no ciberespaço (Santos et al., 2022). O país figura entre os mais afetados por delitos digitais, com prejuízos anuais superiores a 20 bilhões de dólares, o que levou à formulação da Estratégia Nacional de Segurança da Informação (ENSI), atualizada pelo Decreto n. 12.572/2025, com base na Lei n. 13.709/2018. Contudo, a implementação enfrenta obstáculos de integração institucional e monitoramento,

revelando o descompasso entre a norma e a prática (Santos et al., 2022).

Colli (2009) aponta que a PF enfrenta dificuldades nas investigações preliminares devido às garantias constitucionais de inviolabilidade de dados (art. 5º, CF/1988). A necessidade de autorização judicial para acessar informações em ambiente digital dinâmico gera atrasos e perda de provas, o que expressa o dilema entre eficiência e garantismo descrito por Ferrajoli (2006). Nesse contexto, a busca por agilidade não pode se sobrepor ao devido processo legal.

Além disso, o combate ao cibercrime se insere em um ambiente marcado pela vigilância digital e pelos desafios éticos da proteção de dados. Moreira, Razzolini Filho e Adrião (2023) alertam que a Lei Geral de Proteção de Dados (Lei n. 13.709/2018) contém lacunas quanto à segurança pública, criando um vácuo regulatório que fragiliza a delimitação entre monitoramento legítimo e abuso estatal. Foucault (2024) já advertia que a vigilância tende a se tornar norma disciplinar permanente se não houver freios institucionais. Assim, é necessário equilibrar a proteção social e a preservação das liberdades individuais.

Cruz e Rodrigues (2018) observam que a sensação de impunidade decorre não da ausência de leis, mas das barreiras técnicas, criptografia, anonimato e lentidão da cooperação internacional. A ICPO-Interpol (2022) e a Europol (2024) reforçam que a eficácia depende da integração global e do compartilhamento de informações em tempo real.

Na Região Norte, especialmente no Amazonas, a falta de delegacias especializadas e de infraestrutura tecnológica agrava a vulnerabilidade (Leão et al., 2021). Essa assimetria confirma as análises de Beck (1998) sobre a sociedade de risco e de Castells (2003) sobre a rede global, nas quais o risco digital cresce mais rápido que a capacidade de resposta. Avaliar a proporção entre MBAs e prisões permite, portanto, medir se a PF avança para uma atuação proativa e integrada ou permanece restrita a respostas reativas e regionais.

Relevância Regional: Amazônia e o Norte do Brasil

O debate sobre a eficiência operacional da Polícia Federal (PF) no combate ao cibercrime requer um recorte territorial que considere as desigualdades regionais brasileiras. A Região Norte, especialmente o Amazonas, apresenta vulnerabilidades estruturais e sociais que condicionam tanto a ocorrência quanto a repressão desses delitos, conferindo especificidade ao estudo e urgência à formulação de políticas públicas diferenciadas.

Caracterizada pela vasta extensão territorial, baixa densidade populacional e dificuldades

logísticas, a região enfrenta limitações na capacidade de resposta policial. Delegacias especializadas concentram-se nas capitais, enquanto o interior carece de infraestrutura e profissionais capacitados (Brochado, 2025). Essa carência compromete a preservação de evidências digitais e agrava a subnotificação. No Amazonas, a expansão do acesso à internet móvel não foi acompanhada por políticas de educação digital ou investimentos em cibersegurança (Castells, 2003), o que torna populações vulneráveis alvos de fraudes e golpes eletrônicos. Leão et al. (2021) destacam que delitos como exploração sexual infantil, tráfico de pessoas e crimes ambientais frequentemente utilizam meios digitais para difusão e lavagem de recursos. A natureza transnacional dessas práticas exige cooperação internacional e atuação integrada. O Fórum Brasileiro de Segurança Pública (FBSP, 2024) aponta crescimento acelerado dos crimes de estelionato eletrônico em estados do Norte, evidenciando a combinação entre fragilidade institucional e exposição ao risco.

A atuação no Norte depende fortemente da PF, dada a escassez de recursos das polícias civis estaduais. Brochado (2025) defende que a Gestão do Conhecimento pode melhorar a eficiência ao padronizar metodologias e reduzir a perda de provas digitais. Contudo, sem cooperação entre PF, Ministérios Públicos e instituições locais, os esforços permanecem fragmentados. A adesão do Brasil à Convenção de Budapeste e o Decreto nº 11.491/2023 ampliaram a cooperação internacional, mas sua efetividade nas regiões periféricas ainda é limitada.

