RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo-SP.
Ano VI, v.1 2026. | submissão: 09/02/2026 | aceito: 11/02/2026 | publicação: 13/02/2026

O desafio da pós-verdade: o impacto das milícias digitais e da desinformação na atividade de inteligência policial e as perspectivas para a curadoria crítica da informação

The post-truth challenge: the impact of digital militias and disinformation on police intelligence activities and perspectives for critical information curation

Jorge Magalhães do Carmo - Bacharel em Direito pela Faculdade Metropolitana de Manaus – FAMETRO; Especialista em Direito Constitucional e Direito Administrativo pelo Centro de Ensino Superior Dom Alberto - DOM ALBERTO; Cadete da Polícia Militar do Amazonas e Bacharelando em Segurança Pública e Cidadania na Universidade do Estado do Amazonas – UEA; Lattes: http://lattes.cnpq.br/6027924121344463 ID Lattes: 6027924121344463; https://orcid.org/0009-0009- 8317-2388 ; Contato: jorgemagalhaesdc@gmail.com

Kristorferson Almeida do Rêgo - Cadete da Polícia Militar do Amazonas. Bacharelando em Segurança Pública e do Cidadão pela Universidade do Estado do Amazonas – https://lattes.cnpq.br/4078604726881272 Contato: kr.asafe.noah.pedro@gmail.com

Yracles da Silva Rodrigues - Bacharelando em Segurança pública e do cidadão pela UEA, bacharel em direito pela UNIFACISA, Especialista em segurança pública pela faculdade focus. - Lattes https://lattes.cnpq.br/3163889181737429
- Contato: yracles@gmail.com

Flávio Carvalho Cavalcante - Doutorando no Programa de Pós-graduação em Ciências do Ambiente e Sustentabilidade na Amazônia PPGCASA da Universidade Federal do Amazonas. Mestre em Segurança Pública, Cidadania e Direitos Humanos do Programa de Pós-Graduação em Segurança Pública-PPGSP da Universidade do Estado do Amazonas - UEA. Especialista em Gestão Estratégica em Segurança Pública. Especialista em Inteligência de Segurança Pública pelo MJSP/ANP-PF. Especialista em Gestão Pública Aplicada à Segurança pela Universidade do Estado do Amazonas - UEA. Especialista em Segurança Pública e Inteligência Policial pela UNIC/LITERATUS. Especialista em Direito Militar pela UNINORTE. Especialista em Ciências Jurídicas pela Universidade Cidade de São Paulo - UNICID. Possui graduação em Segurança Pública pela Universidade do Estado do Amazonas - UEA. Bacharel em Direito pela Universidade Cidade de São Paulo - UNICID. É membro do Grupo de Pesquisa "Sujeitos, Ações e Percepções: Grupo de Pesquisa em Violência e Conflitualidades", da Universidade Federal do Acre.Atualmente é Oficial da Polícia Militar do Estado do Amazonas com atuação em Inteligência e Investigação Criminal (MPAM). Tem experiência na área de Gestão, Administração, Inteligência de Segurança Pública, Gestão do conhecimento e Análise Criminal, com ênfase em GESTÃO ESTRATÉGICA EM SEGURANÇA PÚBLIC

Resumo

Este artigo analisa os impactos operacionais e analíticos que as milícias digitais e a desinformação sistemática impõem aos órgãos de Inteligência Policial no Brasil, contextualizando essa ameaça contemporânea dentro do paradigma do policiamento orientado por inteligência. Partindo das origens e do modelo teórico dessa abordagem policial, o estudo problematiza como a desinformação organizada deixou de ser mera opinião para se tornar uma ferramenta de desestabilização institucional e obstrução da justiça, demandando uma adaptação dos processos de inteligência. Utilizando a metodologia de revisão bibliográfica e análise documental, com base em doutrinas oficiais, literatura internacional especializada e casos emblemáticos, o trabalho explora a convergência entre o modelo tradicional de interpretação do ambiente criminal e a necessidade de filtrar um ecossistema informacional hostil. Conclui-se que a Inteligência Policial moderna deve evoluir para uma prática de curadoria crítica da informação, integrando técnicas de *Open Source Intelligence* (OSINT), contrainteligência, comunicação estratégica e cooperação interinstitucional para proteger o processo decisório e o próprio Estado Democrático de Direito contra a guerra cognitiva digital.

