

IX ENCONTRO VIRTUAL DO CONPEDI

CRIMINOLOGIAS E POLÍTICA CRIMINAL II

Todos os direitos reservados e protegidos. Nenhuma parte destes anais poderá ser reproduzida ou transmitida sejam quais forem os meios empregados sem prévia autorização dos editores.

Diretoria - CONPEDI

Presidente - Profa. Dra. Samyra Haydêe Dal Farra Napolini - FMU - São Paulo

Diretor Executivo - Prof. Dr. Orides Mezzaroba - UFSC - Santa Catarina

Vice-presidente Norte - Prof. Dr. Jean Carlos Dias - Cesupa - Pará

Vice-presidente Centro-Oeste - Prof. Dr. José Querino Tavares Neto - UFG - Goiás

Vice-presidente Sul - Prof. Dr. Leonel Severo Rocha - Unisinos - Rio Grande do Sul

Vice-presidente Sudeste - Profa. Dra. Rosângela Lunardelli Cavallazzi - UFRJ/PUCRio - Rio de Janeiro

Vice-presidente Nordeste - Prof. Dr. Raymundo Juliano Feitosa - UNICAP - Pernambuco

Representante Discente: Prof. Dr. Abner da Silva Jaques - UPM/UNIGRAN - Mato Grosso do Sul

Conselho Fiscal:

Prof. Dr. José Filomeno de Moraes Filho - UFMA - Maranhão

Prof. Dr. Caio Augusto Souza Lara - SKEMA/ESDHC/UFMG - Minas Gerais

Prof. Dr. Valter Moura do Carmo - UFERSA - Rio Grande do Norte

Prof. Dr. Fernando Passos - UNIARA - São Paulo

Prof. Dr. Edinilson Donisete Machado - UNIVEM/UENP - São Paulo

Secretarias

Relações Institucionais:

Prof. Dra. Claudia Maria Barbosa - PUCPR - Paraná

Prof. Dr. Heron José de Santana Gordilho - UFBA - Bahia

Profa. Dra. Daniela Marques de Moraes - UNB - Distrito Federal

Comunicação:

Prof. Dr. Robison Tramontina - UNOESC - Santa Catarina

Prof. Dr. Liton Lanes Pilau Sobrinho - UPF/Univali - Rio Grande do Sul

Prof. Dr. Lucas Gonçalves da Silva - UFS - Sergipe

Relações Internacionais para o Continente Americano:

Prof. Dr. Jerônimo Siqueira Tybusch - UFSM - Rio Grande do Sul

Prof. Dr. Paulo Roberto Barbosa Ramos - UFMA - Maranhão

Prof. Dr. Felipe Chiarello de Souza Pinto - UPM - São Paulo

Relações Internacionais para os demais Continentes:

Profa. Dra. Gina Vidal Marcilio Pompeu - UNIFOR - Ceará

Profa. Dra. Sandra Regina Martini - UNIRITTER / UFRGS - Rio Grande do Sul

Profa. Dra. Maria Claudia da Silva Antunes de Souza - UNIVALI - Santa Catarina

Educação Jurídica

Profa. Dra. Viviane Coêlho de Séllos Knoerr - Unicuritiba - PR

Prof. Dr. Rubens Beçak - USP - SP

Profa. Dra. Livia Gaigher Bosio Campello - UFMS - MS

Eventos:

Prof. Dr. Yuri Nathan da Costa Lannes - FDF - São Paulo

Profa. Dra. Norma Sueli Padilha - UFSC - Santa Catarina

Prof. Dr. Juraci Mourão Lopes Filho - UNICHRISTUS - Ceará

Comissão Especial

Prof. Dr. João Marcelo de Lima Assafim - UFRJ - RJ

Profa. Dra. Maria Creusa De Araújo Borges - UFPB - PB

Prof. Dr. Antônio Carlos Diniz Murta - Fumec - MG

Prof. Dr. Rogério Borba - UNIFACVEST - SC

C928

Criminologias e política criminal II [Recurso eletrônico on-line] organização CONPEDI

Coordenadores: Edith Maria Barbosa Ramos; Maiquel Ângelo Dezordi Wermuth ; Flavia Piccinin Paz – Florianópolis: CONPEDI, 2026.

Inclui bibliografia

ISBN: 978-65-5274-621-4

Modo de acesso: www.conpedi.org.br em publicações

Tema: Constituição, Processo e Justiça Social: o papel da jurisdição constitucional na efetivação de direitos

2. Criminologias. 3. Política criminal. IX Encontro Virtual do CONPEDI (2: 2026: Florianópolis, Brasil).

CDU: 34



Conselho Nacional de Pesquisa
e Pós-Graduação em Direito Florianópolis
Santa Catarina – Brasil
www.conpedi.org.br

IX ENCONTRO VIRTUAL DO CONPEDI

CRIMINOLOGIAS E POLÍTICA CRIMINAL II

Apresentação

O Grupo de Trabalho Criminologias e Política Criminal II, realizado no âmbito do IX Encontro Virtual do CONPEDI, em 22 de junho de 2026, reuniu pesquisadores de diferentes instituições brasileiras para debater temas centrais da criminologia contemporânea, das políticas criminais e dos direitos humanos. As apresentações evidenciaram a pluralidade de perspectivas teóricas e metodológicas que atualmente orientam a pesquisa jurídica nacional, proporcionando um espaço qualificado para o intercâmbio científico e para o aprofundamento de reflexões críticas acerca dos desafios enfrentados pelo sistema de justiça criminal.

A programação contemplou pesquisas dedicadas à análise das relações entre direito penal, seguridade social e políticas públicas, como o estudo "Entre a Repressão Penal e a Seguridade Social: a Vedação do Auxílio-Reclusão aos Dependentes de Integrantes de Organizações Criminosas pela Lei nº 15.358/2026", de Giovanna Duarte Fighera, Rodrigo Zimmermann Martins e Higor Lameira Gasparetto, bem como investigações sobre os impactos da política de drogas na seletividade penal, a exemplo de "Entre a Subjetividade da Lei e a Seletividade Penal: alguns efeitos sobre o encarceramento de mulheres negras no Brasil a partir da política de Guerra às Drogas", de Fernanda da Silva Lima, Rafaela Meyer Ielo de Oliveira e Fernanda Analu Marcolla, e de "Entre a Universalidade Formal e a Exclusão Material: Seletividade Penal, Política de Drogas e Camadas de Vulnerabilidade no Cárcere Brasileiro", de José Antonio Nunes Aguiar, Silvio Carlos Leite Mesquita e Jade Tereza Almeida Ferreira.

