O ENQUADRAMENTO JURÍDICO DO MODELO DE RANSOMWARE-AS-A-SERVICE COMO ORGANIZAÇÃO CRIMINOSA DIGITAL NO BRASIL

THE LEGAL CLASSIFICATION OF THE RANSOMWARE-AS-A-SERVICE MODEL AS A DIGITAL CRIMINAL ORGANIZATION IN BRAZIL

Yuri Saldanha Vilanova[1]
Emerson Wendt[2]

SUMÁRIO: 1. Introdução; 2. *Ransomware* e a evolução do modelo *Ransomware-as-a-Service*; 2.1 Conceito e evolução histórica do *ransomware*; 2.2 Características operacionais do *ransomware*; 2.3 Consolidação do modelo *Ransomware-as-a-Service* (RaaS); 3. Organização criminosa digital no Brasil; 3.1 Conceito legal e requisitos da organização criminosa; 3.2 Lei nº 15.358/2026 e o combate às organizações criminosas; 3.3 Crime organizado cibernético; 4. Análise do modelo *Ransomware-as-a-Service* como organização criminosa digital; 4.1 Aspectos jurídicos do crime de *ransomware*; 4.2 Enquadramento jurídico do *Ransomware-as-a-Service* como organização criminosa; 4.3 Limites jurídicos do *Ransomware-as-a-Service* e perspectivas legislativas; 5. Considerações finais; Referências.

RESUMO: Esta pesquisa analisa o enquadramento jurídico do modelo *Ransomware-as-a-Service* (RaaS) como organização criminosa digital no Brasil, a partir da evolução do *ransomware* e da consolidação de estruturas criminosas organizadas voltadas à prática de ataques cibernéticos. O problema consiste em verificar se o modelo RaaS apresenta elementos suficientes para a caracterização como organização criminosa nos termos da Lei nº 12.850/2013. A hipótese é a de que, apesar da descentralização operacional típica dos ecossistemas digitais, essa modalidade

[1] Bacharel em Direito pela Universidade La Salle - Unilasalle (Canoas/RS).
[2] Professor no PPGD e na Graduação em Direito da Universidade La Salle (Canoas/RS). Professor e Coordenador do Programa de Pós-Graduação Lato Sensu da Fabin. Criador e Editor-Revisor da revista Direito TI (ISSN 2447-1097). Possui graduação em Ciências Jurídicas e Sociais - Direito - pela Universidade Federal de Santa Maria (1997). Pós-graduado em Direito pela URI-Frederico Westphalen. Mestre e Doutor em Direito pela Universidade LaSalle Canoas-RS. Delegado de Polícia. Ex-Secretário Municipal de Segurança Pública de Canoas-RS. Ex-Diretor do Departamento de Inteligência de Segurança Pública do RS, ex-Chefe de Polícia da Polícia Civil do Rio Grande do Sul e ex-Presidente do Conselho Nacional de Chefes de Polícia Civil. Na Polícia Civil também foi Diretor do Gabinete de Inteligência e Assuntos Estratégicos (GIE) e do Departamento Estadual de Investigações do Narcotráfico (DENARC). É Coordenador do Grupo de Pesquisa Teorias Sociais do Direito (PPGD La Salle). Lattes: http://lattes.cnpq.br/9475388941521093; ORCID: https://orcid.org/0000-0002-0195-5445.

apresenta estrutura organizacional, divisão funcional, coordenação e finalidade econômica compatíveis com os requisitos legais. Adota-se o método dedutivo, mediante pesquisa bibliográfica e documental, de natureza qualitativa, fundamentada na legislação, na doutrina e na produção científica sobre crimes cibernéticos e organização criminosa. Conclui-se, em caráter condicionado à demonstração dos elementos no caso concreto, que o modelo RaaS pode ser compatível com os requisitos previstos na Lei nº 12.850/2013. Todavia, a ausência de disciplina normativa específica para as organizações criminosas digitais evidencia a necessidade de aperfeiçoamento legislativo compatível com os princípios constitucionais que orientam o exercício do poder punitivo estatal e asseguram maior segurança jurídica no enfrentamento da criminalidade cibernética.

PALAVRAS-CHAVE: *Ransomware*; *Ransomware-as-a-Service*; Organização criminosa digital; Crimes cibernéticos; Direito Penal.

ABSTRACT: This article analyzes the legal characterization of the *Ransomware-as-a-Service* (RaaS) model as a digital criminal organization in Brazil, based on the evolution of *ransomware* and the consolidation of organized criminal structures dedicated to cyberattacks. The research problem is whether the RaaS model meets the requirements for characterization as a criminal organization under Brazilian Law No. 12,850/2013. The hypothesis is that, despite the operational decentralization typical of digital ecosystems, this model presents an organizational structure, division of functions, coordination among its members, and an economic purpose compatible with the legal requirements. The study adopts a deductive approach through qualitative bibliographic and documentary research, supported by legislation, legal doctrine, and academic studies on cybercrime and criminal organizations. The findings indicate, subject to proof of the legal elements in each case, that the RaaS model may be compatible with the requirements established by Law No. 12,850/2013. However, the absence of specific legal regulation addressing digital criminal organizations highlights the need for legislative improvement while preserving the constitutional guarantees that limit the State's punitive power.

KEYWORDS: *Ransomware*; *Ransomware-as-a-Service*; Digital criminal organization; Cybercrime; Criminal Law.

1. INTRODUÇÃO

A evolução tecnológica observada nas últimas décadas trouxe importantes avanços para a sociedade. Em contrapartida, esse mesmo cenário favoreceu o surgimento de novas modalidades criminosas praticadas em ambiente virtual, conhecidas como crimes cibernéticos. Nesse contexto, destaca-se o *ransomware*, espécie de *malware* desenvolvida para restringir ou impedir o acesso aos dados da vítima mediante bloqueio ou criptografia, condicionando sua recuperação ao pagamento de resgate.

A constante evolução do *ransomware* resultou no modelo *Ransomware-as-a-Service* (RaaS), no qual desenvolvedores disponibilizam infraestrutura tecnológica e suporte operacional a afiliados responsáveis pela execução dos ataques, mediante a divisão dos lucros obtidos com os resgates. Diante desse cenário, o estudo do RaaS não se limita aos aspectos técnicos do *ransomware*, mas exige a análise dos institutos jurídicos destinados ao enfrentamento do crime organizado.

Para tanto, tornou-se necessário examinar a evolução do conceito de organização criminosa no ordenamento jurídico brasileiro, especialmente a definição e os requisitos estabelecidos pela Lei nº 12.850/2013, bem como verificar a eventual aplicabilidade da Lei nº 15.358/2026 ao modelo RaaS. Além disso, examina-se a adaptação do crime organizado ao ambiente cibernético.

A presente pesquisa tem como tema o enquadramento jurídico do modelo *Ransomware-as-a-Service* (RaaS) como organização criminosa digital no Brasil. O problema de pesquisa consiste em verificar se o modelo RaaS apresenta elementos suficientes para a caracterização como organização criminosa na legislação vigente. Parte-se da hipótese de que, apesar da descentralização operacional típica dos ecossistemas digitais, o modelo *Ransomware-as-a-Service* apresenta estrutura organizacional, divisão funcional e finalidade econômica compatíveis com os requisitos legais de organização criminosa previstos na Lei nº 12.850/2013.

Para responder ao problema proposto, adotou-se o método dedutivo, mediante pesquisa bibliográfica e documental, de natureza qualitativa, fundamentada na análise da legislação, da doutrina e da produção científica relacionada aos crimes cibernéticos, ao *ransomware*, ao crime organizado e ao Direito Penal. O estudo concentrou-se na evolução do *ransomware* e do modelo RaaS, na análise da legislação sobre organização criminosa e na verificação da compatibilidade desse modelo com os requisitos previstos no ordenamento jurídico brasileiro.

2. RANSOMWARE E A EVOLUÇÃO DO MODELO RANSOMWARE-AS-A-SERVICE

Este capítulo apresenta o fenômeno do *ransomware* e sua evolução histórica, evidenciando as transformações e as formas de atuação ao longo do tempo. Na sequência, analisam-se as principais características operacionais dos ataques de *ransomware* e, posteriormente, aborda-se o desenvolvimento do *Cybercrime-as-a-Service* (CaaS) e sua influência na consolidação do modelo *Ransomware-as-a-Service* (RaaS).

2.1 Conceito e evolução histórica do *ransomware*

O conceito de *ransomware* resulta da combinação das palavras inglesas *ransom*, que significa quantia exigida como resgate de alguém ou de algo, e *ware*, sufixo utilizado na informática para indicar espécies de programas de computador. Portanto, o *ransomware* consiste em uma classe de códigos maliciosos conhecida como *malware*[3], voltada à restrição, ao bloqueio ou à criptografia de dados da vítima, mediante posterior exigência de pagamento para o restabelecimento do acesso.[4]

O *ransomware* tem origem em 1989, com o programa conhecido como AIDS PC CYBORG, desenvolvido pelo Dr. Joseph L. Popp e considerado um cavalo de Troia (*Trojan*)[5], distribuído por meio de disquetes para diversos países. O funcionamento do programa consistia na coleta de informações do usuário e na geração de relatórios contendo riscos e recomendações relacionados ao contágio da AIDS.[6]

Após a instalação, durante a nonagésima inicialização do sistema operacional, os arquivos e as pastas da vítima eram criptografados, tornando o sistema inutilizável. Em

---

[3] BOMFATI, Cláudio Adriano; KOLBE JÚNIOR, Armando. *Crimes cibernéticos*. Curitiba: InterSaberes, 2020, p. 122. O termo *malware* refere-se a programas desenvolvidos com finalidade maliciosa, abrangendo diferentes espécies, como vírus, *worms* e *spywares*.

[4] BARBOSA, Guilherme Gueiros de Freitas. *A tipicidade dos ataques de ransomware no Brasil: uma interseção entre criptovirologia e direito penal*. São Paulo: D'Plácido, 2022, p. 49.