Palavras-chave: Policiamento Orientado por Inteligência. Milícias Digitais. Desinformação.

Abstract
This article analyzes the operational and analytical impacts that digital militias and systematic disinformation impose on police intelligence agencies in Brazil, contextualizing this contemporary threat within the paradigm of intelligence-led policing. Starting from the origins and theoretical model of this police approach, the study problematizes how organized disinformation has ceased to be mere opinion and has become a tool for institutional destabilization and obstruction of justice, demanding an adaptation of intelligence processes. Using the methodology of bibliographic review and document analysis, based on official doctrines, specialized international literature, and emblematic cases, the work explores the convergence between the traditional model of interpreting the criminal environment and the need to filter a hostile informational ecosystem. It concludes that modern police intelligence must evolve into a practice of critical information curation, integrating Open Source Intelligence (OSINT) techniques, counterintelligence, strategic communication, and interinstitutional cooperation to protect the decision-making process and the democratic rule of law itself against digital cognitive warfare.
Keywords: Intelligence-Driven Policing. Digital Militias. Disinformation. Counterintelligence.

Introdução

Este artigo é oportuno, dado que o policiamento está atualmente passando por um período de mudança significativa tanto nas táticas operacionais quanto nas estruturas organizacionais. Novas ideias na redução da criminalidade e mudanças nas estratégias policiais de curto e longo prazo estão em andamento. O policiamento orientado por inteligência representa uma abordagem recente e é uma das mais prevalentes das atuais "mudanças na filosofia de controle do crime e na prática policial" (MAGUIRE, 2000). Surpreendentemente, dada a ampla distribuição do termo, ainda há uma considerável

confusão em relação ao seu significado real, tanto para os oficiais da linha de frente quanto para a gestão policial (RATCLIFFE, 2002b).

A paisagem das ameaças à segurança pública sofreu uma transição profunda, migrando de atuações predominantemente físicas para um domínio híbrido onde o cibernético e o informacional são palcos centrais. Neste novo ambiente, a guerra por narrativas e a manipulação da percepção social tornaram-se ferramentas tão impactantes quanto as armas convencionais. A atividade de Inteligência de Segurança Pública (ISP), cujo cerne é a produção de conhecimento estratégico para assessorar a prevenção e repressão de ilícitos (BRASIL, 2016), se vê confrontada com um adversário difuso e complexo: as milícias digitais e a máquina de desinformação sistemática.

A problemática central reside no fato de que a desinformação organizada transcende a esfera da mera opinião ou do debate político legítimo. Ela é instrumentalizada com *dolo* específico para desestabilizar instituições, obstruir a ação da justiça, proteger organizações

criminosas e minar a confiança pública nos órgãos de Estado. Esse fenômeno configura, nas palavras da Política Nacional de Inteligência de Segurança Pública (PNISP), uma clara "ação contrária à segurança pública no espaço cibernético" e "ação contrária ao Estado Democrático de Direito" (BRASIL, 2021a, p. 10), exigindo resposta proporcional do aparato estatal.

Este artigo tem como objetivo duplo: primeiro, revisitar e detalhar os princípios e o modelo do policiamento orientado por inteligência conforme estabelecido por Ratcliffe (2003) e difundido internacionalmente; segundo, analisar os impactos concretos que a nova modalidade de ameaça representada pelas milícias digitais impõe à atividade de Inteligência Policial.

Busca-se investigar como o *modus operandi* desses grupos contamina fontes, sobrecarrega os ciclos analíticos e ataca a credibilidade institucional, demandando uma reestruturação doutrinária e operacional das agências de inteligência dentro do paradigma do policiamento orientado por inteligência. A análise se fundamenta na revisão da literatura original, na Doutrina Nacional de Inteligência de Segurança Pública (DNISP), na PNISP, em literatura especializada e em casos emblemáticos, como os ataques de 8 de janeiro de 2023 no Brasil, que evidenciaram a materialização do risco informacional.

2. Policiamento orientado por inteligência à guerra cyber- cognitiva

Para compreender a dimensão do desafio atual, é essencial delimitar a evolução do conceito central. O Policiamento Orientado por Inteligência entrou no léxico policial por volta do início dos anos 1990, originário do Reino Unido, em resposta à crescente criminalidade e pressões por eficiência (GILL, 1998).