Também integraram o GT pesquisas voltadas à compreensão dos mecanismos estruturais de

A expansão das tecnologias de controle penal e seus impactos sobre os direitos fundamentais também esteve presente nas discussões, por meio dos trabalhos "Gestão Seletiva da Memória: Criminologia Crítica e Epistemologia da Prova frente à Portaria MJSP nº 1122/2026", de Laura Rosa Martins e Jaime Domingues Brito; "Cadeia de Custódia na Apreensão de Criptoativos: a Presunção de Inocência no Âmbito da Resolução 288/2024 do Conselho Nacional do Ministério Público", de Hernani Deon Klaus e Reginaldo Pereira; "Biovigilância Genética e Expansão do Poder Punitivo: análise da coleta compulsória de DNA no processo penal brasileiro", de Marcelo Yukio Misaka, Kauã de Oliveira Sanches e Luís Guilherme Augusti Sampaio; e "Hibridismo Criminal: a simbiose operacional entre o crime organizado e os crimes cibernéticos", de Lucas Allebrandt Peres, Eraldo Cruz Martins Filho e Renata Almeida da Costa.

O enfrentamento ao crime organizado e às novas configurações da criminalidade constituiu outro eixo de reflexão, reunindo contribuições como "Facções Criminosas no Brasil e Custo da Atividade Delitiva: Fundamentos para um Modelo Repressivo de Enfrentamento Estatal à Luz do Direito Penal do Inimigo e da Análise Econômica do Crime", de Pedro Henrique Fidelis Costa, e "A Rota Bioceânica e os Desafios da Segurança Fronteiriça: impactos sociais e humanos diante da criminalidade transnacional", de Cauê Coutinho Netto.

As discussões sobre execução penal, sistema prisional e alternativas à resposta estritamente retributiva foram representadas pelos trabalhos "Falar com os Homens é Proteger as Mulheres: Grupos Reflexivos para Autores de Violência Doméstica no Sistema Prisional", de Ana Maria Rodrigues da Cunha e Claudia Luiz Lourenço; "Sistema Progressivo de Pena: uma revisão sistemática sobre livramento condicional e progressão de regime a partir da Plataforma CAPES", de Deylane Azevedo Moraes Leite; "Direito Penal, Criminologia Crítica e Direitos Fundamentais: diagnóstico das violações em Pedrinhas sob o prisma da legitimidade do direito de punir", de Antonio Coêlho Soares Junior, Anália Márcia Gracinda Marques dos Santos e Maria Luiza Rolim Ribeiro; e "A 'Psicopatía' Infantojuvenil: desafios e

O conjunto dos trabalhos evidencia a atualidade e a relevância dos debates contemporâneos em torno da criminologia, das políticas criminais e dos direitos humanos. Apesar da diversidade temática, as pesquisas convergem para uma preocupação comum: compreender criticamente os limites, as racionalidades e os impactos do poder punitivo em sociedades marcadas por profundas desigualdades sociais. Destaca-se, nesse contexto, a forte presença da criminologia crítica como referencial teórico capaz de problematizar a seletividade penal, o encarceramento em massa, a criminalização de grupos vulnerabilizados e as novas formas de vigilância e controle social.

As apresentações também demonstraram a crescente interdisciplinaridade da pesquisa jurídica brasileira, incorporando contribuições provenientes da sociologia, da ciência política, da economia, dos estudos de gênero e raça, da criminologia, da ciência da informação e das tecnologias digitais. Tal pluralidade permitiu ampliar a compreensão dos desafios contemporâneos relacionados à expansão do sistema penal, às transformações da criminalidade organizada, à proteção dos direitos fundamentais e à construção de políticas públicas orientadas pelos valores do Estado Democrático de Direito.

Os coordenadores registram seu agradecimento a todos os autores, avaliadores e participantes pelas relevantes contribuições apresentadas durante o GT, cuja qualidade científica e diversidade temática enriqueceram os debates realizados no IX Encontro Virtual do CONPEDI. Os estudos reunidos nestes anais constituem importante contribuição para o fortalecimento da pesquisa em criminologia e política criminal, reafirmando o compromisso da comunidade acadêmica com a produção de conhecimento crítico, rigoroso e socialmente comprometido.

Edith Maria Barbosa Ramos

Maiquel Ângelo Dezordi Wermuth

HIBRIDISMO CRIMINAL: A SIMBIOSE OPERACIONAL ENTRE O CRIME ORGANIZADO E OS CRIMES CIBERNÉTICOS

CRIMINAL HYBRIDISM: THE OPERATIONAL SYMBIOSIS BETWEEN ORGANIZED CRIMES AND CYBER CRIMES

Lucas Allebrandt Peres ¹
Eraldo Cruz Martins Filho ²
Renata Almeida Da Costa ³

Resumo

O presente artigo analisa o fenômeno do hibridismo criminal no Brasil, caracterizado pela simbiose operacional entre organizações criminosas de matriz territorial e o ecossistema dos crimes cibernéticos. Historicamente alicerçadas no domínio prisional e periférico, facções hegemônicas evoluíram para atuar como autênticas corporações transdimensionais. A pesquisa, amparada em revisão bibliográfica, investiga como essas estruturas promovem uma metamorfose digital, substituindo estrategicamente o emprego dispendioso e arriscado da força bélica pelas fraudes eletrônicas de alta rentabilidade e mitigada exposição punitiva, a troca de armas bélicas pelo phishing. O estudo demonstra que essa transição é viabilizada pela industrialização do ilícito digital, principalmente por meio do modelo corporativo fraud-as-a-service. Esse modelo permite a terceirização do conhecimento técnico, capacitando membros do crime organizado a operar esquemas de engenharia social diretamente do interior do sistema carcerário. Consequentemente, constata-se uma vitimização sistemática e assimétrica, direcionada a populações vulneráveis, com destaque para idosos e mulheres, gerando danos patrimoniais e psicológicos. A pesquisa conclui que a consolidação dessas novas facções digitais, capazes de exercer governança extralegal manipulando infraestruturas do ciberespaço, expõe a insuficiência do modelo tradicional de policiamento ostensivo. O enfrentamento deste paradigma complexo exige a atuação transnacional e a modernização do Estado democrático de direito mediante uma sólida governança da inteligência financeira, o emprego de técnicas especiais de investigação, a exemplo da infiltração virtual e do confisco alargado, e a desarticulação da logística que sustenta a comercialização de dados ilícitos.

ecosystem. Historically rooted in the domination of prisons and peripheral areas, hegemonic factions have evolved to act as authentic transdimensional corporations. Supported by a literature review, the research investigates how these structures promote a digital metamorphosis, strategically replacing the costly and risky use of armed force with high-profitability electronic fraud and reduced punitive exposure, trading firearms for phishing. The study demonstrates that this transition is made possible by the industrialization of digital crime, primarily through the corporate fraud-as-a-service model. This model enables the outsourcing of technical expertise, empowering organized crime members to operate social engineering schemes directly from within the prison system. Consequently, there is a systematic and asymmetric victimization directed at vulnerable populations, particularly the elderly and women, resulting in financial and psychological damage. The research concludes that the consolidation of these new digital factions, capable of exercising extralegal governance by manipulating cyberspace infrastructures, exposes the inadequacy of the traditional model of overt policing. Tackling this complex paradigm requires transnational action and the modernization of the democratic rule of law through robust financial intelligence governance, the use of special investigative techniques, such as virtual infiltration and extended confiscation, and the dismantling of the logistics that sustain the trade of illicit data.