[5] BOMFATI, Cláudio Adriano; KOLBE JÚNIOR, Armando. *Crimes cibernéticos*. Curitiba: InterSaberes, 2020, p. 122. Cavalo de troia (*Trojan*), que consiste em um *malware* que se apresenta como um programa aparentemente inofensivo, permitindo ao invasor obter acesso remoto ao computador da vítima e coletar informações sem o conhecimento do usuário.

[6] CARMO, Marcus Fábio Fontenelle do. Ransomware: uma perspectiva histórica. In: GUEIROS, Guilherme; WENDT, Emerson (org.). *Ransomware 360°: abordagens multidisciplinares da extorsão criptoviral*. São Paulo: Mizuno, 2024, p. 17.

seguida, era exibido um alerta que exigia a renovação da licença mediante pagamento à corporação PC Cyborg Corporation, como condição para a liberação dos dados.[7]

Até 2005, não houve registros de novos ataques relevantes envolvendo *ransomware*. Esse cenário ocorreu principalmente em razão das limitações tecnológicas da época, que dificultavam o desenvolvimento de ataques mais sofisticados e a própria monetização da atividade, especialmente diante da predominância das transações bancárias presenciais, que possibilitavam maior rastreamento dos pagamentos.[8]

Com os avanços tecnológicos, surgiram novos meios de extorsão digital, acompanhados de sistemas de criptografia cada vez mais complexos e difíceis de romper. Ademais, a partir de 2013, o crescimento das *exchanges* de criptomoedas facilitou o recebimento de pagamentos com maior grau de anonimato.

Nesse contexto, o ano de 2015 foi marcado por uma evolução estrutural do *ransomware*, que passou a operar em modelos baseados na prestação de serviços, dando origem ao *Ransomware-as-a-Service* (RaaS), cuja estrutura e dinâmica operacional serão analisadas em subcapítulo específico.[9]

Após 2019, sobretudo durante o período da pandemia, a elevada incidência de ataques cibernéticos impulsionou o desenvolvimento de novas ameaças relacionadas ao *ransomware* e o crescimento de comunidades voltadas à prática de cibercrimes. Esses fatores contribuíram para a adoção de múltiplos métodos de extorsão, considerados marco significativo na evolução dos ataques de *ransomware*.[10]

No próximo subcapítulo, serão analisadas as características operacionais do *ransomware*, com foco nas principais formas de infiltração nos sistemas das vítimas e nos mecanismos utilizados durante a execução dos ataques.

---

[7] CARMO, Marcus Fábio Fontenelle do. Ransomware: uma perspectiva histórica. In: GUEIROS, Guilherme; WENDT, Emerson (org.). *Ransomware 360°: abordagens multidisciplinares da extorsão criptoviral*. São Paulo: Mizuno, 2024, p. 18-22.

[8] CARMO, Marcus Fábio Fontenelle do. Ransomware: uma perspectiva histórica. In: GUEIROS, Guilherme; WENDT, Emerson (org.). *Ransomware 360°: abordagens multidisciplinares da extorsão criptoviral*. São Paulo: Mizuno, 2024, p. 23.

[9]CARMO, Marcus Fábio Fontenelle do. Ransomware: uma perspectiva histórica. In: GUEIROS, Guilherme; WENDT, Emerson (org.). *Ransomware 360°: abordagens multidisciplinares da extorsão criptoviral*. São Paulo: Mizuno, 2024, p. 26-27.

[10] CARMO, Marcus Fábio Fontenelle do. Ransomware: uma perspectiva histórica. In: GUEIROS, Guilherme; WENDT, Emerson (org.). *Ransomware 360°: abordagens multidisciplinares da extorsão criptoviral*. São Paulo: Mizuno, 2024, p. 34-39.

2.2 Características operacionais do *ransomware*

O *ransomware* consiste em um tipo de *malware* que infecta sistemas computacionais, frequentemente por meio de técnicas de engenharia social[11]. Uma vez executado, pode atuar de diversas formas. Barbosa[12], ao apresentar a classificação proposta por Liska e Gallo, destaca que "o *ransomware* pode ser dividido em duas categorias: *Locker Ransomware*, que restringe ou bloqueia o acesso do usuário ao sistema, e *Crypto Ransomware*, que impede o acesso do usuário aos arquivos mediante o uso de criptografia".

A invasão pode ocorrer por diversos meios, principalmente por e-mails falsos, links e downloads infectados, além da exploração de falhas de segurança. A operação do *ransomware* pode ocorrer de duas formas: imediata ou retardada. Na ação retardada, o *malware* permanece oculto, coletando dados antes da execução do ataque; na ação imediata, inicia rapidamente o bloqueio ou a criptografia dos arquivos da vítima.[13]

Os *ransomware*s utilizam mecanismos de criptografia para comprometer os dados da vítima, destacando-se os sistemas de chaves simétrica e assimétrica. Em regra, o *ransomware* gera chaves simétricas para criptografar os arquivos da vítima, as quais posteriormente são protegidas por criptografia assimétrica. Após a exclusão dos arquivos originais, as informações necessárias à descriptografia permanecem sob o controle dos operadores do ataque, que condicionam a recuperação dos dados ao pagamento do resgate.[14]

Um fator determinante para a expansão do *ransomware* foi a publicação do artigo *Bitcoin: A Peer-to-Peer Electronic Cash System*[15], que alterou significativamente a dinâmica financeira dos ataques. A utilização de criptomoedas passou a facilitar o recebimento dos

---

[11] BOMFATI, Cláudio Adriano; KOLBE JÚNIOR, Armando. *Crimes cibernéticos*. Curitiba: InterSaberes, 2020, p. 118-119. A Engenharia social consiste em um conjunto de técnicas empregadas para manipular indivíduos, explorando a confiança das vítimas com o objetivo de obter informações sigilosas ou induzi-las à realização de determinadas ações, como a execução de programas maliciosos.

[12] BARBOSA, Guilherme Gueiros de Freitas. *A tipicidade dos ataques de ransomware no Brasil: uma interseção entre criptovirologia e direito penal*. São Paulo: D'Plácido, 2022, p. 51.

[13] CARMO, Marcus Fábio Fontenelle do. Ransomware: uma perspectiva histórica. In: GUEIROS, Guilherme; WENDT, Emerson (org.). *Ransomware 360°: abordagens multidisciplinares da extorsão criptoviral*. São Paulo: Mizuno, 2024, p. 17-26.

[14] CARMO, Marcus Fábio Fontenelle do. Ransomware: uma perspectiva histórica. In: GUEIROS, Guilherme; WENDT, Emerson (org.). *Ransomware 360°: abordagens multidisciplinares da extorsão criptoviral*. São Paulo: Mizuno, 2024, p. 23-24.

[15] NAKAMOTO, Satoshi. *Bitcoin: A Peer-to-Peer Electronic Cash System*. 2008. Bitcoin: A Peer-to-Peer Electronic Cash System é o título do famoso artigo científico publicado em 31 de outubro de 2008 por uma pessoa ou grupo sob o pseudônimo de Satoshi Nakamoto. Este documento lançou as bases conceituais e técnicas para a criação do Bitcoin e da tecnologia blockchain. Disponível em: https://bitcoin.org/files/bitcoin-paper/bitcoin_pt_br.pdf. Acesso em: 3 jun. 2026.

pagamentos exigidos das vítimas, ampliando a lucratividade e a expansão digital desse modelo criminoso.[16]

Na busca por novos mecanismos de coerção para obter o pagamento do resgate, os criminosos passaram a adotar múltiplos métodos de extorsão mediante o uso do *ransomware*. Um dos primeiros foi a dupla extorsão, na qual os atacantes exfiltram arquivos antes de criptografar os dados, aumentando a eficácia do ataque mediante a ameaça de vazamento ou comercialização de informações confidenciais.[17]

Na modalidade conhecida como tripla extorsão, grupos de *ransomware* podem empregar ataques de negação de serviço distribuído, chamados de *DDoS* (*Distributed Denial-of-Service*), como forma adicional de pressionar a vítima ao pagamento do resgate. Nesses ataques, os agentes criminosos utilizam *botnets*[18] compostas por diversos dispositivos previamente infectados e controlados remotamente para sobrecarregar o sistema-alvo por meio de múltiplos acessos simultâneos, comprometendo a disponibilidade do serviço.[19]

Por fim, surgiu a denominada extorsão quádrupla. Nessa modalidade, os agentes passam a contatar diretamente clientes, parceiros comerciais e concorrentes da organização atacada. A estratégia busca ampliar os danos reputacionais e econômicos da vítima, levando-a a reconsiderar a possibilidade de pagar o resgate diante do risco de perda de confiança por parte de clientes e parceiros, bem como de prejuízos perante os concorrentes.[20]

No próximo subcapítulo, será abordado como as sucessivas evoluções e estratégias empregadas pelo *ransomware* culminaram no surgimento da modalidade *Ransomware-as-a-Service* (RaaS), nova metodologia criminosa baseada em estruturas organizacionais e na divisão de tarefas entre diferentes agentes.

---

[16] CARMO, Marcus Fábio Fontenelle do. Ransomware: uma perspectiva histórica. In: GUEIROS, Guilherme; WENDT, Emerson (org.). *Ransomware 360°: abordagens multidisciplinares da extorsão criptoviral*. São Paulo: Mizuno, 2024, p. 25-26.

[17] CARMO, Marcus Fábio Fontenelle do. Ransomware: uma perspectiva histórica. In: GUEIROS, Guilherme; WENDT, Emerson (org.). *Ransomware 360°: abordagens multidisciplinares da extorsão criptoviral*. São Paulo: Mizuno, 2024, p. 34.