Seu objetivo era deslocar o foco do crime *per se* para o criminoso ativo, direcionando recursos de forma mais eficaz. O UK National Intelligence Model, por exemplo, concentrava-se em direcionar infratores, gerenciar pontos críticos, investigar séries vinculadas de crimes e aplicar medidas preventivas (NCIS, 2000). Trata-se da "aplicação da análise de inteligência criminal como uma ferramenta objetiva de tomada de decisão, a fim de facilitar a redução e prevenção do crime através de estratégias policiais eficazes e projetos de parceria externa extraídos de uma base probatória" (RATCLIFFE, 2003, adaptado).

Sobre a importância da pós verdade no contexto de conflitos leciona PINHEIRO, AGUIAR, LIMA (2019, p.775) que :

> é um elemento que vem se mostrando-se determinante, tanto na resolução de conflitos quanto em sua criação. Anualmente, a Oxford Dictionary, departamento da Universidade de Oxford compelido a editoração

> dos dicionários em inglês, elege um termo na língua inglesa como palavra do ano. Em 2016 o termo selecionado foi "pós-verdade", post-truth. Pós verdade é um temo utilizado para descrever um momento em que "as circunstâncias em que os fatos objetivos tem menos influência para moldar a opinião pública do que os apelos à crenças e emoções pessoais"

Além disso PINHEIRO, AGUIAR, LIMA (2019. p.776) menciona magistralmente que:

> E como é de se esperar de uma doença infeciosa (KUCHARSKI,2016), a pós-verdade tomou carona nas hemácias da modernidade líquida, onde o essencial é o movimento das informações não importando sua veracidade ou conveniência (BAUMAN,1999), e transmitiu-se pelas veias da globalização até chegar ao Brasil, tornando-se mister uma análise de seus efeitos, pois não se trata de um problema de países subdesenvolvidos mas sim de uma mazela global, que vem mostrando- se semelhantes aos do Reino Unido e Estados Unidos(SOUZA,2017 e TARDÁGUILA, 2018).

No entanto, o ambiente criminal que a polícia deve interpretar sofreu uma expansão radical. Não se trata mais apenas de um ambiente físico ou de redes criminosas tradicionais. O "ambiente criminal" no século XXI inclui ativamente um ecossistema informacional onde atores mal-intencionados, incluindo milícias digitais, operam para distorcer a realidade. O termo refere-se a grupos organizados que atuam de forma coordenada e, muitas vezes, profissionalizada no ambiente digital, utilizando estruturas que simulam aparência legítima para disseminar em massa conteúdos falsos (*fake news*), manipulados ou tendenciosos com objetivos políticos, ideológicos ou criminais (BRASIL, 2023 – CPMI dos Atos de 8 de Janeiro).

Nesse contexto, é crucial diferenciar desinformação de *misinformação*. Enquanto a segunda pode ser a disseminação involuntária de informações incorretas, a desinformação é caracterizada pela intencionalidade (*dolo*). Trata-se de uma "estratégia de manipulação informacional" onde notícias falsas são fabricadas e propagadas sistematicamente para "gerar confusão entre fato e opinião" e alcançar objetivos predeterminados, configurando verdadeiras operações psicológicas no espaço digital (SILVA FILHO, 2024). Esta intencionalidade malévola é que eleva o fenômeno à categoria de ameaça à segurança pública e objeto legítimo da atividade de inteligência, exigindo que o modelo de policiamento orientado por inteligência seja ampliado para incorporar a análise e o contra-ataque a essa nova camada de ameaça.

3. Modus operandi das milícias digitais e a contaminação do ciclo de inteligência

A eficácia das milícias digitais reside em uma arquitetura operacional sofisticada que ataca diretamente os pilares do policiamento orientado por inteligência. Essa arquitetura assenta-se em três pilares interligados que corroem o processo tradicional. Primeiro, a infraestrutura técnica, que utiliza *bots*, fazendas de cliques e algoritmos de segmentação para amplificar exponencialmente o alcance de narrativas falsas. Como demonstrado no Relatório da CPMI dos Atos de 8 de Janeiro, a velocidade e o alcance das falsidades superam em muito os das informações verdadeiras (BRASIL, 2023), criando um volume artificial que sobrecarrega os sistemas de coleta.