Keywords/Palabras-claves/Mots-clés: Criminal factions, Criminal hybridism, Criminology, Cybercrime, Organized crime

INTRODUÇÃO

A dinâmica da criminalidade organizada no Brasil atravessa um período de transição caracterizado pela migração de táticas puramente territoriais para operações complexas no ciberespaço. Historicamente, as facções criminosas brasileiras, como o Primeiro Comando da Capital (PCC)¹ e o Comando Vermelho², consolidaram o seu poder a partir do sistema prisional, expandindo o domínio para as periferias urbanas através do controle do narcotráfico e do uso ostensivo da violência. Entretanto, o encarceramento e a repressão física deixaram de ser obstáculos intransponíveis, tornando-se, ao invés disso, catalisadores para a busca de novas fronteiras de lucro e influência, agora situadas na intangibilidade das redes digitais (Lourenço, 2023, p. 167-168).

Nesse cenário, emerge o que podemos chamar de hibridismo criminal, que define a simbiose operacional entre as estruturas clássicas do crime organizado e as modalidades avançadas de crimes cibernéticos. Não se trata apenas da utilização de redes sociais para comunicação ou propaganda, mas de uma integração profunda onde a força de coerção física das facções se funde à técnica da fraude eletrônica. Esta simbiose permite que as organizações operem como entidades transdimensionais, exercendo uma governança extralegal³ que desafia as fronteiras entre o mundo físico e o virtual, configurando-se como verdadeiros Estados paralelos com elevada capacidade de adaptação tecnológica (Cardoso; Germano, 2026, p. 25-28).

A evolução dos delitos informáticos, que deixaram de ser incidentes isolados para se tornarem uma indústria global altamente rentável, forneceu a estrutura necessária para essa transformação. O cibercrime contemporâneo se caracteriza pela profissionalização e pela industrialização, operando sob lógicas de mercado que minimizam os riscos de confronto direto com as forças de segurança (Maia; Costa, 2023, p. 115-116). A migração das facções para este ambiente é motivada pela percepção de que o ciberespaço oferece uma rentabilidade superior com uma exposição punitiva reduzida, permitindo a acumulação de capital ilícito que é, posteriormente, reinvestido em estruturas bélicas e logísticas no mundo físico (Alves, 2023, p. 8-14).

¹ Fundado em 1993 no sistema prisional paulista como rede de proteção após o massacre do Carandiru, o PCC, diferente das facções fluminenses, atua como uma agência reguladora que monopoliza e pacifica a violência letal entre criminosos para garantir o fluxo eficiente e lucrativo de seus mercados ilícitos.

² Originado no final dos anos 1970 no presídio de Ilha Grande, o Comando Vermelho atua com foco no domínio territorial armado. A organização possui uma estrutura mais descentralizada de franquias, caracterizada pelo controle ostensivo e bélico de favelas e pelo confronto direto para a manutenção de seus territórios.

³ Assunção, por organizações criminosas, de funções regulatórias tipicamente estatais em territórios ou instâncias onde a presença do poder público é precária ou ausente.

Um dos pilares desta metamorfose é a substituição estratégica do fuzil pelo *phishing*⁴, termo que sintetiza a transição do *modus operandi* das facções brasileiras. Enquanto a violência de rua atrai a atenção imediata do Estado e consome vastos recursos operacionais, as fraudes virtuais e a engenharia social permitem uma exploração predadora e sistemática da sociedade com maior discrição. Esta mudança de paradigma é evidenciada pela emergência das novas facções digitais e pela adoção do modelo *fraud-as-a-service*⁵, que democratiza o acesso a ferramentas de ataque sofisticadas para membros do crime organizado que não possuem formação técnica especializada (Silva; Pedrosa, 2026, p. 21-25).

O impacto social desta simbiose operacional é profundo, manifestando-se de forma mais aguda na vitimização de grupos vulneráveis, como idosos e mulheres, que se tornam alvos preferenciais de esquemas de estelionato eletrônico. A eficácia destas ações criminosas reside na exploração das lacunas de letramento digital⁶ e na fragilidade das instituições em rastrear ativos digitais e punir os articuladores dessas redes (Alves, 2023, p. 13-15). A visibilidade que os membros de facções ostentam em plataformas digitais serve, simultaneamente, como ferramenta de recrutamento e como demonstração de uma soberania que o Estado parece incapaz de conter integralmente (Barberino, 2025, p. 181-182).

O presente artigo objetiva analisar as nuances deste hibridismo, explorando como a união entre o poder territorial e a proficiência digital reconfigura o crime organizado no Brasil. Metodologicamente, a pesquisa sustenta-se numa revisão bibliográfica e documental, analisando desde a origem prisional das facções até à estruturação técnica do cibercrime industrializado.

1 FACÇÕES CRIMINOSAS: DA ORIGEM PRISIONAL À GOVERNANÇA EXTRALEGAL

O estudo das facções criminosas no Brasil exige uma ruptura com visões reducionistas que as limitam a meras associações eventuais para o tráfico de entorpecentes. Pelo contrário, estas organizações configuram-se como atores políticos e sociais complexos que redefiniram a dinâmica da violência e da ordem pública no território nacional. A origem deste fenômeno

⁴ Técnica de engenharia social que utiliza mensagens fraudulentas, simulando instituições legítimas, para enganar a vítima. Seu objetivo é a extração ilícita de dados sensíveis e senhas.

⁵ Modelo de negócios ilícito em que infraestruturas e ferramentas prontas para ataques cibernéticos são comercializadas ou alugadas. Isso permite que criminosos sem conhecimento técnico executem fraudes complexas mediante assinaturas ou taxas.

⁶ Capacidade de utilizar, compreender e interagir de forma crítica e segura com ambientes virtuais. Sua ausência dificulta o reconhecimento de ameaças, aumentando significativamente a vulnerabilidade do usuário a golpes eletrônicos e engenharia social.

reside na incontornável relação entre o crime e a prisão, onde o cárcere atua não como um fim da atividade delitiva, mas como o centro de comando, de produção de identidades coletivas e de arregimentação de mão de obra (Lourenço, 2023, p. 186-187).