Como observa Castells (2003), as redes digitais reproduzem desigualdades sociais existentes. Na Amazônia, isso se traduz em vulnerabilidade ampliada, onde comunidades isoladas e com baixa escolaridade tornam-se mais suscetíveis a fraudes e exploração digital. Tal dinâmica confirma a tese de Beck (1998) sobre a sociedade de risco, em que ameaças contemporâneas concentram-se em espaços com menor resiliência institucional.

Assim, analisar a eficiência operacional da PF no Norte não é apenas exercício acadêmico, mas diagnóstico estratégico. A proporção entre mandados de busca e apreensão e prisões indica se a resposta estatal privilegia inteligência e prevenção ou se permanece reativa. Com base nisso, este estudo contribui para compreender as assimetrias regionais e propor caminhos para uma governança cibernética mais equitativa, eficiente e adaptada às realidades amazônicas.

METODOLOGIA

A pesquisa adota abordagem quantitativa, descritiva e exploratória, voltada à análise da eficiência operacional da Polícia Federal (PF) no enfrentamento ao crime cibernético no Brasil, com ênfase na Região Norte e, em especial, no Estado do Amazonas. A escolha dessa metodologia fundamenta-se na necessidade de mensurar, com base em evidências empíricas, o perfil das ações estatais diante de um fenômeno ainda pouco explorado sob perspectivas analíticas objetivas, considerando que os estudos nacionais sobre o tema são majoritariamente qualitativos e normativos (Cruz; Rodrigues, 2018; Colli, 2009).

A dimensão quantitativa permite operacionalizar a variável central do estudo — a proporção entre mandados de busca e apreensão (MBAs) e prisões (flagrantes, temporárias e preventivas) —, enquanto o caráter descritivo possibilita identificar padrões de comportamento ao longo do período de 2023 a 2025. A natureza exploratória se justifica pelo ineditismo do indicador proposto, inexistente em pesquisas anteriores. Os dados foram extraídos do Painel Power BI da PF, que reúne informações consolidadas sobre operações, prisões e medidas cautelares deferidas em todo o território nacional. As imagens dos painéis referentes aos anos de 2023, 2024 e 2025 foram processadas por meio de reconhecimento óptico de caracteres (OCR), sistematizadas em planilhas e analisadas estatisticamente. Essa estratégia assegura fidelidade aos dados, respeitando os limites de transparência e divulgação da PF.

Complementarmente, utilizaram-se fontes secundárias, como o Anuário Brasileiro de Segurança Pública (FBSP, 2024), relatórios da Europol (2024) e da ICPO-Interpol (2022), além do Decreto nº 12.572/2025, para contextualizar os resultados com parâmetros nacionais e internacionais. A unidade de análise compreende o conjunto das operações da PF relacionadas ao cibercrime entre janeiro de 2023 e julho de 2025, período escolhido pela disponibilidade e atualidade das informações. A ênfase na Região Norte e no Amazonas deve-se à relevância geopolítica e à carência de estudos que abordem a eficiência policial em territórios periféricos (Leão et al., 2021).

A análise foi estruturada em três etapas: sistematização dos dados em planilhas por ano e unidade federativa; cálculo da proporção entre MBAs e prisões, com médias nacionais e recortes regionais; e comparação temporal para identificar variações na estratégia da PF e distinguir tendências de ações proativas ou reativas.

Reconhecem-se limitações, como o uso de dados restritos à PF e a impossibilidade de

segmentar tipos específicos de cibercrimes (Wall, 2024). Os dados são públicos e não envolvem seres humanos, conforme a Lei nº 12.527/2011. A adoção do indicador MBAs/Prisões representa uma inovação metodológica ao medir objetivamente a maturidade estratégica da PF, alinhando o estudo à tendência internacional de avaliação de outcomes, redução de riscos e desarticulação de redes criminosas, conforme Europol (2024) e ICPO-Interpol (2022).