Sendo assim, Almeida (2025, p. 32) assevera isso quando afirma que :

> Presume-se que o policial deva armazenar dados coletados pela agência de inteligência local, além disso, é necessário que certos dados sejam submetidos a procedimentos de processamento e indexação, caso tais
>
> dados sejam armazenados e processados no computador de trabalho do policial, apesar das diretrizes de controle de informações implementadas na rede, o controle de dados protegidos torna-se mais abrangente quando realizado em um servidor específico e adequadamente configurado para essa finalidade. Essa abordagem não apenas otimiza o tempo de trabalho do agente, mas também reduz os custos associados à implantação de múltiplas máquinas para processamento em inúmeras unidades, em favor de uma única estrutura servidora interconectada. Esta permite aos agentes policiais o acesso cliente-servidor, conforme mencionado anteriormente. Além disso, facilita que, em qualquer momento ou em qualquer computador da rede da instituição policial, seja possível realizar o acesso para atualizar, modificar ou coletar informações já processadas. Assim, o computador utilizado regularmente pelo agente serviria meramente como uma ferramenta de acesso, e não mais como um dispositivo de processamento e armazenamento de dados cruciais para a segurança pública.

Segundo, a exploração das câmaras de eco. A fragmentação do espaço público em bolhas ideológicas homogêneas, facilitada pelos algoritmos das plataformas, permite que narrativas falsas circulem e se reforcem sem contraponto crítico. Para a inteligência policial, isso significa que os dados coletados de fontes abertas (OSINT) podem já estar severamente distorcidos, representando não a realidade social, mas uma realidade fabricada e amplificada digitalmente (SILVA FILHO, 2024).

Por fim, opera-se uma guerra cognitiva. As mensagens são cuidadosamente construídas para acionar gatilhos emocionais primários, medo, ódio, tribalismo, inibindo o pensamento crítico racional. Este ataque é duplamente perigoso: visa tanto a população, para

manipular sua percepção sobre a polícia e a justiça, quanto os próprios analistas e tomadores de decisão, potencialmente levando a vieses cognitivos na análise ou à paralisia decisória por medo de retaliação midiática.

O impacto desse ecossistema na atividade de inteligência é multifacetado. O primeiro pilar afetado é a confiabilidade das fontes e a contaminação do ciclo de produção. O analista, que depende da coleta e triagem de dados de diversas procedências, corre o risco constante de utilizar informações "plantadas" ou distorcidas por campanhas de desinformação.

Dados fabricados podem ser inseridos deliberadamente para desviar recursos investigativos, proteger criminosos ou incriminar inocentes, configurando um ato de contra-inteligência por parte dos adversários. A Doutrina da ABIN alerta que a proteção do conhecimento e a detecção de interferências são funções primordiais da contrainteligência (BRASIL, 2023).

O segundo pilar é a sobrecarga informativa ou *infoxicação*. O volume massivo e a velocidade de propagação de conteúdos falsos geram um ruído ensurdecedor. Os analistas, muitas vezes com equipes enxutas, podem ser soterrados pelo trabalho de verificar uma miríade de informações duvidosas, atrasando o processamento de dados genuinamente relevantes. Como aponta Espuny (2021), a "tempestade de dados" pode fazer com que as capacidades analíticas fiquem para trás das capacidades de coleta, comprometendo o princípio da tempestividade, a produção de conhecimento no momento oportuno para a decisão.

Por fim, as milícias digitais promovem um ataque direto à credibilidade institucional. Campanhas coordenadas visam especificamente desmoralizar órgãos de inteligência, ministérios públicos, polícias e seus agentes. A narrativa de "perseguição política" ou "incompetência" visa invalidar perante a opinião pública futuras operações, provas ou relatórios de inteligência. Este ataque mina a autoridade das instituições e pode intimidar servidores, fragilizando todo o sistema de segurança pública e justiça, corroendo a própria capacidade da polícia de "influenciar os tomadores de decisão" uma etapa crucial no modelo de Ratcliffe.

4. Contingências para a desinformação no processo de inteligência

O modelo clássico do policiamento orientado por inteligência, conforme representado na literatura (RATCLIFFE, 2002b), é um processo que começa com a interpretação do ambiente criminal, segue para a produção de inteligência que deve influenciar os tomadores

de decisão, para que estes possam finalmente impactar o ambiente criminal positivamente. No entanto, este modelo não considera explicitamente um ambiente de informação contaminado. As milícias digitais operam para corromper cada uma dessas estruturas, exigindo uma ampliação defensiva do modelo.