Essas estruturas evoluíram para o exercício de uma governança extralegal, preenchendo o vácuo deixado pela precariedade e ausência das instituições estatais em territórios periféricos e unidades prisionais. Ao operarem sob a lógica do que a doutrina descreve como Estados paralelos, as facções estabelecem normas de conduta, sistemas próprios de resolução de conflitos e a regulação de mercados informais, exercendo uma soberania de fato que se sobrepõe à ordem jurídica convencional (Cardoso; Germano, 2026, p. 25-27). Tal poder não se sustenta apenas na força bélica, mas em uma legitimidade local construída pela imposição de uma ordem interna e pela gestão da vida cotidiana das populações sob seu domínio.

Ademais, a sofisticação organizacional destas siglas reflete uma aguda visão de mercado e uma capacidade de adaptação modular às pressões da perseguição penal. A transição de grupos locais para corporações criminosas com alcance transnacional envolveu a padronização de condutas por meio de regimentos próprios e a gestão profissional de fluxos financeiros, logísticos e de pessoal (Uchôa, 2024, p. 150-154, 164-166). Esta complexidade organizacional é o que permite à facção transitar com fluidez entre os mercados legais e ilegais, utilizando a mobilidade estratégica de pessoas e bens para consolidar sua capilaridade em todo o território brasileiro, conectando economias regionais a redes globais de ilicitude (Rodrigues; Andrade; Farias, 2025, p. 2-10).

1.1 Evolução Histórica e Organização das Facções no Brasil

A compreensão contemporânea das facções criminosas no Brasil pressupõe a análise da indissociabilidade entre o ambiente prisional e a dinâmica das ruas. Conforme aponta a literatura Lourenço (2023, p. 167-169), o fenômeno das facções não é meramente um subproduto da criminalidade comum, mas uma construção social e política que emergiu no interior do sistema carcerário, transformando as prisões em centros de comando. Esse processo histórico consolidou a ideia de que o crime e a prisão são partes integrantes de uma mesma engrenagem operacional, onde o encarceramento, em vez de neutralizar o indivíduo, muitas vezes o integra a redes de proteção e disciplina coletiva.

A organização interna desses grupos transcende a simples associação para o tráfico, assemelhando-se a estruturas corporativas com códigos de conduta rigorosos. Documentos

capturados em investigações revelam a existência de estatutos ou regimentos internos que ditam desde a hierarquia até a partilha de lucros (Uchôa, 2024, p. 151-153). Essas normas estabelecem obrigações claras, como o cumprimento de ordens superiores e a proibição de outras siglas em determinados territórios, evidenciando uma busca constante por hegemonia e controle disciplinar sobre seus membros.

A evolução dessas organizações permitiu que elas passassem a operar como Estados paralelos, exercendo uma governança extralegal em territórios onde a presença estatal é precária. De acordo com Cardoso e Germano (2026, p. 25-28), essa governança manifesta-se na provisão de segurança, na resolução de conflitos locais e na regulação de mercados informais e ilegais. Esse cenário impõe ao Estado um desafio que vai além da repressão policial direta, exigindo uma compreensão de como essas facções substituem as instituições públicas na gestão da vida cotidiana das populações periféricas.

No plano econômico, as facções demonstraram uma notável visão de mercado e capacidade de adaptação às mudanças globais. O Primeiro Comando da Capital (PCC) e o Comando Vermelho são exemplares nessa transição de grupos locais para organizações com alcance transnacional e multivariado (Uchôa, 2025). A migração de investimentos do narcotráfico para outros setores ilícitos demonstra que o lucro é o vetor principal, orientando a estratégia dessas corporações criminosas para atividades que ofereçam maior rentabilidade com menor exposição ao confronto bélico tradicional.

Além disso, a expansão dessas facções para pequenas e médias cidades brasileiras demonstra uma simbiose entre as novas lógicas criminais e as estruturas de poder locais preexistentes. Rodrigues, Andrade e Farias (2025, p. 1-2) argumentam que a mobilidade de pessoas e bens, exemplificada pelo trânsito de sobreviventes do cárcere e mercadorias, conecta mercados legais e ilegais, fortalecendo o alcance das facções. Esse processo de clandestinidade móvel permite que a lógica política das facções se entrelace com os coronelatos regionais, redesenhando o mapa da violência no território nacional.

A sofisticação organizacional atingiu um nível em que a especialização funcional se tornou o padrão. A estrutura modular permite que as facções operem de forma descentralizada, facilitando a terceirização de serviços e a diluição de riscos (Silva; Pedrosa, 2026, p. 24-26). Essa metamorfose organizacional é o sinal necessário para a entrada definitiva dessas organizações no universo digital, onde a força física é gradualmente complementada, ou até substituída, pela expertise técnica e pela manipulação informacional.

1.2 Territorialidade e Atuações Midiáticas no Ciberespaço

A transposição do domínio territorial físico para o ciberespaço representa uma das mudanças mais significativas na estratégia das facções criminosas no século XXI. A ocupação do ambiente digital não ocorre de forma aleatória, mas como uma extensão da soberania exercida nas periferias e presídios. Conforme analisa Barberino (2025, p. 19, 181-182), as plataformas digitais tornaram-se novos palcos de visibilidades marginais, onde membros dessas organizações utilizam a rede para projetar poder, delimitar fronteiras simbólicas e reafirmar identidades coletivas perante rivais e o próprio Estado.

As performances midiáticas em plataformas de mídia e redes sociais funcionam como ferramentas de propaganda e governança. Nesses espaços, a ostentação de poderio bélico e a divulgação de rituais internos servem para converter o conflito territorial em um ativo comunicacional, gerando temor e admiração (Barberino, 2025, p. 182-183, 204-206). A performance do crime no ambiente virtual permite que a facção mantenha sua influência sobre a base de seguidores e recrutas, transcendendo as limitações geográficas do bairro ou da unidade prisional. A utilização de aplicativos de mensagens instantâneas revolucionou a logística e o comando operacional das facções. O ciberespaço permite a transmissão instantânea de ordens e o monitoramento em tempo real de atividades ilícitas, garantindo que a hierarquia se mantenha rígida mesmo à distância. Como observado em estudos sobre o sistema carcerário (Nascimento, 2025), o acesso à tecnologia dentro das prisões modifica a relação de forças entre policiais penais e detentos, permitindo que a guerra externa seja coordenada de dentro das celas via dispositivos móveis.