RESULTADOS E DISCUSSÃO

A análise dos dados quantitativos da PF referentes ao período de 2023 a 2025 permitiu organizar os achados empíricos em dois eixos principais: (i) o volume total de operações, MBAs e prisões e (ii) a proporção de MBAs por prisões, indicador inédito proposto nesta pesquisa como métrica de eficiência operacional.

O primeiro eixo fornece um panorama do esforço institucional em termos absolutos, revelando a quantidade de operações deflagradas, medidas cautelares expedidas e prisões efetivadas a cada ano. Essa dimensão permite compreender o nível de atividade operacional da PF no enfrentamento ao cibercrime e identificar tendências de expansão ou retração ao longo do tempo. O segundo eixo, representado pela proporção de MBAs por prisões, busca avaliar a qualidade estratégica da resposta policial. Conforme discutido no referencial teórico (Ratcliffe, 2016; De Andrade, 2024), ações proativas tendem a se refletir em maior número de MBAs, voltados à coleta de provas digitais e desarticulação de redes, enquanto ações reativas se expressam principalmente por prisões imediatas. Assim, um índice elevado de MBAs por prisão indica uma estratégia ancorada em inteligência, enquanto índices baixos sugerem predomínio de respostas episódicas e repressivas.

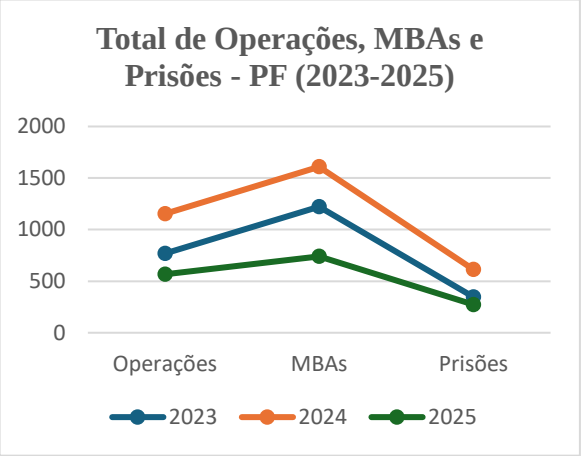
Para melhor visualização, os resultados foram organizados em:

Quadro 1. Distribuição Nacional por Ano (2023–2025)

Ano	Op.	MBAs	Prisões	MBAs/Prisões
2023	770	1222	347	3,52
2024	1152	1609	613	2,62
2025	568	740	273	2,71

Fonte: Adaptado dos dados estatísticos de Combate a Crimes Cibernéticos cadastrados no E-POL e SIGACRIM.

Gráfico 1. Evolução do total de operações, MBAs e prisões no período



Fonte: Adaptado dos dados estatísticos de Combate a Crimes Cibernéticos cadastrados no E-POL e SIGACRIM.

A partir desse arcabouço, é possível aprofundar a análise dos dados nacionais e, em seguida, discutir suas implicações para a eficiência operacional da PF e para a formulação de políticas públicas no campo da segurança cibernética.

Panorama Nacional (2023–2025)

A análise dos dados da PF evidencia uma evolução significativa no enfrentamento ao cibercrime. Entre 2023 e 2025 (até julho), observou-se o seguinte: 2023: 770 operações, 1.222 MBAs e 347 prisões; 2024: 1.152 operações, 1.609 MBAs e 613 prisões; e 2025 (jan–jul): 568 operações, 740 MBAs e 273 prisões.

A proporção MBAs/Prisões variou de 3,52 (2023) para 2,62 (2024) e 2,71 (2025). Isso indica que, em média, a cada prisão foram expedidos entre 2 e 3 MBAs, reforçando o caráter proativo da atuação da PF (Ratcliffe, 2016), já que a busca de provas antecede a responsabilização penal.

Justificativa da Abordagem Estatística

A utilização de estatísticas descritivas — médias, variâncias e desvios-padrão — fundamenta-se na necessidade de mensurar a dispersão e estabilidade da estratégia policial. Segundo Triola (2008), o desvio-padrão é a medida mais adequada de variabilidade, permitindo avaliar o quanto os valores se afastam da média.

Aplicando-se essa lógica aos dados da PF (2023–2025), temos:

Quadro 2. Estatísticas descritivas (2023–2025)

Indicador	Média	Variância	DP
Operações	830	87.964	296,6
MBAs	1.190	189.542	435,4
Prisões	411	31.972	178,8

Fonte: Adaptado dos dados estatísticos de Combate a Crimes Cibernéticos cadastrados no E-POL e SIGACRIM.