[18] BOMFATI, Cláudio Adriano; KOLBE JÚNIOR, Armando. *Crimes cibernéticos*. Curitiba: InterSaberes, 2020, p. 121. *Botnets* consistem em redes de computadores infectados por programas maliciosos (bots), controlados remotamente por agentes criminosos para a execução coordenada de atividades ilícitas, geralmente sem o conhecimento dos proprietários dos dispositivos.

[19] TRELEAVEN, Philip et al. The future of cybercrime: AI and emerging technologies are creating a cybercrime tsunami. *SSRN Electronic Journal*, 2023. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4507244. Acesso em: 9 jun. 2026.

[20] CARMO, Marcus Fábio Fontenelle do. Ransomware: uma perspectiva histórica. In: GUEIROS, Guilherme; WENDT, Emerson (org.). *Ransomware 360°: abordagens multidisciplinares da extorsão criptoviral*. São Paulo: Mizuno, 2024, p. 35.

2.3 Consolidação do modelo *Ransomware-as-a-Service* (RaaS)

Inspirado em modelos legítimos de prestação de serviços digitais, especialmente o *Software-as-a-Service*[21] (SaaS), surgiu o *Cybercrime-as-a-Service* (CaaS), no qual cibercriminosos comercializam ferramentas e serviços ilícitos voltados à prática de crimes cibernéticos. Esse modelo ampliou o alcance do cibercrime ao permitir que indivíduos com pouca habilidade técnica realizassem ataques cibernéticos.[22]

Nesse contexto, surgiu o *Ransomware-as-a-Service* (RaaS), e o *ransomware* passou a operar sob uma lógica empresarial, oferecendo ferramentas prontas para uso, acompanhadas de manuais e de uma estrutura organizada pelos próprios operadores do serviço. Com isso, reduziram-se significativamente as barreiras técnicas para a prática desse tipo de delito. Tais plataformas costumam disponibilizar funcionalidades integradas, como processamento de pagamentos, acompanhamento estatístico das infecções e suporte operacional aos afiliados.[23]

O formato de "afiliação", no qual o indivíduo se vincula à plataforma de RaaS e passa a utilizar sua infraestrutura para a prática de crimes, pode ocorrer por meio de diferentes estratégias de monetização: assinatura mensal por taxa fixa; programa de afiliados com percentual dos lucros; taxa única sem participação nos lucros; e programa de participação nos lucros e resultados. Cumpre destacar, ainda, que essas comunidades passaram a estabelecer regras internas e mecanismos de punição aplicáveis aos próprios afiliados.[24]

A consolidação desse modelo de negócios incentivou os criminosos a desenvolver novos *ransomware*s para a realização de ataques. Mesmo que a vítima não efetue o pagamento, os responsáveis pelo *ransomware* ainda podem obter ganhos financeiros por meio da venda dos dados obtidos ilicitamente na internet, prática que também pode envolver organizações criminosas.[25]

---

[21] ZUCCA, Maria Vittoria. Mappare il Crime-as-a-Service: analisi delle strutture, dei ruoli e dei servizi nell'offerta criminale digitale. *Rivista italiana di informatica e diritto*, v. 7, n. 2, p. 159-169, 2025. Software como Serviço (SaaS) é um modelo legítimo de negócios no qual os usuários realizam assinatura para acesso e utilização de aplicações em nuvem.

[22] ZUCCA, Maria Vittoria. Mappare il Crime-as-a-Service: analisi delle strutture, dei ruoli e dei servizi nell'offerta criminale digitale. *Rivista italiana di informatica e diritto*, v. 7, n. 2, p. 159-169, 2025.

[23] NAGAR, Gourav. The evolution of *ransomware*: tactics, techniques, and mitigation strategies. *SSRN Electronic Journal*, 2024. Disponível em: https://ssrn.com/abstract=4881213. Acesso em: 3 jun. 2026.

[24] CARMO, Marcus Fábio Fontenelle do. *Ransomware*: uma perspectiva histórica. In: GUEIROS, Guilherme; WENDT, Emerson (org.). *Ransomware 360°: abordagens multidisciplinares da extorsão criptoviral*. São Paulo: Mizuno, 2024, p. 28.

[25] ELSAD, A. Threat assessment: Black Basta ransomware. *Unit 42 – Palo Alto Networks*, 2022. Disponível em: https://unit42.paloaltonetworks.com/threat-assessment-black-basta-ransomware/. Acesso em: 3 jun. 2026.

Com a adoção de múltiplos métodos de extorsão, diversos operadores de RaaS passaram a empregar esse modelo em razão de sua lucratividade. Conforme Carmo[26], entre os grupos que adotaram essa estratégia destacou-se o REvil, identificado em 2019 e relacionado a um dos maiores pedidos de resgate já registrados, no valor aproximado de US$ 100.000.000. O grupo também esteve associado ao ataque de *ransomware* sofrido pelo Tribunal de Justiça do Rio Grande do Sul (TJRS), ocorrido em abril de 2021, conforme noticiado à época:

> De acordo com o BleepingComputer, que recebeu capturas de tela de conversas entre funcionários do tribunal, o TJ-RS foi infectado com um ransomware REvil que criptografou dados do servidor e dos funcionários, interrompendo sistemas eletrônicos além de ter forçado o tribunal desligar sua rede, por precaução. Os cibercriminosos estão pedindo U$ 5 milhões (R$ 27 milhões) pelo resgate dos dados criptografados. O grupo REvil, responsável pelo ransomware que atingiu o tribunal, oferece o malware no formato de *Ransomware* as a Service (RaaS). Ou seja, o malware pode ser "alugado" para outras pessoas, interessadas em comprometer determinada empresa. Após um ataque bem-sucedido, os desenvolvedores do REvil e a pessoa que alugou seus serviços dividem o valor do resgate.[27]

Outro grupo de *ransomware* que se destacou pela mesma dinâmica foi o LockBit. Segundo Carmo[28], seu fundador teria iniciado as atividades em comunidades de *ransomware* até desenvolver estrutura própria, da qual surgiram as variantes LockBit Red e LockBit Black, com métodos de criptografia mais rápidos e eficientes. O grupo também adotava práticas semelhantes às dos programas de "*Bug Bounty*" utilizados por empresas de tecnologia, oferecendo recompensas a pesquisadores de segurança que identificassem vulnerabilidades capazes de aperfeiçoar suas operações. Além disso, buscava consolidar sua marca e incentivar a fidelização de afiliados por meio de campanhas de divulgação.

Compreendidos os conceitos e as características do *ransomware* e da modalidade RaaS, torna-se necessário examinar a evolução do instituto da organização criminosa e sua aplicação diante das novas formas de criminalidade digital, especialmente quanto às estruturas organizadas no ambiente virtual.

---

[26] CARMO, Marcus Fábio Fontenelle do. *Ransomware*: uma perspectiva histórica. In: GUEIROS, Guilherme; WENDT, Emerson (org.). *Ransomware 360°: abordagens multidisciplinares da extorsão criptoviral*. São Paulo: Mizuno, 2024, p. 36.

[27] PETRY, Guilherme. TJ-RS é vítima do ransomware REvil. *The Hack*, 2021. Disponível em: https://thehack.com.br/tj-rs-e-vitima-do-ransomware-revil-gangue-pede-u-5-milhoes-pelo-resgate/. Acesso em: 9 jun. 2026.

[28] CARMO, Marcus Fábio Fontenelle do. *Ransomware*: uma perspectiva histórica. In: GUEIROS, Guilherme; WENDT, Emerson (org.). *Ransomware 360°: abordagens multidisciplinares da extorsão criptoviral*. São Paulo: Mizuno, 2024, p. 36-38.

3. ORGANIZAÇÃO CRIMINOSA DIGITAL NO BRASIL

Neste capítulo, discute-se o conceito legal de organização criminosa e os requisitos estabelecidos na Lei nº 12.850/2013. Em seguida, analisa-se a evolução legislativa no combate às organizações criminosas promovida pela Lei nº 15.358/2026. Por fim, examinam-se as adaptações do crime organizado ao ambiente cibernético.

3.1 Conceito legal e requisitos da organização criminosa

O conceito legal de organização criminosa foi objeto de intensos debates no ordenamento jurídico brasileiro. Desde a vigência do Código Penal de 1940[29] e, posteriormente, da Lei nº 9.034/1995[30], previam-se mecanismos destinados à repressão das ações praticadas por grupos criminosos; contudo, nenhum desses diplomas estabelecia uma definição jurídica de organização criminosa, circunstância que contribuía para interpretações divergentes.[31]

Um dos primeiros marcos ocorreu com a adesão do Brasil à Convenção das Nações Unidas contra o Crime Organizado Transnacional (Convenção de Palermo), promulgada pelo Decreto nº 5.015/2004[32]. A Convenção introduziu o conceito de grupo criminoso organizado e influenciou o desenvolvimento da legislação nacional. Contudo, sua incorporação ao direito interno não foi suficiente para solucionar as divergências de enquadramento, diante da ausência de definição legal no Código Penal brasileiro.[33]

Diante dessa necessidade, sobreveio inicialmente a Lei nº 12.694/2012[34], que apresentou o primeiro conceito legal de organização criminosa. Posteriormente, a Lei nº 12.850

---

[29] BRASIL. *Decreto-Lei nº 2.848, de 7 de dezembro de 1940*. Código Penal. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 2 jul. 2026.

[30] BRASIL. *Lei nº 9.034, de 3 de maio de 1995*. Dispõe sobre a utilização de meios operacionais para a prevenção e repressão de ações praticadas por organizações criminosas. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9034.htm. Acesso em: 25 jun. 2026.

[31] FAYET JÚNIOR, Ney; MAYA, André Machado; MARCELLO, Diogo. *Criminalidade organizada*. Porto Alegre: Núria Fabris, 2012, p. 31-43.

[32] BRASIL. *Decreto nº 5.015, de 12 de março de 2004*. Promulga a Convenção das Nações Unidas contra o Crime Organizado Transnacional. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2004-2006/2004/decreto/d5015.htm. Acesso em: 15 jun. 2026.