Na fase de interpretar o ambiente criminal, a capacidade analítica é seriamente comprometida quando uma parte significativa dos dados disponíveis, especialmente de fontes abertas (OSINT), é deliberadamente falsa. Portanto, uma subfunção crítica nesta etapa deve ser a validação e a triagem contrainformacional. Os sistemas e analistas precisam de ferramentas e treinamento para identificar *bots*, *deepfakes*, padrões de astroturfing e campanhas coordenadas. A cooperação com especialistas em segurança cibernética e *fact-checking* torna-se essencial. A infoxicação é uma tática do adversário; contra ela, a polícia precisa de curadoria de fontes e triagem tecnológica assistida.

Ao produzir inteligência, o analista não pode mais apenas sintetizar dados; deve qualificá-los com um selo de confiabilidade que considere a saúde do ecossistema informacional daquele tema. O produto de inteligência deve, quando pertinente, conter uma avaliação sobre a presença e o potencial impacto de campanhas de desinformação relacionadas ao alvo.

Na etapa de influenciar os tomadores de decisão, a inteligência policial baseada em evidências agora compete com narrativas virais, simples e emocionalmente carregadas que também chegam aos comandantes, gestores públicos e parceiros. A unidade de inteligência, portanto, deve desenvolver habilidades de comunicação estratégica.

Seu produto não pode ser apenas um relatório técnico; ele deve, quando necessário, ser acompanhado de materiais que desmintam narrativas falsas antecipadamente e preparem o decisor para enfrentar a desinformação que inevitavelmente surgirá. Parceiros externos, como autoridades municipais ou líderes comunitários, são especialmente vulneráveis e devem ser alertados e capacitados contra essas ameaças.

Finalmente, ao impactar o ambiente criminal, o planejamento operacional deve incluir um plano de comunicação integrado. Isso envolve transparência seletiva para ocupar o espaço informacional com fatos, monitoramento em tempo real das narrativas de resposta e capacidade de correção ágil de falsidades. Sem isso, o sucesso tático de uma operação pode ser anulado por um fracasso narrativo, corroendo a legitimidade policial, um ativo fundamental para a eficácia de longo prazo (SCOTT, 1998).

O princípio da proporcionalidade (RATCLIFFE, 2002b) é ainda mais desafiado quando táticas policiais são distorcidas digitalmente, exigindo que a polícia se prepare para

justificar publicamente suas ações de maneira clara e acessível.

5. O papel da inteligência policial no enfrentamento

Face a essa ameaça assimétrica, a Inteligência Policial não pode ser passiva. Ela deve integrar capacidades específicas de combate no campo informacional ao seu modelo de atuação. Uma ferramenta fundamental é o uso estratégico e forense da Inteligência de Fontes Abertas (OSINT). Mais do que coletar dados da internet, trata-se de aplicar metodologia analítica rigorosa para monitorar padrões de comportamento dessas redes, identificar influenciadores-chave, rastrear a origem de campanhas e desvendar suas conexões financeiras ou logísticas (CEPIK, 2023).

A tecnologia e a Inteligência Artificial (IA) surgem como aliadas indispensáveis, porém cautelosas. Ferramentas de análise de vínculos, mineração de dados e detecção de *bots* podem automatizar a identificação de padrões de disseminação e *clusters* de desinformação. No entanto, como alerta a literatura, a IA também traz riscos, como a perda do contexto humano e a geração de conteúdo falso ainda mais convincente (MARR, 2023). O elemento humano-analítico permanece insubstituível na interpretação final e na atribuição de intencionalidade.

A integração com a Contrainteligência torna-se imperativa. A função de "proteger a ação de interferência sobre a decisão" (BRASIL, 2023) é central. Isso envolve proteger os ativos (agentes, fontes, métodos), as infraestruturas críticas de comunicação das polícias e, principalmente, a imagem e credibilidade institucionais contra narrativas fraudulentas. Ações de contrapropaganda, baseadas em informações verdadeiras e transparentes, podem ser necessárias para desconstruir narrativas adversas e proteger o espaço decisório, atuando como uma barreira no modelo ampliado.

6. Desafios éticos, jurídicos e de cultura organizacional

Esta atuação mais incisiva no ambiente digital coloca dilemas complexos. O principal é equilibrar a vigilância necessária para identificar ameaças com a garantia das liberdades de expressão e privacidade. O monitoramento de redes públicas para identificar padrões criminosos coordenados é distinto da vigilância indiscriminada de cidadãos. A atuação deve ser sempre lastreada em lei, com controle externo robusto, para não repetir os abusos do passado.