Esses resultados demonstram que MBAs e operações apresentam maior volatilidade, refletindo oscilações estratégicas e possivelmente limitações orçamentárias ou priorização de alvos (Santos et al., 2022). Já as prisões apresentam menor dispersão, indicando certa estabilidade na política repressiva.

Projeção para 2025

Uma vez que os dados de 2025 contemplam apenas os meses de janeiro a julho, utilizou-se a técnica de projeção linear simples, multiplicando-se os resultados parciais por um fator de 12/7. Esse método, embora limitado, é amplamente aceito para estimativas de curto prazo (Montgomery; Runger, 2010).

Quadro 3. Comparativo 2025 parcial (jan–jul) e projeção anualizada

Indicador	Jan–Jul 2025	Projeção 2025 (12 meses)
Operações	568	973
MBAs	740	1.268
Prisões	273	468

Fonte: Adaptado dos dados estatísticos de Combate a Crimes Cibernéticos cadastrados no E-POL e SIGACRIM.

Com base nessa projeção: Operações e MBAs devem ser inferiores a 2024, mas ainda maiores que 2023, sugerindo um ano intermediário; e o número de prisões projetadas (468) indica retração em relação a 2024 (613), mas expansão frente a 2023 (347).

Esse comportamento confirma o que Ulrich Beck (1998) chama de “oscilação típica de sociedades de risco”, nas quais a resposta estatal tende a se adaptar a contextos conjunturais.

Interpretação Estratégica

A partir dos cálculos, algumas inferências são possíveis: Perfil Proativo Consolidado: a predominância de MBAs em relação a prisões confirma a estratégia de inteligência e antecipação, condizente com boas práticas internacionais (Europol, 2024; ICPO-Interpol, 2022); Oscilações

Estratégicas: o alto desvio-padrão para MBAs (435,4) sugere instabilidade operacional. Isso pode estar associado à sazonalidade das operações ou a mudanças de prioridade institucional (Colli, 2009); Relação Operações/Prisões: em média, menos de uma prisão por operação (0,45 em 2023; 0,53 em 2024; 0,48 em 2025 projetado). Esse dado evidencia que o foco da PF está menos na prisão imediata e mais na coleta probatória, em linha com o papel de polícia judiciária (Ferrajoli, 2006; De Andrade, 2024).

Tendência para 2025: os cálculos sugerem que 2025 terá retração em relação ao pico de 2024, mas sem retroceder ao patamar de 2023. Isso sugere consolidação parcial da estratégia proativa, ainda que sujeita a limitações externas.

Relevância dos Resultados

Do ponto de vista acadêmico, o uso de estatística aplicada permite superar análises exclusivamente qualitativas do cibercrime, trazendo métricas objetivas para o debate (Triola, 2008). Já do ponto de vista da segurança pública, a análise indica que a PF: tem priorizado a coleta de provas digitais em detrimento da prisão imediata; encontra dificuldades em manter consistência estratégica (volatilidade dos dados); e apresenta tendência de consolidação gradual do modelo proativo.

Assim, este estudo contribui para a literatura ao propor um indicador (MBAs/Prisões) e demonstrar, com base em cálculos estatísticos, que a eficiência operacional da PF no ciberespaço está em transição para maior maturidade estratégica.

CONCLUSÃO

O presente estudo teve como objetivo central analisar a eficiência operacional da PF no enfrentamento ao crime cibernético, tomando como referência a proporção entre MBAs e prisões (flagrantes, preventivas e temporárias) realizadas entre 2023 e 2025. A questão norteadora indagava se tal proporção poderia indicar um perfil proativo ou reativo da atuação policial, especialmente na Região Norte e no Estado do Amazonas, dada sua relevância estratégica e suas vulnerabilidades específicas.

Os resultados empíricos demonstraram que, em todos os anos analisados, a proporção MBAs/Prisões se manteve superior a 2, variando de 3,52 em 2023 para 2,62 em 2024 e 2,71 em

2025 (projeção anualizada). Esses índices confirmam que, para cada prisão efetivada, a PF expediu entre dois e três MBAs, evidenciando uma estratégia predominantemente proativa. Isso significa que a prioridade da instituição tem sido a produção de provas digitais e a coleta de informações estratégicas, em consonância com modelos internacionais de intelligence-led policing.