[33] FAYET JÚNIOR, Ney; MAYA, André Machado; MARCELLO, Diogo. *Criminalidade organizada*. Porto Alegre: Núria Fabris, 2012, p. 58-60.

[34] BRASIL. *Lei nº 12.694, de 24 de julho de 2012*. Dispõe sobre o processo e o julgamento colegiado em primeiro grau de jurisdição de crimes praticados por organizações criminosas; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal, o Decreto-Lei nº 3.689, de 3 de outubro de 1941 – Código de Processo Penal, e as Leis nºs 9.503, de 23 de setembro de 1997 – Código de Trânsito Brasileiro, e 10.826, de 22 de dezembro de 2003; e dá outras providências. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12694.htm. Acesso em: 25 jun. 2026.

revogou a Lei nº 9.034/1995, consolidando a definição vigente de organização criminosa[35] e passou a disciplinar a investigação criminal, os meios de obtenção de prova, as infrações penais correlatas e o procedimento criminal aplicável.[36]

Nessa conceituação, destacam-se os elementos da composição da organização criminosa, especialmente a reunião de quatro ou mais pessoas com finalidade voltada à prática de infrações penais. A partir desse elemento quantitativo, passa-se à análise da estrutura ordenada e da divisão de tarefas, que a diferenciam de formas menos estruturadas de atuação. Para tanto, exige-se um mínimo de organização hierárquica estável, com distribuição de tarefas e obrigações mútuas, sem que seja necessária formalização.[37]

A legislação também estabelece requisitos relacionados à finalidade da atuação criminosa, especialmente a exigência de obter, direta ou indiretamente, vantagem de qualquer natureza. Trata-se de elemento do tipo penal e de finalidade da prática delituosa, indispensável à caracterização da organização criminosa. Nesse sentido, o legislador optou por não restringir o conceito, utilizando a expressão "vantagem de qualquer natureza". Por isso, a vantagem não pode ser compreendida exclusivamente como econômica, pois a prática delituosa pode visar a outras finalidades além da obtenção de proveito patrimonial.[38]

Além disso, constitui requisito legal a prática de infrações penais cujas penas máximas sejam superiores a quatro anos ou que tenham caráter transnacional. Desse modo, o legislador delimitou as infrações que podem ser praticadas no âmbito da organização criminosa, mantendo conformidade com os tratados e as convenções internacionais.[39]

Embora a Lei nº 15.358/2026 tenha sido concebida para combater organizações ultraviolentas, sua edição evidencia a ampliação dos mecanismos de enfrentamento ao crime organizado e reforça a necessidade de examinar sua manifestação no ambiente digital.

---

[35] BRASIL. *Lei nº 12.850, de 2 de agosto de 2013*. Considera-se organização criminosa a associação de 4 (quatro) ou mais pessoas estruturalmente ordenada e caracterizada pela divisão de tarefas, ainda que informalmente, com objetivo de obter, direta ou indiretamente, vantagem de qualquer natureza, mediante a prática de infrações penais cujas penas máximas sejam superiores a 4 (quatro) anos, ou que sejam de caráter transnacional. Art. 1º, § 1º. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12850.htm. Acesso em: 15 jun. 2026.

[36] BITENCOURT, Cezar Roberto; BUSATO, Paulo César. *Comentários à Lei de Organização Criminosa: Lei n. 12.850/2013*. São Paulo: Saraiva, 2014, p. 17-25.

[37] BITENCOURT, Cezar Roberto; BUSATO, Paulo César. *Comentários à Lei de Organização Criminosa: Lei n. 12.850/2013*. São Paulo: Saraiva, 2014, p. 27-32.

[38] BITENCOURT, Cezar Roberto; BUSATO, Paulo César. *Comentários à Lei de Organização Criminosa: Lei n. 12.850/2013*. São Paulo: Saraiva, 2014, p. 32-35.

[39] BITENCOURT, Cezar Roberto; BUSATO, Paulo César. *Comentários à Lei de Organização Criminosa: Lei n. 12.850/2013*. São Paulo: Saraiva, 2014, p. 35-37.

3.2 Lei nº 15.358/2026 e o combate às organizações criminosas

A Lei nº 15.358, promulgada em 24 de março de 2026 e denominada Lei Raul Jungmann, instituiu o Marco Legal do Combate ao Crime Organizado no Brasil. Conhecida também como Lei Antifacção, a norma não substitui a definição geral de organização criminosa prevista na Lei nº 12.850/2013. Seu objetivo central é enfrentar organizações criminosas ultraviolentas, grupos paramilitares e milícias privadas, além de tipificar os crimes de domínio social estruturado e de favorecimento ao domínio social estruturado.[40]

A nova disciplina considera a escalabilidade que certas organizações criminosas alcançaram no contexto atual, ao utilizarem estruturas que ultrapassam um simples grupo de indivíduos e se aproximam de uma empresa, com setores organizados e divisão de tarefas. Essa estrutura supera a ideia tradicional de hierarquia, pois seus integrantes podem ser substituídos sem comprometer a continuidade das atividades, consolidando uma organização resistente e capaz de operar em escala superior à capacidade de resposta do Estado.[41]

No contexto de aplicação da nova lei, é importante identificar os elementos nucleares da criminalidade por ela abrangida, especialmente diante da distinção conceitual entre associação criminosa, organização criminosa, milícia privada e facção criminosa. A Lei nº 15.358/2026 acrescenta a esse quadro a figura da organização criminosa ultraviolenta, denominada expressamente facção criminosa. O art. 2º, § 2º, dispõe nos seguintes termos:[42]

> Para os fins desta Lei, considera-se organização criminosa ultraviolenta, denominada facção criminosa, o agrupamento de 3 (três) ou mais pessoas que emprega violência, grave ameaça ou coação para impor controle territorial ou social, intimidar populações ou autoridades ou atacar serviços, infraestrutura ou equipamentos essenciais ou que pratica atos destinados à execução dos crimes tipificados nesta Lei.[43]

A partir disso, constatam-se elementos nucleares que não se confundem com aqueles previstos na Lei nº 12.850/2013. A facção criminosa exige número inferior de

---

[40] MARQUES, Vinicius Martins. *O Brasil sob domínio: nova Lei Antifacção*. [S. l.]: [s. n.], 2026. E-book, p 9-12.
[41] MARQUES, Vinicius Martins. *O Brasil sob domínio: nova Lei Antifacção*. [S. l.]: [s. n.], 2026. E-book, p. 13-16.
[42] MARQUES, Vinicius Martins. *O Brasil sob domínio: nova Lei Antifacção*. [S. l.]: [s. n.], 2026. E-book, p. 17-21.
[43] BRASIL. *Lei nº 15.358, de 24 de março de 2026.* Institui o Marco Legal do Combate ao Crime Organizado no Brasil (Lei Raul Jungmann); tipifica os crimes de domínio social estruturado e de favorecimento ao domínio social estruturado; e altera os Decretos-Leis nºs 2.848/1940 (Código Penal) e 3.689/1941 (Código de Processo Penal), e as Leis nºs 8.072/1990, 7.210/1984, 11.343/2006, 10.826/2003, 9.613/1998, 4.737/1965, 13.756/2018 e 14.790/2023. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2026/lei/l15358.htm. Acesso em: 27 jun. 2026.

integrantes para sua caracterização, sendo suficiente a reunião de três pessoas, além de possuir finalidade voltada ao controle territorial ou social mediante violência, grave ameaça ou coação. Para fins de aplicação, o art. 4º, parágrafo único, da Lei nº 15.358/2026 prevê a incidência subsidiária das disposições materiais da Lei nº 12.850/2013.[44]

A partir dos avanços introduzidos pela Lei Antifacção, verifica-se o endurecimento do enfrentamento de crimes de elevada violência. Apesar disso, a nova lei evidencia a coexistência de múltiplos conceitos relacionados à organização criminosa, circunstância que pode gerar dificuldades na aplicação do processo penal. Diante de conceitos com elevado grau de subjetividade, impõe-se a observância do princípio da estrita legalidade, evitando-se termos genéricos que possam comprometer a efetividade da norma.[45]

Além dos argumentos já apresentados, a nova legislação suscita discussões em relação a princípios constitucionais como a presunção de inocência, a proporcionalidade e a taxatividade. O combate às organizações criminosas ultraviolentas, embora legítimo e necessário, não pode se sobrepor aos limites constitucionais previstos na Constituição Federal[46], especialmente quanto à proteção dos direitos e garantias fundamentais.[47]

A lei também suscita debates acerca de sua constitucionalidade e de eventual manifestação de populismo penal, ao apresentar soluções simplificadas para problemas que afetam a sociedade há longo tempo. A adoção de medidas como o aumento de penas, sob o argumento de combater a impunidade, pode ser insuficiente diante de problemas estruturais que efetivamente deveriam ser enfrentados pelo Estado.[48]

Embora a Lei nº 15.358/2026 tenha sido concebida para combater organizações ultraviolentas, sua edição evidencia a ampliação dos mecanismos de enfrentamento ao crime organizado e reforça a necessidade de examinar sua manifestação no ambiente digital.

---

[44] MARQUES, Vinicius Martins. *O Brasil sob domínio: nova Lei Antifacção*. [S. l.]: [s. n.], 2026. E-book, p. 22-29.

[45] PAULINO, Galtiênio da Cruz. Lei Antifacção e a fragmentação do conceito de organização criminosa. *JOTA*, 24 abr. 2026. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/lei-antifaccao-e-a-fragmentacao-do-conceito-de-organizacao-criminosa. Acesso em: 29 jun. 2026.

[46] BRASIL. *[Constituição (1988)]. Constituição da República Federativa do Brasil de 1988*. Brasília, DF: Presidência da República, [2026]. Disponível em: https://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm. Acesso em: 2 jul. 2026.