Nesse contexto, emerge o conceito da metamorfose digital, caracterizado pela substituição estratégica de táticas violentas de rua por métodos de exploração virtual. Uchôa (2025) destaca que o uso de técnicas de *phishing* e estelionato digital pelas facções reflete uma percepção de que o ciberespaço oferece lucros elevados com um risco de punição consideravelmente menor em comparação ao confronto físico. A territorialidade, portanto, deixa de ser meramente física e se torna uma rede de conexões e dados, onde o controle da informação é o novo fuzil.

A construção da identidade faccionada na era digital também impacta a seletividade penal e o policiamento. A exposição voluntária de membros em redes sociais cria um rastro digital que, embora sirva como ferramenta de poder para o grupo, também se torna objeto de monitoramento algorítmico e inteligência policial (Uchôa, 2024, p. 227, 320). Contudo, essa visibilidade é calculada e busca legitimar a governança da facção perante a comunidade como uma força organizada e inevitável frente à ineficiência das instituições oficiais.

O hibridismo entre o território físico e o digital consolidou uma nova forma de soberania criminosa. O domínio de plataformas e a proficiência em comunicação digital permitem que as facções operem em múltiplas dimensões simultaneamente, dificultando a aplicação de métodos tradicionais de investigação. A simbiose operacional entre o crime de rua e o crime de rede não é apenas uma evolução técnica, mas uma reconfiguração da própria natureza do crime organizado brasileiro, que agora habita, com igual desenvoltura, o beco e o *bit*⁷.

2 CRIMES CIBERNÉTICOS: A INDUSTRIALIZAÇÃO DO ILÍCITO DIGITAL

O estudo da cibercriminalidade na contemporaneidade impõe a superação de estigmas e visões estereotipadas que, historicamente, relegaram o delito informático a uma categoria marginal da pesquisa criminológica. Longe da figura do infrator solitário motivado por curiosidade tecnológica ou desafio intelectual, os crimes cibernéticos consolidaram-se como uma das mais rentáveis expressões da macrocriminalidade moderna. Essa transição reflete uma mudança ontológica no perfil do ilícito, os ataques no ciberespaço deixaram de ser incidentes isolados de vandalismo digital para se estruturarem como verdadeiros empreendimentos corporativos globais, cuja finalidade é a acumulação rápida e escalável de capital ilícito (Maia; Costa, 2023, p. 111-117).

A industrialização do ilícito digital encontra respaldo na massificação do acesso à internet e na digitalização quase irrestrita das relações econômicas e sociais. Ao explorar as vulnerabilidades inerentes a essa hiperconectividade, redes cibercriminosas desenvolveram métodos operacionais pautados pela eficiência técnica, pela impessoalidade e, sobretudo, pela transnacionalidade. Diferentemente da criminalidade de rua, onde as amarras territoriais facilitam o mapeamento e a repressão estatal, o cibercrime dilui a autoria em servidores pulverizados, exigindo respostas estatais que transcendam as fronteiras tradicionais e fomentem a cooperação internacional (Maia; Costa, 2023, p. 122-123).

No contexto brasileiro, essa evolução assume contornos críticos em virtude da rápida adesão da população aos serviços financeiros digitais, processo muitas vezes desacompanhado de letramento informacional adequado para a proteção de dados. Essa conjuntura fomentou a criação de um ecossistema predatório onde a exploração da engenharia social se tornou a principal engrenagem de monetização, vitimizando de forma sistemática populações vulneráveis (Alves, 2023, p. 14-16). Além disso, a sofisticação contínua desse mercado

⁷ Unidade básica de informação digital, empregada aqui como metonímia para o ciberespaço.

marginal culminou na fragmentação das atividades criminosas em nichos de especialização, viabilizando a comercialização de insumos fraudulentos para terceiros (Silva; Pedrosa, 2026, p. 22-25).

2.1 Evolução dos Delitos Informáticos e o Cenário Brasileiro

A compreensão contemporânea da cibercriminalidade exige a desconstrução da figura folclórica do infrator cibernético solitário. Como evidenciado por Maia e Costa (2023, p. 114-115), os crimes cibernéticos passaram por uma profunda evolução histórica ao longo das últimas décadas. Inicialmente caracterizados como incidentes isolados, motivados preponderantemente por curiosidade tecnológica ou desafio intelectual, esses delitos transmutaram-se de forma irreversível. Na atualidade, configuram-se como ameaças globais sistêmicas e empreendimentos criminosos estruturados, cuja finalidade é a maximização e a acumulação de capital ilícito.

Essa metamorfose ocorreu em compasso com a massificação do acesso à internet e o avanço contínuo das tecnologias de informação. À medida que a sociedade migrou suas relações econômicas e sociais para o ciberespaço, as oportunidades para a prática delitiva expandiram-se exponencialmente. O ecossistema criminal se adaptou a essa nova realidade, desenvolvendo modelos de negócios ilícitos que se assemelham, em complexidade e eficiência, a corporações legítimas (Maia; Costa, 2023, p. 116-117). A escala de atuação deixou de ser local para tornar-se invariavelmente transnacional, desafiando os limites clássicos da jurisdição territorial.

Essa evolução sistêmica da fraude e do estelionato digital reflete uma arquitetura criminal em constante sofisticação. Estudos recentes sobre a estrutura organizacional do cibercrime apontam para o surgimento de tipologias emergentes de delitos que exploram lacunas na segurança digital nacional (Maragno; Yamazato *apud* Silva; Pedrosa, 2026, p. 18). O Brasil, em virtude de sua expressiva população conectada e da rápida adoção de serviços bancários digitais, converteu-se em um terreno fértil para a proliferação de redes cibercriminosas autônomas e altamente especializadas.

Diante da mutação constante dessa realidade delitiva, o arcabouço normativo tem sido instado a se adaptar. Maia e Costa (2023, p. 122-123) ressaltam a necessidade de criação e desenvolvimento de legislações e tratados vocacionados a combater tais crimes. A transnacionalidade inerente ao cibercrime impõe que as respostas estatais não se restrinjam às

fronteiras domésticas, exigindo cooperação mútua e a harmonização de tipificações penais entre diferentes nações para evitar a formação de paraísos cibernéticos de impunidade.

O papel do poder público se mostra crucial não apenas na repressão, mas sobretudo na prevenção desses delitos. O enfrentamento eficaz demanda o aparelhamento de agências de aplicação da lei e a estruturação de departamentos de segurança cibernética dotados de altíssima capacidade técnica (Maia; Costa, 2023, p. 122-123). A investigação criminal informacional requer o domínio de técnicas forenses avançadas para a identificação da autoria, a quebra de anonimato em redes complexas e a responsabilização dos verdadeiros articuladores financeiros dessas operações. A consolidação do cibercrime como uma indústria rentável e organizada alterou o paradigma da segurança pública. Essa industrialização do ilícito digital preparou o terreno operacional para que atores criminais alheios ao ambiente tecnológico, como as facções de matriz prisional, enxergassem no ciberespaço um mercado altamente atrativo, catalisando o fenômeno do hibridismo criminal.