Do ponto de vista estatístico, a análise revelou médias elevadas de operações (830), MBAs (1.190) e prisões (411) no período, porém acompanhadas de altos valores de variância e desvio-padrão, sobretudo em MBAs e operações. Tal volatilidade reforça a interpretação de que a estratégia ainda se encontra em fase de consolidação, oscilando entre momentos de maior expansão e fases de retração. A projeção para 2025 indicou um ano intermediário, com números inferiores aos de 2024, mas superiores aos de 2023, sugerindo uma tendência de estabilização gradual. No recorte regional, a análise destacou que a Região Norte, e particularmente o Amazonas, apresenta fortes vulnerabilidades estruturais e digitais, como a carência de delegacias especializadas, precariedade tecnológica e elevada incidência de crimes cibernéticos associados a delitos regionais, como exploração sexual infantil, tráfico de pessoas e crimes ambientais. Esses fatores reforçam a necessidade de políticas públicas diferenciadas e de maior investimento em capacitação técnica, forense digital e cooperação interinstitucional, para que a estratégia proativa observada no plano nacional também se consolide no plano regional.

Em relação aos objetivos da pesquisa, pode-se afirmar que foram plenamente atingidos. O objetivo geral de analisar o perfil da resposta policial foi cumprido, ao demonstrar a prevalência de uma atuação proativa da PF. O primeiro objetivo específico, de calcular a proporção MBAs/Prisões, foi realizado de forma detalhada com dados de 2023 a 2025. O segundo objetivo, de examinar a evolução temporal, foi atendido com a análise comparativa e a projeção estatística para 2025. O terceiro objetivo, de conferir ênfase à Região Norte e ao Amazonas, foi alcançado ao destacar as especificidades locais e sua relevância estratégica. O quarto objetivo, de discutir as implicações para a eficiência operacional e para a política de segurança pública, foi desenvolvido nas seções de discussão, evidenciando a importância da inteligência, da cooperação internacional e da adequação das políticas às realidades regionais.

Em síntese, este estudo contribui de forma inédita para a literatura ao propor e aplicar um indicador objetivo — a proporção MBAs/Prisões — para avaliar a eficiência operacional da PF no enfrentamento ao cibercrime. As evidências apontam para um perfil de maturidade estratégica em construção, onde a ênfase na coleta de provas digitais supera a prisão imediata, mas ainda

carece de maior estabilidade institucional e regionalização efetiva. Do ponto de vista das políticas públicas, os achados sugerem a necessidade de consolidação da estratégia proativa, especialmente no Amazonas, por meio de investimentos em infraestrutura tecnológica, formação especializada e mecanismos de cooperação multinível, garantindo que a atuação da PF se mantenha alinhada às melhores práticas internacionais, mas sensível às peculiaridades do contexto amazônico.

REFERÊNCIAS

ARAGÃO, D. F. D. **Crimes cibernéticos na pós-modernidade: direitos fundamentais e a efetividade da investigação criminal de fraudes bancárias eletrônicas no Brasil** (Dissertação de mestrado). – Curso de Direito - Universidade Federal do Maranhão, São Luís, Maranhão, Brasil, 2015.

BAYLEY, David H. **Changing the guard: Developing democratic police abroad.** Oxford University Press, 2005.

BRASIL. **Decreto nº 9.637, de 26 de dezembro de 2018.** Institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação. Diário Oficial da União, Brasília, DF, 2018.

BRASIL. **Decreto nº 12.572, de 4 de agosto de 2025.** Institui a Estratégia Nacional de Segurança da Informação e dispõe sobre a governança da segurança da informação no âmbito da administração pública federal. Diário Oficial da União, Brasília, DF, 2025.

BRASIL. **Lei nº 12.527, de 18 de novembro de 2011.** Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal. Diário Oficial da União, Brasília, DF, 2011.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União, Brasília, DF, 2018.

BROCHADO, I. P. D. S. **Investigação de crimes cibernéticos nas Polícias Civis do Brasil: contribuição da gestão do conhecimento** (Dissertação de mestrado). – Curso de Engenharia, Gestão e Mídia do Conhecimento - Universidade Federal de Santa Catarina, Florianópolis, Santa Catarina, Brasil, 2025.