[47] COELHO, Daniela Caldas Rosa Alves; COELHO, Renato Gustavo Alves. O marco legal do combate ao crime organizado: análise crítica da Lei 15.358/26 (Lei Raul Jungmann). *Migalhas*, 27 abr. 2026. Disponível em: https://www.migalhas.com.br/depeso/454683/o-marco-legal-do-combate-ao-crime-organizado-analise-da-lei-15-358-26. Acesso em: 27 jun. 2026.

[48] YAROCHEWSKY, Leonardo Isaac. Breves considerações sobre a Lei Antifacção. *Jornal de Ciências Criminais do IBCCRIM*, 30 mar. 2026. Disponível em: https://jcc.ibccrim.org.br/colunistas/breves-consideracoes-sobre-a-lei-antifaccao/. Acesso em: 27 jun. 2026.

3.3 Crime organizado cibernético

As organizações criminosas passaram a adotar novos mecanismos de atuação em razão dos avanços tecnológicos, empregando recursos digitais para a prática de atividades ilícitas. Nesse contexto, o cibercrime representa um mercado ilícito em ascensão, que opera sob uma lógica empresarial e em estruturas de rede (*networks*), afastando-se dos modelos tradicionais de organização criminosa e diversificando suas operações relacionadas aos crimes cibernéticos.[49]

Os grupos que integram as redes criminosas relacionadas ao crime organizado cibernético variam de acordo com a atividade desempenhada, com a divisão do trabalho estabelecida a partir da especialização de seus integrantes ou com a demanda de agentes externos. Em muitos casos, não utilizam nomes para identificar suas organizações nem nomeiam suas operações, embora atuem de forma coordenada. As identidades dos agentes podem ser conhecidas apenas pelo mentor da atividade criminosa, enquanto a comunicação é realizada por meio de pseudônimos, dificultando a identificação dos próprios membros da organização entre si.[50]

As operações ocorrem tanto *online* quanto *offline*. Nas categorias *online*, os grupos têm como atividade principal a prática de crimes cibernéticos, destacando-se as estruturas denominadas enxames e *hubs*.

Na modalidade enxame, observa-se uma rede descentralizada que distribui tarefas específicas com a finalidade de cometer crimes cibernéticos em curto espaço de tempo. Após a conclusão da atividade, os participantes podem abandonar o grupo, que permanece aberto à adesão de novos integrantes. Em geral, essas estruturas têm como objetivo comum a prática de cibercrimes motivados por razões ideológicas, como ocorre com o grupo *Anonymous*.[51]

---

[49] NURSE, Jason R. C.; BADA, Maria. The group element of cybercrime: types, dynamics, and criminal operations. In: ATTRILL-SMITH, Alison; FULLWOOD, Chris; KEEP, Melanie; KUSS, Daria J. (ed.). *The Oxford handbook of cyberpsychology*. Oxford: Oxford University Press, 2019. cap. 34. DOI: 10.1093/oxfordhb/9780198812746.013.36. Disponível em: https://doi.org/10.1093/oxfordhb/9780198812746.013.36. Acesso em: 12 jun. 2026.

[50] CUNHA, Bruno Requião da. Facções criminais: estrutura, energia e neutralização seletiva em sistemas complexos do crime organizado. In: BRASIL. Ministério da Justiça e Segurança Pública. Secretaria Nacional de Acesso à Justiça. *Criminalidade organizada: diagnóstico e políticas públicas e legislativas.* Brasília: Ministério da Justiça e Segurança Pública, 2026. p. 14-37. Disponível em: https://www.gov.br/mj/pt-br/assuntos/noticias/especialistas-apresentam-dez-caminhos-para-enfrentar-o-crime-organizado/PublicacaoCriminalidadeOrganizada_FINAL.pdf. Acesso em: 27 jun. 2026.

[51] MARTINS, Thiago Messias. *Ransomware*: tipologia do crime organizado cibernético. In: GUEIROS, Guilherme; WENDT, Emerson (org.). *Ransomware 360°: abordagens multidisciplinares da extorsão criptoviral*. São Paulo: Mizuno, 2024, p. 187-193.

Por sua vez, os *hubs* são compostos por um núcleo de criminosos cercado por agentes periféricos, motivados principalmente pela obtenção de lucro. Apresentam estrutura mais ordenada e disponibilizam serviços ilícitos para contratação, caracterizando modelos conhecidos como *Cybercrime-as-a-Service* (CaaS).

Também existem grupos híbridos clusterizados, que utilizam o ambiente digital como meio para a prática de crimes predominantemente *offline*. Por fim, há grupos que atuam de maneira essencialmente *offline*, aproximando-se das organizações criminosas tradicionais e utilizando recursos tecnológicos apenas como instrumento de expansão de suas atividades ilícitas.[52]

No processo de formação e integração entre os agentes, o próprio ambiente *online* atua como facilitador da interação entre os integrantes dessas redes criminosas, uma vez que a comunicação ocorre por meio de chats e fóruns virtuais, preservando o anonimato dos participantes.

Além disso, a confiança constitui fator determinante para a formação e a manutenção dos grupos, uma vez que os participantes dependem da credibilidade atribuída aos serviços disponibilizados no ambiente da *Dark Web*[53]. Por essa razão, diversos fóruns exigem a utilização do *Tor*[54] e a realização de transações por meio de criptomoedas, reforçando o anonimato e o cumprimento de regras internas.[55]

A expansão da criminalidade cibernética trouxe novos grupos e novas modalidades criminosas, tornando necessária a adequada tipificação dessas condutas à luz da legislação existente. Diante disso, o capítulo seguinte analisa o enquadramento jurídico do modelo RaaS a partir dos conceitos e elementos apresentados.

---

[52] MARTINS, Thiago Messias. *Ransomware*: tipologia do crime organizado cibernético. In: GUEIROS, Guilherme; WENDT, Emerson (org.). *Ransomware 360°: abordagens multidisciplinares da extorsão criptoviral*. São Paulo: Mizuno, 2024, p. 194.

[53] BOMFATI, Cláudio Adriano; KOLBE JÚNIOR, Armando. *Crimes cibernéticos*. Curitiba: InterSaberes, 2020, p. 99-100. A *Dark Web* é uma pequena parcela da *Deep Web*, acessível apenas por programas específicos, não indexada pelos mecanismos tradicionais de busca e frequentemente utilizada para preservar o anonimato dos usuários, inclusive em atividades ilícitas.

[54] BOMFATI, Cláudio Adriano; KOLBE JÚNIOR, Armando. *Crimes cibernéticos*. Curitiba: InterSaberes, 2020, p. 100-101. O *Tor* (*The Onion Router*) é um software de navegação que permite o acesso anônimo à *Dark Web* por meio de uma rede que oculta a origem da conexão do usuário.

[55] NURSE, Jason R. C.; BADA, Maria. The group element of cybercrime: types, dynamics, and criminal operations. In: ATTRILL-SMITH, Alison; FULLWOOD, Chris; KEEP, Melanie; KUSS, Daria J. (ed.). *The Oxford handbook of cyberpsychology*. Oxford: Oxford University Press, 2019. cap. 34. DOI: 10.1093/oxfordhb/9780198812746.013.36. Disponível em: https://doi.org/10.1093/oxfordhb/9780198812746.013.36. Acesso em: 12 jun. 2026.

4. ANÁLISE DO MODELO RANSOMWARE-AS-A-SERVICE COMO ORGANIZAÇÃO CRIMINOSA DIGITAL

O presente capítulo analisa os aspectos jurídicos do *ransomware*, a compatibilidade do modelo RaaS com os requisitos da Lei nº 12.850/2013, os desafios relacionados ao seu enquadramento jurídico e sua possível adaptação a partir de novas perspectivas legislativas.

4.1 Aspectos jurídicos do crime de *ransomware*

O *ransomware* tem origem na cibercriminalidade e constitui crime informático[56], resultante da evolução de práticas criminosas tradicionais com o incremento do uso da tecnologia. Sua execução por intermédio de dispositivos eletrônicos permite maior eficiência e escalabilidade dos ataques.[57]

No Brasil, o Congresso Nacional aprovou a adesão do país à Convenção de Budapeste por meio do Decreto Legislativo nº 37/2021[58]. Esse ato representou marco no reconhecimento da informática como objeto de tutela jurídica e relaciona-se às diretrizes voltadas à adequação dos ordenamentos jurídicos dos países signatários para o enfrentamento transnacional dos crimes informáticos.[59]

Até então, o ordenamento brasileiro ainda carecia de tipificação específica para determinados crimes informáticos. Conforme Masson[60], esse cenário mudou após a invasão do computador e o vazamento de fotografias íntimas da atriz Carolina Dieckmann, episódio que gerou forte repercussão pública. Com isso, foi promulgada a Lei nº 12.737/2012[61], que incluiu

---

[56] SYDOW, Spencer Toth. *Curso de direito penal informático: partes geral e especial*. Salvador: JusPodivm, 2021, p. 45.
[57] CABRAL SAISSE, Renan. *Ransomware*: sequestro de dados e extorsão digital. *Direito & TI*, [S. l.], v. 1, n. 6, 2016. DOI: 10.63451/ti.v1i6.44. Disponível em: https://direitoeti.com.br/direitoeti/article/view/44. Acesso em: 9 jun. 2026.
[58] BRASIL. *Decreto Legislativo nº 37, de 16 de dezembro de 2021*. Aprova o texto da Convenção sobre o Crime Cibernético, celebrada em Budapeste, em 23 de novembro de 2001. Disponível em: https://www2.camara.leg.br/legin/fed/decleg/2021/decretolegislativo-37-16-dezembro-2021-792105-norma-pl.html. Acesso em: 15 jun. 2026.
[59] BARBOSA, Guilherme Gueiros de Freitas. *A tipicidade dos ataques de ransomware no Brasil: uma interseção entre criptovirologia e direito penal*. São Paulo: D'Plácido, 2022, p. 45-48.
[60] MASSON, Cleber. *Código penal comentado*. 2. ed. São Paulo: Método, 2018, p. 608.
[61] BRASIL. *Lei nº 12.737, de 30 de novembro de 2012*. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal; e dá outras providências. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 15 jun. 2026.

o art. 154-A no Código Penal e introduziu a terminologia "dispositivo informático". Ainda assim, permaneceram lacunas legislativas decorrentes da complexidade interpretativa.[62]

O *ransomware* ainda não possui tipificação expressa no Código Penal. Entretanto, conforme o *iter criminis*, a conduta pode ser enquadrada, em tese, como invasão de dispositivo informático simples ou qualificada (art. 154-A e § 3º), dano (art. 163) e extorsão (art. 158), todos do Código Penal. Tais delitos podem ser absorvidos pelo princípio da consunção, quando os delitos-meio constituírem etapas necessárias do crime-fim.[63] Todavia, ela poderá ser afastada quando houver resultados autônomos. Assim, a complexidade dos ataques permite o preenchimento concomitante de diferentes tipos penais, conforme as condutas do agente.[64]

Quanto ao tipo penal da extorsão, Nucci[65] sustenta que se trata de crime de natureza formal, não dependendo da ocorrência de efetivo dano patrimonial para a consumação, bastando que a vítima seja constrangida pela exigência formulada pelo agente.