2.2 Modalidades de Fraudes Virtuais e Vitimização

A profissionalização do cibercrime materializa-se, de forma contundente, na diversificação e na sofisticação das modalidades de fraudes virtuais. Diferentemente dos crimes contra o patrimônio praticados no ambiente físico, que frequentemente envolvem grave ameaça ou violência, a fraude perpetrada por organizações criminosas no ciberespaço baseia-se na manipulação da confiança e na exploração de vulnerabilidades sistêmicas ou humanas (Alves, 2023, p. 11-12). O estelionato digital, o *phishing*, a clonagem de aplicativos de mensagens e a engenharia social figuram como os instrumentos preferenciais para a consecução desses delitos informáticos.

O *modus operandi* dessas organizações revela um planejamento meticuloso que antecede a execução da fraude. O emprego de engenharia social, por exemplo, consiste na utilização de artifícios psicológicos para induzir a vítima a fornecer dados sensíveis, credenciais bancárias ou realizar transferências financeiras de forma voluntária. Essa tática demonstra que o elo mais fraco da segurança cibernética contemporânea raramente é a infraestrutura tecnológica, mas sim o comportamento do usuário diante de abordagens criminosas bem elaboradas (Alves, 2023, p. 12, 19).

A escolha dos alvos pelas organizações criminosas obedece a uma lógica predadora que se aproveita de assimetrias informacionais. Segundo Alves (2023, p. 14-15), o aumento substancial na prática de fraudes virtuais recai, de forma assimétrica, sobre populações

vulneráveis. As estatísticas e análises criminológicas demonstram que idosos e mulheres constituem os principais grupos vitimizados por essas organizações, evidenciando uma seletividade criminal orientada pela presunção de menor letramento digital e maior suscetibilidade a narrativas fraudulentas, sobretudo as de cunho emocional ou de suposta urgência financeira.

A vitimização no ambiente virtual acarreta consequências que transcendem o mero prejuízo patrimonial. Alves (2023, 11-12, 15) adverte que a repercussão desses crimes se projeta gravemente no mundo físico, gerando abalos psicológicos profundos, perda de confiança nas instituições financeiras e um sentimento crônico de insegurança. A investigação da privacidade, inerente à extração não autorizada de dados pessoais, impõe às vítimas um dano moral de difícil reparação, intensificado pela frequente impunidade e pela dificuldade de rastreio dos ativos subtraídos.

Para viabilizar essas fraudes em larga escala, as organizações adotam estruturas de terceirização pautadas na lógica de serviços. Como analisado por Silva e Pedrosa (2026, p. 21-22), o cibercrime contemporâneo fragmentou-se em nichos de especialização, onde atores criminosos não precisam possuir conhecimento técnico integral para aplicar um golpe. Eles podem adquirir bancos de dados vazados, softwares maliciosos e serviços de lavagem de dinheiro em mercados clandestinos, configurando a espinha dorsal operacional que sustenta a escalada das fraudes virtuais.

Diante da magnitude e da gravidade dessas consequências, emerge uma necessidade de formulação de políticas públicas robustas. A mera criminalização *a posteriori* é insuficiente. É necessário o desenvolvimento de campanhas de educação digital focadas nos grupos vulneráveis e a promulgação de legislações que exijam maior responsabilidade solidária das plataformas tecnológicas e instituições financeiras (Alves, 2023, p. 15-16, 20). O combate a essa modalidade de crime exige, impreterivelmente, a neutralização da arquitetura que facilita a monetização do golpe.

3 A SIMBIOSE OPERACIONAL, O SURGIMENTO DO HIBRIDISMO CRIMINAL

A compreensão do cenário de segurança pública contemporâneo culmina na análise do que se passa a designar como hibridismo criminal. Este fenômeno não consiste em uma mera aglutinação acidental de práticas delitivas, mas na convergência estrutural e estratégica entre o crime organizado de matriz territorial, forjado no interior do sistema prisional e nas margens urbanas, e a criminalidade cibernética corporativa. Ao cruzar as trajetórias evolutivas

abordadas, percebe-se que corporações criminosas hegemônicas alcançaram um estágio de maturidade organizacional que lhes permitiu transcender as limitações geográficas imperativas, fundindo a ameaça da coerção física à sofisticação do ilícito digital.

O motor propulsor dessa simbiose operacional é pautado por uma lógica de mercado e análise de custo-benefício (Uchôa, 2025). As facções tradicionais, confrontadas com o encarecimento logístico do narcotráfico, a intensificação do policiamento ostensivo e as elevadas penas associadas aos crimes violentos contra o patrimônio, identificaram no ciberespaço uma fronteira de expansão altamente rentável. A decisão de redirecionar parte substancial de seu capital, atenção e força de trabalho para as fraudes virtuais obedece à equação de maximização de lucros aliada à drástica mitigação de riscos operacionais. O ambiente virtual oferece a oportunidade de subtrair volumes financeiros expressivos de forma assíncrona, silenciosa e remota, reduzindo a vulnerabilidade ao confronto letal com o aparato repressivo estatal.

Para viabilizar essa atuação transdimensional, as organizações criminosas promoveram uma reestruturação profunda em suas redes de colaboração, estabelecendo alianças pragmáticas com especialistas em informática, hackers, desenvolvedores de softwares maliciosos e articuladores financeiros do ciber mundo (Silva; Pedrosa, 2026, p. 15-16, 21-22). Essa intersecção resolve a assimetria técnica originária das facções. Enquanto o crime organizado fornece o capital de investimento, a complexa teia de contas para lavagem de ativos e uma rede de membros cativos, dentro e fora das prisões, para operar os golpes, o ecossistema cibercriminoso entrega a tecnologia empacotada. Configura-se, desse modo, uma economia do crime altamente especializada, modular e interdependente.

3.1 A Metamorfose Digital: Estratégias de Substituição do Fuzil pelo *Phishing*

O hibridismo criminal constitui o ponto de convergência entre a criminalidade violenta de matriz territorial e a criminalidade de colarinho branco⁸ do ambiente virtual. Esta simbiose não representa a mera utilização de ferramentas tecnológicas de forma episódica, mas uma reconfiguração profunda na estratégia de acumulação de capital ilícito. As facções criminosas, outrora limitadas ao controle de bairros periféricos e unidades prisionais, compreenderam que o ciberespaço oferece um ambiente de expansão onde as fronteiras físicas deixam de ser um obstáculo para a projeção de poder e a maximização dos lucros (Uchôa, 2025).

⁸ Conceito cunhado por Edwin Sutherland que se refere a crimes econômicos ou corporativos praticados por agentes de alto status social valendo-se de suas posições de poder.