Há uma urgência por uma legislação mais robusta e específica. Embora leis como a de Crimes contra o Estado Democrático de Direito (Lei nº 14.197/2021) e a de Organizações

Criminosas (Lei nº 12.850/2013) possam ser aplicadas, a tipificação clara da desinformação sistemática e financiada como crime seja contra a administração pública, seja como instrumento de organização criminosa, daria maior segurança jurídica às investigações.

Internamente, os serviços policiais enfrentam o desafio da cultura de desempenho. A pressão por métricas quantitativas pode desviar o foco da análise qualitativa profunda necessária para entender redes de influência (SCOTT, 1998). A avaliação de resultados deve priorizar a prevenção de crimes facilitada pela desinformação e a neutralização de campanhas de interferência, e não apenas volumes de processamento.

Conclusão

O impulso para o policiamento orientado por inteligência deve ser temperado por expectativas realistas e adaptado às novas ameaças. A capacidade da polícia de impactar o nível de crime na sociedade é limitada, mas ganhos são possíveis através da colaboração com agências externas que detêm a chave para fatores causais mais profundos (HEATON, 2000; WEATHERBURN, 2001). Esta conclusão permanece válida, mas requer uma expansão crucial. As "agências externas" com as quais a polícia deve colaborar agora incluem plataformas de mídia social, empresas de tecnologia e organizações de verificação de fatos. O compartilhamento de inteligência deve incluir a troca de dados sobre campanhas de desinformação maliciosas.

A era da pós-verdade e das milícias digitais impõe uma redefinição paradigmática à Inteligência Policial. Não basta mais ser um mero coletor e processador de dados; é preciso tornar-se um curador crítico da verdade em um mar de manipulação. A ISP deve evoluir para uma atividade que não apenas prevê crimes físicos, mas também identifica, neutraliza e se protege de ataques informacionais destinados a paralisá-la e deslegitimá- la.

O enfrentamento eficaz exigirá cooperação multissetorial e internacional, dada a natureza transnacional das plataformas e das redes de desinformação. O investimento em capacitação contínua dos analistas, dotando-os de conhecimentos em psicologia, comunicação, direito digital e análise de mídias sociais, é um imperativo estratégico. O modelo de policiamento orientado por inteligência, conforme concebido no final do século XX, fornece uma estrutura sólida; cabe à próxima geração de profissionais fortificá-la para os desafios do século XXI, onde as ideias falsas são as novas armas e a clareza analítica, o principal escudo.

Referências

ALMEIDA, ANDRÉ MARCELO DE. *Uso da infraestrutura de redes de computadores, processamento de dados e a implementação de inteligência artificial em agências locais de segurança pública*. In: ZOGAHIB, ANDRÉ LUIZ NUNES (org.). *Segurança pública, cidadania e direitos humanos: pesquisas, relatos e reflexões*. Ponta Grossa: Aya, 2024. p. 349.

AUSTRALIAN CUSTOMS SERVICE. *Intelligence doctrine*. Canberra: ACS, 2000.

AUDIT COMMISSION. *Helping with enquiries: tackling crime effectively*. London: HMSO, 1993.

BRASIL. *Doutrina Nacional de Inteligência de Segurança Pública (DNISP)*. 4. ed. Brasília: Ministério da Justiça; ABIN, 2016.

BRASIL. *Decreto nº 10.777, de 24 de agosto de 2021*. Aprova a Política Nacional de Inteligência de Segurança Pública (PNISP). Diário Oficial da União: Brasília, 2021.

BRASIL. Congresso Nacional. *Relatório final da Comissão Parlamentar Mista de Inquérito (CPMI) dos Atos de 8 de Janeiro de 2023*. Brasília: Congresso Nacional, 2023.

BRASIL. Agência Brasileira de Inteligência. *Doutrina da Atividade de Inteligência*. Brasília: ABIN, 2023.

CEPIK, MARCO. *Espionagem e democracia: agilidade e transparência como dilemas na institucionalização de serviços de inteligência*. 2. ed. Belo Horizonte: Fórum, 2023.

CHILVERS, M.; WEATHERBURN, D. *Operation and Crime Review panels: their impact on break and enter*. Crime and Justice Statistics Bureau Brief. Sydney: NSW Bureau of Crime Statistics and Research, 2001.