CASTELLS, Manuel. **A Galáxia Internet: reflexões sobre a Internet, negócios e a sociedade.** Zahar, 2003.

CERQUEIRA, Silvio Castro; ROCHA, Claudionor. Crimes cibernéticos: desafios da investigação. **Cadernos Aslegis,** p. 131-161, 2013.

COLLI, M. **Cibercrimes: limites e perspectivas para a investigação preliminar policial brasileira de crimes cibernéticos** (Dissertação de mestrado). – Curso de Ciências Criminais - Pontifícia Universidade Católica do Rio Grande do Sul, Porto Alegre, RS, Brasil. 2009.

CRUZ, Diego; RODRIGUES, Juliana. Crimes cibernéticos e a falsa sensação de impunidade. **Revista Científica Eletrônica do Curso de Direito,** v. 13, n. 1, p. 1-18, 2018.

DALAL, Reeshad S.; GORAB, Aiva K. Insider threat in cyber security: What the organizational psychology literature on counterproductive work behavior can and cannot (yet) tell us. In: **Psychosocial dynamics of cyber security.** Routledge, p. 92-110, 2016

EUROPOL. AGÊNCIA DA UNIÃO EUROPEIA PARA A COOPERAÇÃO POLICIAL. **Internet Organised Crime Threat Assessment (IOCTA).** 2024. Recuperado de https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-threat-assessment-iocta-2024

LIMA DE ANDRADE, Ingrid. Forense digital aplicada ao combate de crimes cibernéticos: uma revisão. **Revista Foco (Interdisciplinary Studies Journal),** v. 17, n. 7, 2024.

FERRAJOLI, Luigi et al. **Direito e razão: teoria do garantismo penal.** São Paulo: editora revista dos tribunais, 2006.

FBSP. FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA. **Anuário Brasileiro de Segurança Pública 2024.** 2024. Recuperado de https://publicacoes.forumseguranca.org.br/items/f62c4196-561d-452d-a2a8-9d33d1163af0

FOUCAULT, Michel. **Vigiar e punir: nascimento da prisão.** Editora Vozes, 2024.

HOLT, Thomas; BOSSLER, Adam; SEIGFRIED-SPELLAR, Kathryn. **Cybercrime and digital forensics: An introduction.** Routledge, 2022.

LEÃO, Paulo Sérgio Remígio et al. Violência de gênero e vulnerabilidade no ambiente virtual: uma realidade cruel na era digital. **Derecho y Cambio Social,** v. 18, n. 64, 2021.

MONTGOMERY, Douglas C.; RUNGER, George C. **Applied statistics and probability for engineers.** John wiley & sons, 2010.

MOREIRA, Arnaldo Luis Darg; RAZZOLINI FILHO, Edelvino; ADRIÃO, Milton Cesar. Vigilância e privacidade no ambiente digital. **RDBCI: Revista Digital de Biblioteconomia e Ciência da Informação,** v. 21, p. e023012, 2023.

ICPO-INTERPOL. ORGANIZAÇÃO INTERNACIONAL DE POLÍCIA CRIMINAL. **Global Crime Trend Report 2022.** Recuperado de https://www.interpol.int/News-and-Events/News/2022/Financial-and-cybercrimes-top-global-police-concerns-says-new-INTERPOL-report

RATCLIFFE, Jerry H. **Intelligence-led policing.** Routledge, 2016.

SANTOS, Clarice Saraiva Andrade dos et al. Proposta de avaliação da Política Nacional de Segurança da Informação por Processo de Análise Hierárquica. **Perspectivas em Ciência da Informação,** v. 27, n. 4, p. 108-145, 2022.

TRIOLA, Mario F. Introdução à estatística. In: **Introdução à estatística. 2008.** p. xxvi, 310-xxvi, 310.

ULRICH, Beck. **La sociedad del riesgo. Hacia una nueva modernidad.** Barcelona, España, 1998.

WALL, David S. **Cybercrime: The transformation of crime in the information age.** John Wiley & Sons, 2024.

WEBER, Max. **Economia e sociedade: fundamentos da sociologia compreensiva.** Universidade de Brasília, 2004.