Conforme postula Uchôa (2025), organizações hegemônicas brasileiras, a exemplo do Primeiro Comando da Capital (PCC) e do Comando Vermelho, demonstram uma notável capacidade de adaptação e uma aguçada visão de mercado. Perante o encarecimento da atividade criminal tradicional, decorrente do aumento do policiamento ostensivo, dos custos operacionais do narcotráfico e das elevadas penas associadas a crimes violentos, estas corporações iniciaram uma migração calculada dos seus investimentos financeiros e recursos humanos para o ambiente cibernético.

A substituição figurativa e literal do fuzil pelo *phishing* traduz a essência desta transição. Enquanto o fuzil simboliza a coerção física, o domínio territorial e o elevado risco de confronto letal com as forças de segurança do Estado, o *phishing* e o estelionato digital representam a coerção psicológica e a fraude invisível (Uchôa, 2025). A adoção destas táticas permite às facções subtrair volumes substanciais de capital com uma exposição ao risco de prisão significativamente menor, alterando a equação de custo-benefício que historicamente norteou o crime organizado.

Consequentemente, o ecossistema criminal sofre uma reestruturação nas suas redes de colaboração. A operação no ciberespaço exige um *know-how*⁹ técnico que, tradicionalmente, não fazia parte do repertório dos membros das facções de origem prisional. Para suprir esta lacuna, observa-se uma aproximação tática entre líderes de facções e especialistas em informática, hackers e desenvolvedores de malwares (Silva; Pedrosa, 2026, p. 15-16, 21-22). Esta união de competências consolida a simbiose. As facções fornecem o capital inicial, a rede de lavagem de dinheiro e a estrutura de poder punitivo extralegal, enquanto os cibercriminosos fornecem a tecnologia e os meios de execução.

Esta nova realidade dilui as barreiras tradicionais da Criminologia que separavam os crimes de rua dos crimes cibernéticos. A facção híbrida opera simultaneamente em múltiplas dimensões, utilizando o lucro obtido nas fraudes virtuais para financiar a compra de armamentos e narcóticos no mundo físico, criando um ciclo contínuo de retroalimentação financeira (Alves, 2023, p. 14-15). O capital digitalizado transita de forma célere, dificultando o rastreamento por parte dos órgãos de controle financeiro do Estado.

Em suma, a metamorfose digital não extingue a violência física, mas relega-a para um plano na gestão dos negócios ilícitos. A simbiose operacional confere às organizações criminosas uma resiliência sem precedentes, exigindo que o Estado repense a sua cartografia de combate ao crime. A repressão focada exclusivamente no patrulhamento territorial

⁹ Conjunto de conhecimentos práticos, técnicos e operacionais acumulados pela experiência, necessários para a execução eficiente de uma atividade específica ou processo tecnológico.

mostra-se anacrónica perante corporações criminais que estabeleceram bases lucrativas na intangibilidade das redes de dados.

3.2 *Fraud-as-a-Service* e a Estrutura das Facções Digitais

A materialização técnica e comercial do hibridismo criminal atinge grande eficiência através da adoção do modelo *Fraud-as-a-Service*. Transposto da lógica corporativa do setor de tecnologia, o *Fraud-as-a-Service* representa a industrialização definitiva do cibercrime. De acordo com Silva e Pedrosa (2026, p. 21-22), este modelo baseia-se na oferta e comercialização de serviços e ferramentas ilícitas em mercados clandestinos, permitindo a terceirização de etapas complexas do estelionato digital.

O *Fraud-as-a-Service* democratiza o acesso à criminalidade cibernética, atuando como o elo perfeito para as facções tradicionais que desejam ingressar no ambiente digital sem dominar o código de programação. Através deste sistema, membros do crime organizado podem alugar infraestruturas prontas para ataques, desde painéis para envio massivo de mensagens de texto fraudulentas, pacotes de dados vazados com informações sensíveis de cidadãos, até esquemas de lavagem de dinheiro através de contas intermédias, de terceiros, e criptoativos (Silva; Pedrosa, 2026, p. 21-22). A fraude deixa de ser uma ação isolada para se tornar uma linha de montagem interconectada.

A estruturação deste ecossistema deu origem as novas facções digitais. Diferentemente das organizações prisionais, cujo estatuto se baseia na violência e na lealdade territorial (Uchôa, 2024, p. 67-68, 151-153), as facções digitais operam estritamente sob uma lógica empresarial. Possuem hierarquias baseadas em competências técnicas, departamentos de desenvolvimento, esquemas de suporte técnico e até estratégias de marketing na *dark web* e fóruns restritos (Silva; Pedrosa, 2026, p. 20, 25-26).

A intersecção destas facções digitais com os grupos criminosos de matriz física resulta numa potencialização de danos à sociedade. Ao adquirirem pacotes de modelos de fraude digital, as facções territoriais direccionam a sua vasta base de membros, muitas vezes recrutados nas periferias ou no interior do sistema prisional, para atuar como os operadores finais das fraudes, multiplicando exponencialmente o número de ataques (Nascimento, 2025, p. 17-18). As celas das prisões, munidas de dispositivos móveis clandestinos, convertem-se em verdadeiros *call centers* do crime organizado.

A lógica industrializada do *Fraud-as-a-Service* exacerba a vitimização de grupos vulneráveis. Conforme sublinhado por Alves (2023, p. 14-15), a padronização da engenharia

social, aliada à capacidade de processamento de dados dos modelos de fraude digital, permite uma precisão predadora na escolha dos alvos, focando predominantemente em idosos e mulheres. O hibridismo criminal automatizou a identificação de perfis com menor letramento digital, transformando a extorsão e o estelionato num processo sistemático e de altíssima rentabilidade. A simbiose estruturada pelo *Fraud-as-a-Service* consolida as organizações criminosas brasileiras como entidades transdimensionais. A fusão entre o poder de coação física e a hiper-eficiência da fraude modular torna o hibridismo criminal uma grande ameaça à segurança pública contemporânea, operando numa zona cinzenta onde as táticas tradicionais de investigação enfrentam grande limite operacional.

CONCLUSÕES

A pesquisa desenvolvida ao longo deste artigo mostra que o fenômeno das facções criminosas no Brasil transcendeu o paradigma exclusivamente territorial e prisional, consolidando o que se convencionou denominar de hibridismo criminal. A análise da literatura aponta que a criminalidade organizada, outrora atrelada estritamente à coerção física e ao narcotráfico, reconfigura-se perante as inovações tecnológicas e as pressões estatais repressivas. O resultado dessa reconfiguração é uma simbiose letal e altamente lucrativa entre as organizações de matriz de rua e o ecossistema do cibercrime, caracterizando uma evolução sistêmica no perfil da criminalidade pátria (Lourenço, 2023, p. 167-168 e Maia; Costa, 2023, p. 115-116).