DUNNINGHAM, C.; NORRIS, C. *The detective, the snout, and the Audit Commission: the real costs in using informants*. Howard Journal of Criminal Justice, v. 38, p. 67–86, 1999.

ECK, J. E.; SPELMAN, W. *Problem solving: problem-oriented policing in Newport News*. Washington, DC: Police Executive Research Forum, 1987.

ERICKSON, R. V.; HAGGERTY, K. D. *Policing the risk society*. Oxford: Clarendon Press, 1997.

ESPUNY, HERBERT GONÇALVES. *Inteligência de segurança pública: destaques de sua prática*. In: BELIATO, ARACELI M. et al. (org.). *Inteligência policial*. Série Mizuno. 2024. p. 156–168.

GILL, P. *Making sense of police intelligence? The use of a cybernetic model in analysing information and power in police intelligence processes*. Policing and Society, v. 8, p. 289–314, 1998.

GOLDSTEIN, HERMAN. *Problem-oriented policing*. New York: McGraw-Hill, 1990.

HEATON, R. *The prospects for intelligence-led policing: some historical and quantitative considerations*. Policing and Society, v. 9, p. 337–356, 2000.

HER MAJESTY'S INSPECTORATE OF CONSTABULARY. *Policing with intelligence*. London: HMIC, 1997.

HER MAJESTY'S INSPECTORATE OF CONSTABULARY. *Northamptonshire Police: intelligence-led policing and proactive investigation of crime*. London: HMIC, 2001.
HER MAJESTY'S INSPECTORATE OF CONSTABULARY. *Bedfordshire Police: crime intelligence*. London: HMIC, 2002.

INTERNATIONAL ASSOCIATION OF CHIEFS OF POLICE. *Criminal intelligence sharing: a national plan for intelligence-led policing at the local, state and federal levels*. Alexandria, Virginia: COPS; IACP, 2002.

LAYCOCK, G. *Research for police: who needs it?* Trends and Issues in Crime and Criminal Justice, n. 211. Canberra: Australian Institute of Criminology, 2001.

MAGUIRE, M. *Policing by risks and targets: some dimensions and implications of intelligence-led crime control*. Policing and Society, v. 9, p. 315–336, 2000.

MAGUIRE, M.; JOHN, T. *Intelligence, surveillance and informants: integrated approaches*. Police Research Group: Crime Detection and Prevention Series, n. 64, 1995.

MARR, BERNARD. *Os 15 maiores riscos da inteligência artificial*. Forbes Tech, 2023.

NATIONAL CRIMINAL INTELLIGENCE SERVICE. *The National Intelligence Model*. London: NCIS, 2000.

PAWSON, R.; TILLEY, N. *Realistic evaluation*. London: Sage, 1997.

PINHEIRO, J.; AGUIAR, D.; LIMA, A. *A influência da pós-verdade e da modernidade líquida na resolução consensual de conflitos*. In: VIVAS, ALESSANDRA BENTES T. et al. (org.). *Interdisciplinaridade das políticas públicas*. Rio de Janeiro: Pembroke Collins, 2019. v. 1. p. 774–790.

RATCLIFFE, J. H. *Intelligence-led policing*. Canberra: Australian Institute of Criminology, 2003.

RATCLIFFE, J. H. *Policing urban burglary*. Trends and Issues in Crime and Criminal Justice, n. 213. Canberra: Australian Institute of Criminology, 2001.

RATCLIFFE, J. H. *Burglary reduction and the myth of displacement*. Trends and Issues in Crime and Criminal Justice, n. 232. Canberra: Australian Institute of Criminology, 2002.

RATCLIFFE, J. H. *Intelligence-led policing and the problems of turning rhetoric into practice*. Policing and Society, v. 12, p. 53–66, 2002.

SCOTT, J. *Performance culture: the return of reactive policing*. Policing and Society, v. 8, p. 269–288, 1998.

SHERMAN, L. W. et al. *Preventing crime: what works, what doesn't, what's promising*. Washington, DC: National Institute of Justice, 1998.

SILVA FILHO, MANUEL CAMILO DA. *Desinformação sistemática e fake news pelas milícias digitais e suas implicações na atividade de inteligência*. In: BELIATO, ARACELI M. et al. (org.). *Inteligência policial*. Série Mizuno. 2024. p. 180–196.

WEATHERBURN, D. *What causes crime?* Crime and Justice Bulletin, n. 54. Sydney: NSW Bureau of Crime Statistics and Research, 2001.