Sobre a temática, também merece destaque a redação da Súmula nº 96 do Superior Tribunal de Justiça[66], segundo a qual: "O crime de extorsão consuma-se independentemente da obtenção da vantagem indevida". A partir desse entendimento, extrai-se que a consumação do delito decorre do constrangimento exercido sobre a vítima, independentemente da efetiva obtenção do proveito econômico pretendido.[67]

Embora a responsabilização penal pelos delitos decorrentes dos ataques de *ransomware* encontre possível enquadramento na legislação, surge a questão de saber se a estrutura do modelo RaaS pode configurar também o crime autônomo de organização criminosa. O próximo subcapítulo examina essa possibilidade.

---

[62] WENDT, Emerson. Que expectativas de estruturação normativo-penal sobre o *ransomware* no Brasil? In: GUEIROS, Guilherme; WENDT, Emerson (org.). *Ransomware 360°: abordagens multidisciplinares da extorsão criptoviral*. São Paulo: Mizuno, 2024, p. 279-285.

[63] BARBOSA, Guilherme Gueiros de Freitas. *A tipicidade dos ataques de ransomware no Brasil: uma interseção entre criptovirologia e direito penal*. São Paulo: D'Plácido, 2022, p. 161-165.

[64] MASSENO, Manoel Davi. Ataques de ransomware na Convenção de Budapeste sobre o crime cibernético: um ensaio de qualificação alternativa. In: GUEIROS, Guilherme; WENDT, Emerson (org.). *Ransomware 360°: abordagens multidisciplinares da extorsão criptoviral*. São Paulo: Mizuno, 2024, p. 270-276.

[65] NUCCI, Guilherme de Souza. *Código penal comentado*. 2. ed. São Paulo: Revista dos Tribunais, 2002, p. 451.

[66] BRASIL. Superior Tribunal de Justiça. Súmula n. 96. O crime de extorsão consuma-se independentemente da obtenção da vantagem indevida. Terceira Seção, Brasília, DF, 3 mar. 1994. *Diário da Justiça*, Brasília, DF, 10 mar. 1994, p. 4.021. Disponível em: https://www.stj.jus.br/docs_internet/revista/eletronica/stj-revista-sumulas-2010_7_capSumula96.pdf. Acesso em: 2 jul. 2026.

[67] BARBOSA, Guilherme Gueiros de Freitas. *A tipicidade dos ataques de ransomware no Brasil: uma interseção entre criptovirologia e direito penal*. São Paulo: D'Plácido, 2022, p. 118.

4.2 Enquadramento jurídico do *Ransomware-as-a-Service* como organização criminosa

A organização criminosa somente pode ser caracterizada pela associação de, no mínimo, quatro pessoas, conforme requisito formal previsto no art. 1º, § 1º, da Lei nº 12.850/2013.[68] Assim, o modelo RaaS, formado pela atuação conjunta de desenvolvedores, afiliados e demais envolvidos nos ataques, pode preencher o requisito relativo ao número de integrantes, desde que composto por, no mínimo, quatro pessoas. [69]

Além do número mínimo de integrantes, Nucci[70] destaca a necessidade de uma estrutura organizada, com algum grau de hierarquia e escalonamento interno que permita identificar as funções desempenhadas e a posição dos integrantes. Esse requisito mostra-se compatível, em tese, com o modelo RaaS, que opera sob lógica empresarial e dispõe de estrutura organizada pelos próprios operadores do serviço.[71]

A divisão de tarefas constitui elemento caracterizador da organização criminosa, exigindo que cada integrante desempenhe determinada atividade, sem necessidade de formalização, em razão da natureza ilícita da organização. No modelo RaaS, essa característica pode ser identificada na atuação de desenvolvedores responsáveis pelo desenvolvimento do *ransomware* e de afiliados encarregados da execução dos ataques.[72] Nesse sentido, Bitencourt[73] destaca que a divisão de tarefas também se complementa pela estrutura estável e permanente, circunstância que pode ser observada, em tese, em grupos como LockBit e REvil, que permaneceram em atividade por longos períodos, aperfeiçoando suas variantes e mantendo a continuidade de suas operações criminosas.

Além da divisão de tarefas, a Lei exige que a organização criminosa tenha como finalidade a obtenção de vantagem de qualquer natureza. Essa vantagem constitui elementar do crime de organização criminosa e não se restringe necessariamente ao aspecto econômico, pois o legislador optou pela expressão "vantagem de qualquer natureza". A repartição dos lucros

---

[68] NUCCI, Guilherme de Souza. *Organização criminosa*. 5. ed. Rio de Janeiro: Forense, 2021, p. 1.
[69] **Nota do autor**. A presente pesquisa limita-se à análise da compatibilidade estrutural do modelo *Ransomware-as-a-Service* com os requisitos previstos na Lei nº 12.850/2013, não constituindo seu objetivo examinar, de forma individualizada, os critérios de imputação penal aplicáveis aos diferentes agentes envolvidos no ecossistema do RaaS, como desenvolvedores, afiliados, negociadores ou operadores financeiros.
[70] NUCCI, Guilherme de Souza. *Organização criminosa*. 5. ed. Rio de Janeiro: Forense, 2021, p. 2-3.
[71] NAGAR, Gourav. The evolution of ransomware: tactics, techniques, and mitigation strategies. *SSRN Electronic Journal*, 2024. Disponível em: https://ssrn.com/abstract=4881213. Acesso em: 3 jun. 2026.
[72] NUCCI, Guilherme de Souza. *Organização criminosa*. 5. ed. Rio de Janeiro: Forense, 2021, p. 4.
[73] BITENCOURT, Cezar Roberto. *Tratado de direito penal: parte especial: crimes contra o patrimônio até crimes contra o sentimento religioso e contra o respeito aos mortos*. 10. ed. rev., ampl. e atual. São Paulo: Saraiva, 2014, E-book, n.p.

entre desenvolvedores e afiliados reforça, em tese, a existência de estrutura organizada voltada à obtenção de vantagem econômica[74], já que o modelo RaaS pode ter como finalidade a obtenção de vantagem por meio da exigência de pagamento de resgates e da adoção de múltiplos métodos de extorsão.[75]

Outro requisito consiste na prática de infrações penais cujas penas máximas sejam superiores a quatro anos. Nesse aspecto, o modelo RaaS demonstra compatibilidade, em tese, com esse requisito legal, uma vez que os ataques de *ransomware* podem configurar diferentes infrações penais, a depender das circunstâncias do caso concreto, entre elas os crimes de invasão de dispositivo informático, previsto no art. 154-A do Código Penal, e de extorsão, previsto no art. 158 do mesmo diploma legal, cujas penas máximas podem superar o limite estabelecido pela Lei nº 12.850/2013.

A prática de infrações penais de caráter transnacional também constitui previsão da Lei nº 12.850/2013. Independentemente da natureza da infração penal ou da pena máxima abstratamente cominada, a transposição de fronteiras nacionais permite a caracterização da organização criminosa, tanto quando a atividade criminosa se inicia no Brasil e produz efeitos no exterior quanto na hipótese inversa.[76] Sob esse aspecto, o modelo RaaS apresenta compatibilidade, em tese, com esse requisito, já que seus agentes podem estar distribuídos em diferentes países[77], atuando de forma coordenada contra vítimas localizadas no território nacional ou no exterior.[78]

Diante da análise dos requisitos da Lei nº 12.850/2013, conclui-se que o modelo RaaS apresenta, em tese, compatibilidade com a caracterização de organização criminosa, especialmente pela divisão de funções, pela atuação coordenada e pela finalidade de obtenção de vantagem econômica. Desse modo, a estrutura descentralizada do RaaS não impede seu enquadramento jurídico, desde que demonstrados, no caso concreto, os requisitos legais. No próximo subcapítulo, examinam-se as lacunas da legislação vigente e as perspectivas legislativas relacionadas ao modelo RaaS.