No cerne dessa transformação encontra-se a metamorfose digital, um processo estratégico delineado pela substituição gradual do confronto armado maciço pelas fraudes virtuais silenciosas. Como demonstrado, corporações criminais hegemônicas adotaram o ciberespaço não apenas como palco de afirmação identitária e propaganda de poder (Barberino, 2025, p. 23-24, 181-182), mas como o vetor prioritário de sua expansão econômica. A adoção do estelionato digital em detrimento do uso de armas de guerra reflete uma racionalidade de mercado apurada, visando a obtenção de vultosos lucros com um risco de neutralização policial expressivamente menor (Uchôa, 2025).

A viabilidade técnica dessa expansão corporativa assenta-se na industrialização do ilícito, consubstanciada no modelo de fraude digital. Esta estrutura de mercado clandestino e modular permitiu que as facções tradicionais, desprovidas de expertise informática originária, passassem a atuar no ambiente virtual através da locação de painéis, pacotes de dados e serviços de lavagem de ativos (Silva; Pedrosa, 2026, p. 21-22). Consequentemente, o interior

do sistema carcerário foi ressignificado, impulsionado pelo acesso clandestino a tecnologias móveis, converteu-se em um epicentro de operações de fraude em escala industrial (Nascimento, 2025, p. 17-18), operando de forma predatória sob o anonimato digital.

As repercussões desse arranjo para o tecido social são severas, com destaque para a vitimização assimétrica de populações em situação de vulnerabilidade. A engenharia social, potencializada pela capilaridade do modelo de fraude digital, mira predominantemente em idosos e mulheres, gerando não apenas expressivos prejuízos patrimoniais, mas também abalos psicológicos e perda de confiança nas instituições financeiras (Alves, 2023, p. 14-15). A sofisticação contínua desses ataques demonstra que o crime organizado contemporâneo explora a desinformação e as lacunas no letramento digital como armas primárias para a extorsão.

Diante da consolidação dessas organizações híbridas, que passam a operar como Estados paralelos exercendo governança extralegal (Cardoso; Germano, 2026, p. 25-27), o modelo tradicional de segurança pública mostra-se anacrônico. As estratégias calcadas prioritariamente na repressão ostensiva e no policiamento físico de fronteiras geográficas são insuficientes contra corporações transdimensionais. É preciso que as instituições superem a fragmentação de suas ações e adotem abordagens sistêmicas e transnacionais (Maia; Costa, 2023, p. 122-123), reconhecendo que a vanguarda do crime organizado já não reside apenas no controle de favelas, mas no fluxo invisível de criptoativos e dados.

Por fim, infere-se que o desmantelamento das novas facções digitais requer a adoção de uma governança baseada em inteligência financeira e digital (Cardoso; Germano, 2026, p. 13-14). O combate eficaz a esse hibridismo exige a atualização constante da persecução penal mediante a aplicação rigorosa de técnicas especiais de investigação, como a infiltração de agentes no meio virtual, a ação controlada e a aplicação do confisco alargado de bens (Uchôa, 2024, p. 275, 343). O hibridismo criminal figura como um desafio. Neutralizá-lo exige que o Estado atue com a mesma sofisticação técnica, integração e agilidade das corporações criminosas que visa combater.

REFERÊNCIAS

ALVES, José Gustavo. **Análise da prática do crime de fraude perpetrado por organizações criminosas e suas consequências no ambiente virtual**. 2023. Fundação Universidade Federal de Mato Grosso do Sul (UFMS), [S. l.], 2023.

BARBERINO, Lisieanne Araújo. **Visibilidades marginais:** performances midiáticas de membros de facções criminosas em plataformas digitais. 2025. 280 f. Tese (Doutorado em Comunicação e Culturas Contemporâneas). Faculdade de Comunicação, Universidade Federal da Bahia, Salvador, 2025.

CARDOSO, Kathiussa Costa Leite; GERMANO, Leonardo de Andrade. **Além da repressão:** governança da inteligência e o enfrentamento às facções criminosas como Estados paralelos. 2026. Trabalho de Conclusão de Curso (Especialização em Inteligência e Inovação no Enfrentamento ao Crime Organizado). Centro Tecnológico, Universidade Federal de Santa Catarina, Florianópolis, 2026.

LOURENÇO, Luiz Claudio. **Facções criminosas:** um balanço da produção acadêmica no Brasil (2000-2022). Revista de Ciências Sociais, Fortaleza, v. 53, n. 3, p. 167-197, nov. 2022/fev. 2023. DOI: 10.36517/rcs.53.3.d06.

MAIA, Karolline Barbosa; COSTA, Cezar Henrique Ferreira. **Crimes cibernéticos.** Revista Ibero-Americana de Humanidades, Ciências e Educação (REASE), v. 9, n. 10, p. 11580, 2023. DOI: 10.51891/rease.v9i10.11580.

NASCIMENTO, Francisco Elionardo de Melo. **Tecnologias e guerra:** a produção do corpo e de (des)afetos no trabalho prisional. Mana: Estudos de Antropologia Social, Rio de Janeiro, v. 31, n. 3, e2025030, 2025. DOI: 10.1590/1678-49442025v31n3e2025030.pt.

RODRIGUES, Fernando de Jesus; ANDRADE, Paulo; FARIAS, Nido. **Mobilidades clandestinas:** pessoas e motos, coronelatos e facções. Dilemas: Revista de Estudos de Conflito e Controle Social, Rio de Janeiro, v. 18, n. 1, e63776, 2025. DOI: 10.4322/dilemas.v18.n1.63776.

SILVA, Alexsandro da; PEDROSA, Deyvis Perpétuo de Sales. **Fraud-as-a-Service (FaaS):** a estrutura organizacional das novas facções digitais. 2026. Trabalho de Conclusão de Curso (Especialização em Inteligência e Inovação no Enfrentamento ao Crime Organizado). Centro Tecnológico, Universidade Federal de Santa Catarina, Florianópolis, 2026.

UCHÔA, Roberto. **A metamorfose digital:** como as facções brasileiras estão trocando o fuzil pelo phishing. Página de Polícia / Fórum Brasileiro de Segurança Pública. Publicado em 22 jun. 2025. Disponível em base de dados jornalística digital. Acesso em: 13 abr. 2026.

UCHÔA, Romildson Farias. **Técnicas especiais de investigação em relação aos crimes praticados por facções criminosas:** infiltração, ação controlada e o confisco alargado. 2024. Dissertação (Mestrado em Direito). Centro de Ciências Sociais Aplicadas, Universidade Federal do Rio Grande do Norte, Natal, 2024.