---

[74] NUCCI, Guilherme de Souza. *Organização criminosa*. 5. ed. Rio de Janeiro: Forense, 2021, p. 4.
[75] AGUILAR ANTONIO, Juan Manuel. *Ransomware gangs and hacktivists: cyber threats to governments in Latin America*. Miami: Jack D. Gordon Institute for Public Policy, Florida International University, 2024. Disponível em: https://digitalscholarship.fiu.edu/record/19461?v=pdf. Acesso em: 3 jun. 2026.
[76] NUCCI, Guilherme de Souza. *Organização criminosa*. 5. ed. Rio de Janeiro: Forense, 2021, p. 5-6.
[77] **Nota do autor.** Embora a transnacionalidade constitua característica associada às operações de *RaaS*, a análise dos mecanismos de cooperação jurídica internacional extrapola a delimitação temática desta pesquisa.
[78] ELLOVITCH, Mauro da Fonseca. *Organizações criminosas especializadas em cibercrimes*. Artigo científico. [**No prelo].**

4.3 Limites jurídicos do *Ransomware-as-a-Service* e perspectivas legislativas

Constatada a compatibilidade, em tese, do modelo RaaS com os requisitos previstos na Lei nº 12.850/2013, torna-se necessário analisar os limites desse enquadramento, que decorre da interpretação dos elementos estabelecidos pela legislação vigente. Entretanto, a legislação não contempla, de forma específica, a definição de organização criminosa digital.

Embora o ordenamento jurídico brasileiro permita o enquadramento do *ransomware* e do modelo RaaS por meio da interpretação de dispositivos existentes, inexiste disciplina normativa específica para essas modalidades criminosas. A ausência de definição legal para as organizações criminosas digitais faz com que seu enquadramento decorra da interpretação dos institutos previstos na legislação penal, circunstância que evidencia a necessidade de aperfeiçoamento legislativo diante da evolução das estruturas criminosas cibernéticas.[79]

A ausência de critérios normativos objetivos pode gerar insegurança jurídica e comprometer a proteção dos direitos e das garantias fundamentais assegurados pela Constituição da República. Assim, evidencia-se a necessidade de disciplina normativa específica dessas modalidades, em observância aos postulados da *lex praevia* e, sobretudo, da *lex certa*, impondo ao Estado o dever de delimitar previamente o conteúdo e os limites de sua atuação punitiva. O exercício do *jus puniendi* somente se legitima quando fundado na estrita legalidade e exercido em conformidade com as garantias constitucionais do devido processo legal.[80]

A definição normativa da organização criminosa digital e das modalidades criminosas correlatas revela-se necessária para evitar a utilização de conceitos excessivamente amplos no enfrentamento das novas formas de criminalidade. O processo penal não constitui mero instrumento destinado à punição, mas mecanismo de contenção do poder punitivo estatal; por isso, a atuação do Estado deve permanecer submetida às garantias constitucionais que estruturam o sistema acusatório.[81]

Sob essa perspectiva, a delimitação objetiva dos elementos caracterizadores da organização criminosa digital não apenas reforça a segurança jurídica e a taxatividade da norma

---

[79] FAYET JÚNIOR, Ney; MAYA, André Machado; MARCELLO, Diogo. *Criminalidade organizada*. Porto Alegre: Núria Fabris, 2012, p. 37-40

[80] FAYET JÚNIOR, Ney; MAYA, André Machado; MARCELLO, Diogo. *Criminalidade organizada*. Porto Alegre: Núria Fabris, 2012, p. 33-35.

[81] LOPES JR., Aury. *Fundamentos do processo penal: introdução crítica*. 10. ed. São Paulo: SaraivaJur, 2024, p. 58-62.

penal, mas também reduz o espaço para interpretações subjetivas incompatíveis com o devido processo legal e com a própria legitimidade do exercício do *jus puniendi*.[82]

A necessidade de aperfeiçoamento da legislação penal diante da evolução das organizações criminosas digitais passou a ser reconhecida pelo próprio legislador. Como reflexo dessa preocupação, foi apresentado o Projeto de Lei nº 4.614/2025, que propõe a inclusão da definição de organização criminosa digital na Lei nº 12.850/2013.

O art. 1º-A proposto pelo Projeto de Lei nº 4.614/2025 preserva elementos estruturais previstos na Lei nº 12.850/2013, mas os adapta às particularidades da criminalidade cibernética ao instituir a definição de organização criminosa digital. Para tanto, considera como elemento caracterizador a utilização habitual de meios tecnológicos ou cibernéticos para a prática de infrações penais, conforme dispõe a proposição:

> Art. 1º-A. Considera-se organização criminosa digital a associação de 3 (três) ou mais pessoas, estruturalmente ordenada e caracterizada pela divisão de tarefas, ainda que informalmente, que se valha, prioritária e habitualmente, de meios cibernéticos ou tecnológicos para a prática de crimes cujas penas máximas sejam superiores a 4 (quatro) anos, ou que sejam de caráter transnacional. [83]

Além da definição legal proposta, o projeto estabelece hipóteses específicas de aumento de pena relacionadas ao ambiente digital, como o emprego de mecanismos avançados de anonimização, a utilização de criptoativos e de plataformas virtuais destinadas à movimentação ou à ocultação de recursos ilícitos, bem como ataques direcionados contra infraestruturas críticas e instituições financeiras. Além disso, a proposição reconhece expressamente determinadas modalidades criminosas, incluindo o *ransomware* e o sequestro de dados.

A proposta representa avanço significativo ao conferir tratamento normativo específico a uma modalidade criminosa já consolidada no ambiente digital, reduzindo a dependência de interpretações extensivas e proporcionando maior segurança jurídica. Ressalta-se, contudo, que a análise da proposição não equivale a afirmar sua aprovação ou vigência.

---

[82] LOPES JR., Aury. *Fundamentos do processo penal: introdução crítica*. 10. ed. São Paulo: SaraivaJur, 2024, p. 291-298.

[83] BRASIL. *Projeto de Lei nº 4.614, de 2025*. Altera as Leis nº 12.850, de 2 de agosto de 2013, nº 9.613, de 3 de março de 1998, e nº 12.965, de 23 de abril de 2014, para aprimorar a tipificação, as penas e as medidas contra organizações criminosas digitais. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2561362. Acesso em: 2 jul. 2026.

5. CONSIDERAÇÕES FINAIS

A pesquisa permitiu concluir que, a partir da análise dos requisitos previstos na Lei nº 12.850/2013, a estrutura do RaaS apresenta compatibilidade, em tese, com os elementos caracterizadores da organização criminosa. Dessa forma, confirmou-se a hipótese inicialmente formulada, demonstrando que a descentralização dos ecossistemas digitais não impede o reconhecimento da organização criminosa quando presentes os requisitos legalmente exigidos.

Entretanto, o ordenamento jurídico brasileiro ainda não contempla definição específica do *ransomware* e da modalidade RaaS, tampouco disciplina expressamente as organizações criminosas digitais. Essa circunstância evidencia a necessidade de aplicação do princípio da taxatividade, segundo o qual a norma penal deve descrever de forma clara, precisa e determinada as condutas e os institutos jurídicos por ela disciplinados. A inexistência de previsão específica reduz a precisão normativa e amplia a necessidade de interpretações jurídicas para a adequação dessas condutas ao ordenamento vigente.

Além disso, a pesquisa não identificou precedentes específicos acerca do enquadramento jurídico do RaaS como organização criminosa nas bases de jurisprudência do Superior Tribunal de Justiça e do Supremo Tribunal Federal consultadas pelos autores, o que evidencia o baixo desenvolvimento jurisprudencial da matéria no âmbito dos tribunais superiores.

A pesquisa também examinou a Lei nº 15.358/2026, denominada Lei Antifacção, concebida para disciplinar organizações criminosas ultraviolentas voltadas ao domínio territorial ou social. Embora represente importante marco no combate ao crime organizado, seus pressupostos específicos não se mostram compatíveis, em regra, com a estrutura operacional do modelo RaaS, razão pela qual seu enquadramento nesse diploma legal não se revela adequado sem a demonstração dos elementos previstos na própria lei.

Conclui-se, portanto, que o Projeto de Lei nº 4.614/2025 possui potencial para conferir maior segurança jurídica ao enquadramento de estruturas como o RaaS, não porque a Lei nº 12.850/2013 seja incompatível com essa modalidade, mas porque a proposição estabelece conceitos específicos voltados à criminalidade digital e prevê expressamente práticas como o *ransomware*. Dessa forma, caso aprovado, poderá reduzir a necessidade de interpretações extensivas e reforçar a observância dos princípios da legalidade e da taxatividade, conferindo maior precisão normativa ao enfrentamento das organizações criminosas digitais sem afastar as garantias constitucionais que limitam o exercício do poder punitivo do Estado.

REFERÊNCIAS

AGUILAR ANTONIO, Juan Manuel. *Ransomware gangs and hacktivists: cyber threats to governments in Latin America.* Miami: Jack D. Gordon Institute for Public Policy, Florida International University, 2024. Disponível em: https://digitalscholarship.fiu.edu/record/19461?v=pdf. Acesso em: 3 jun. 2026.

BARBOSA, Guilherme Gueiros de Freitas. *A tipicidade dos ataques de ransomware no Brasil: uma interseção entre criptovirologia e direito penal*. São Paulo: D'Plácido, 2022.

BITENCOURT, Cezar Roberto. *Tratado de direito penal: parte especial: crimes contra o patrimônio até crimes contra o sentimento religioso e contra o respeito aos mortos*. 10. ed. rev., ampl. e atual. São Paulo: Saraiva, 2014. E-book.

BITENCOURT, Cezar Roberto; BUSATO, Paulo César. *Comentários à Lei de Organização Criminosa: Lei n. 12.850/2013*. São Paulo: Saraiva, 2014.

BOMFATI, Cláudio Adriano; KOLBE JÚNIOR, Armando. *Crimes cibernéticos*. Curitiba: InterSaberes, 2020.

BRASIL. *[Constituição (1988)]. Constituição da República Federativa do Brasil de 1988*. Brasília, DF: Presidência da República, [2026]. Disponível em: https://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm. Acesso em: 2 jul. 2026.

BRASIL. *Decreto nº 5.015, de 12 de março de 2004*. Promulga a Convenção das Nações Unidas contra o Crime Organizado Transnacional. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2004-2006/2004/decreto/d5015.htm. Acesso em: 15 jun. 2026.

BRASIL. *Decreto Legislativo nº 37, de 16 de dezembro de 2021*. Aprova o texto da Convenção sobre o Crime Cibernético, celebrada em Budapeste, em 23 de novembro de 2001. Disponível em: https://www2.camara.leg.br/legin/fed/decleg/2021/decretolegislativo-37-16-dezembro-2021-792105-norma-pl.html. Acesso em: 15 jun. 2026.

BRASIL. *Decreto-Lei nº 2.848, de 7 de dezembro de 1940*. Código Penal. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 2 jul. 2026.

BRASIL. *Lei nº 9.034, de 3 de maio de 1995*. Dispõe sobre a utilização de meios operacionais para a prevenção e repressão de ações praticadas por organizações criminosas. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9034.htm. Acesso em: 25 jun. 2026.

BRASIL. *Lei nº 12.694, de 24 de julho de 2012*. Dispõe sobre o processo e o julgamento colegiado em primeiro grau de jurisdição de crimes praticados por organizações criminosas; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal, o Decreto-Lei nº 3.689, de 3 de outubro de 1941 – Código de Processo Penal, e as Leis nºs 9.503, de 23 de setembro de 1997 – Código de Trânsito Brasileiro, e 10.826, de 22 de dezembro de 2003; e dá outras providências. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12694.htm. Acesso em: 25 jun. 2026.

BRASIL. *Lei nº 12.737, de 30 de novembro de 2012*. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal; e dá outras providências. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 15 jun. 2026.

BRASIL. *Lei nº 12.850, de 2 de agosto de 2013*. Define organização criminosa e dispõe sobre a investigação criminal, os meios de obtenção da prova, infrações penais correlatas e o procedimento criminal; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal); revoga a Lei nº 9.034, de 3 de maio de 1995; e dá outras providências. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12850.htm. Acesso em: 15 jun. 2026.

BRASIL. *Lei nº 15.358, de 24 de março de 2026.* Institui o Marco Legal do Combate ao Crime Organizado no Brasil (Lei Raul Jungmann); tipifica os crimes de domínio social estruturado e de favorecimento ao domínio social estruturado; e altera os Decretos-Leis nºs 2.848/1940 (Código Penal) e 3.689/1941 (Código de Processo Penal), e as Leis nºs 8.072/1990, 7.210/1984, 11.343/2006, 10.826/2003, 9.613/1998, 4.737/1965, 13.756/2018 e 14.790/2023. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2026/lei/l15358.htm. Acesso em: 27 jun. 2026.

BRASIL. *Projeto de Lei nº 4.614, de 2025*. Altera as Leis nº 12.850, de 2 de agosto de 2013, nº 9.613, de 3 de março de 1998, e nº 12.965, de 23 de abril de 2014, para aprimorar a tipificação, as penas e as medidas contra organizações criminosas digitais. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2561362. Acesso em: 2 jul. 2026.

BRASIL. Superior Tribunal de Justiça. Súmula n. 96. O crime de extorsão consuma-se independentemente da obtenção da vantagem indevida. Terceira Seção, Brasília, DF, 3 mar. 1994. *Diário da Justiça*, Brasília, DF, 10 mar. 1994, p. 4.021. Disponível em: https://www.stj.jus.br/docs_internet/revista/eletronica/stj-revista-sumulas-2010_7_capSumula96.pdf. Acesso em: 2 jul. 2026.

CABRAL SAISSE, Renan. Ransomware: Sequestro de dados e extorsão digital. *Direito & TI*, [S. l.], v. 1, n. 6, 2016. DOI: 10.63451/ti.v1i6.44. Disponível em: https://direitoeti.com.br/direitoeti/article/view/44. Acesso em: 9 jun. 2026.

CARMO, Marcus Fábio Fontenelle do. Ransomware: uma perspectiva histórica. In: GUEIROS, Guilherme; WENDT, Emerson (org.). *Ransomware 360°: abordagens multidisciplinares da extorsão criptoviral*. São Paulo: Mizuno, 2024.

COELHO, Daniela Caldas Rosa Alves; COELHO, Renato Gustavo Alves. O marco legal do combate ao crime organizado: análise crítica da Lei 15.358/26 (Lei Raul Jungmann). *Migalhas*, 27 abr. 2026. Disponível em: https://www.migalhas.com.br/depeso/454683/o-marco-legal-do-combate-ao-crime-organizado-analise-da-lei-15-358-26. Acesso em: 27 jun. 2026.

CUNHA, Bruno Requião da. Facções criminais: estrutura, energia e neutralização seletiva em sistemas complexos do crime organizado. In: BRASIL. Ministério da Justiça e Segurança

Pública. Secretaria Nacional de Acesso à Justiça. *Criminalidade organizada: diagnóstico e políticas públicas e legislativas*. Brasília: Ministério da Justiça e Segurança Pública, 2026. Disponível em: https://www.gov.br/mj/pt-br/assuntos/noticias/especialistas-apresentam-dez-caminhos-para-enfrentar-o-crime-organizado/PublicacaoCriminalidadeOrganizada_FINAL.pdf. Acesso em: 27 jun. 2026.

ELLOVITCH, Mauro da Fonseca. *Organizações criminosas especializadas em cibercrimes*. Artigo científico. [**No prelo]**.

ELSAD, A. Threat assessment: Black Basta ransomware. *Unit 42 – Palo Alto Networks*, 2022. Disponível em: https://unit42.paloaltonetworks.com/threat-assessment-black-basta-ransomware/. Acesso em: 3 jun. 2026.

FAYET JÚNIOR, Ney; MAYA, André Machado; MARCELLO, Diogo. *Criminalidade organizada*. Porto Alegre: Núria Fabris, 2012.

LOPES JR., Aury. *Fundamentos do processo penal: introdução crítica*. 10. ed. São Paulo: SaraivaJur, 2024.

MARQUES, Vinicius Martins. *O Brasil sob domínio: nova Lei Antifacção*. [S. l.]: [s. n.], 2026. E-book.

MARTINS, Thiago Messias. Ransomware: tipologia do crime organizado cibernético. In: GUEIROS, Guilherme; WENDT, Emerson (org.). *Ransomware 360°: abordagens multidisciplinares da extorsão criptoviral*. São Paulo: Mizuno, 2024.

MASSENO, Manoel Davi. Ataques de ransomware na Convenção de Budapeste sobre o crime cibernético: um ensaio de qualificação alternativa. In: GUEIROS, Guilherme; WENDT, Emerson (org.). *Ransomware 360°: abordagens multidisciplinares da extorsão criptoviral*. São Paulo: Mizuno, 2024.

MASSON, Cleber. *Código penal comentado*. 2. ed. São Paulo: Método, 2018.

NAGAR, Gourav. The evolution of ransomware: tactics, techniques, and mitigation strategies. *SSRN Electronic Journal*, 2024. Disponível em: https://ssrn.com/abstract=4881213. Acesso em: 3 jun. 2026.

NAKAMOTO, Satoshi. *Bitcoin: A Peer-to-Peer Electronic Cash System*. 2008. Disponível em: https://bitcoin.org/files/bitcoin-paper/bitcoin_pt_br.pdf. Acesso em: 3 jun. 2026.

NUCCI, Guilherme de Souza. *Código penal comentado*. 2. ed. São Paulo: Revista dos Tribunais, 2002.

NUCCI, Guilherme de Souza. *Organização criminosa*. 5. ed. Rio de Janeiro: Forense, 2021.

NURSE, Jason R. C.; BADA, Maria. The group element of cybercrime: types, dynamics, and criminal operations. In: ATTRILL-SMITH, Alison; FULLWOOD, Chris; KEEP, Melanie; KUSS, Daria J. (ed.). *The Oxford handbook of cyberpsychology*. Oxford: Oxford University

Press, 2019. cap. 34. DOI: 10.1093/oxfordhb/9780198812746.013.36. Disponível em: https://doi.org/10.1093/oxfordhb/9780198812746.013.36. Acesso em: 12 jun. 2026.

PAULINO, Galtiênio da Cruz. Lei Antifacção e a fragmentação do conceito de organização criminosa. *JOTA*, 24 abr. 2026. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/lei-antifaccao-e-a-fragmentacao-do-conceito-de-organizacao-criminosa. Acesso em: 29 jun. 2026.

PETRY, Guilherme. TJ-RS é vítima do ransomware REvil. *The Hack*, 2021. Disponível em: https://thehack.com.br/tj-rs-e-vitima-do-ransomware-revil-gangue-pede-u-5-milhoes-pelo-resgate/. Acesso em: 9 jun. 2026.

SYDOW, Spencer Toth. *Curso de direito penal informático: partes geral e especial*. Salvador: JusPodivm, 2021.

TRELEAVEN, Philip et al. The future of cybercrime: AI and emerging technologies are creating a cybercrime tsunami. *SSRN Electronic Journal*, 2023. DOI: 10.2139/ssrn.4507244. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4507244. Acesso em: 9 jun. 2026.

WENDT, Emerson. Que expectativas de estruturação normativo-penal sobre o ransomware no Brasil? In: GUEIROS, Guilherme; WENDT, Emerson (org.). *Ransomware 360°: abordagens multidisciplinares da extorsão criptoviral*. São Paulo: Mizuno, 2024.

YAROCHEWSKY, Leonardo Isaac. Breves considerações sobre a Lei Antifacção. *Jornal de Ciências Criminais do IBCCRIM*, 30 mar. 2026. Disponível em: https://jcc.ibccrim.org.br/colunistas/breves-consideracoes-sobre-a-lei-antifaccao/. Acesso em: 27 jun. 2026.

ZUCCA, Maria Vittoria. Mappare il Crime-as-a-Service: analisi delle strutture, dei ruoli e dei servizi nell'offerta criminale digitale. *Rivista italiana di informatica e diritto*, v. 7, n. 2, 2025. DOI: 10.32091/RIID0249. Disponível em: https://www.rivistaitalianadiinformaticaediritto.it/index.php/RIID/article/view/358. Acesso em: 3 jun. 2026.