INSTITUTO BRASILEIRO DE ENSINO, DESENVOLVIMENTO E PESQUISA – IDP
PROGRAMA DE PÓS-GRADUAÇÃO *STRICTO SENSU*
MESTRADO PROFISSIONAL EM DIREITO

RANSOMWARE E INFRAESTRUTURAS CRÍTICAS – ANÁLISE SOBRE O VAZIO LEGAL PENAL NO BRASIL A PARTIR DO CASO *COLONIAL PIPELINE*

Ana Manuela Oliveira Nepomuceno
Orientador: Prof. Dr. Vladimir Barros Aras

Brasília – DF
2025

ANA MANUELA OLIVEIRA NEPOMUCENO

RANSOMWARE E INFRAESTRUTURAS CRÍTICAS – ANÁLISE SOBRE O VAZIO LEGAL PENAL NO BRASIL A PARTIR DO CASO *COLONIAL PIPELINE*

Dissertação de Mestrado desenvolvida no Programa de Mestrado Profissional em Direito, sob a orientação do professor apresentado para obtenção do Título de Mestre pelo Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa – IDP.

Orientador: Prof. Dr. Vladimir Barros Aras

Brasília – DF

2025

Código de catalogação na publicação – CIP

N441r Nepomuceno, Ana Manuela Oliveira

Ransomware e infraestrutura críticas: análise sobre o vazio legal penal no Brasil a partir do caso Colonial Pipeline / Ana Manuela Oliveira Nepomuceno. — Brasília: Instituto Brasileiro Ensino, Desenvolvimento e Pesquisa, 2025.

102 f.: il.

Orientador: Prof. Dr. Vladimir Barros Aras

Dissertação (Mestrado Profissional em Direito) - Instituto Brasileiro Ensino, Desenvolvimento e Pesquisa – IDP, 2025.

1. Direito penal. 2. Análise crítica. 3. Estudo de caso. 4. Crimes cibernéticos. I. Título

CDD 340

Elaborada por Biblioteca Ministro Moreira Alves

ANA MANUELA OLIVEIRA NEPOMUCENO

RANSOMWARE E INFRAESTRUTURAS CRÍTICAS – ANÁLISE SOBRE O VAZIO LEGAL PENAL NO BRASIL A PARTIR DO CASO *COLONIAL PIPELINE*

Dissertação de Mestrado desenvolvida no Programa de Mestrado Profissional em Direito, sob a orientação do professor apresentado para obtenção do Título de Mestre pelo Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa – IDP.

Orientador: Prof. Dr. Vladimir Barros Aras

Brasília, 19 de dezembro de 2025.

BANCA EXAMINADORA

Prof. Dr. Vladimir Barros Aras
Orientador

Prof. Dra. Marília Araújo Fontenele de Carvalho
Examinadora

Prof. Dr. Bruno Freire de Carvalho Calabrich
Examinador

AGRADECIMENTOS

Primeiramente, a Deus, força esta com a qual tenho me conectado cada vez mais, em busca de clareza e paz espiritual. Os caminhos que foram abertos não foram mero acaso.

Aos meus pais, que nunca mediram esforços na construção de quem sou hoje. Não só agradeço, como dedico este trabalho a eles, que sempre acreditaram na minha capacidade e me motivaram a sonhar alto. Se essa produção acadêmica existe, é porque desde a infância plantaram em mim a disciplina e o anseio por conhecimento.

À minha família, forte e determinada, que com raízes maranhenses muito bem fincadas, me ensinou o que é ter sempre para onde voltar. Cada integrante da família Nepomuceno semou, em mim, a vontade de fazer alguma diferença no mundo.

Aos meus amigos e ao meu amor, família que é escolhida por nós ao longo da vida. Sem o apoio e escuta ativa de vocês eu não teria concluído nem metade dessa árdua etapa. Poder compartilhar medos e glórias, fez com que eu me sentisse acolhida e amada.

Ao meu orientador, Vladimir Aras, e demais professores, meu especial agradecimento pela imensa paciência. Até o momento, uma das jornadas mais difíceis que já enfrentei, mas a confiança e suporte de vocês me deu segurança para lutar até o fim.

Obrigada!

RESUMO

O presente trabalho acadêmico analisa os ataques cibernéticos de *ransomware* sob a perspectiva do Direito Penal Brasileiro, a partir do caso *Colonial Pipeline*, ocorrido nos Estados Unidos em 2021, considerado um dos mais emblemáticos episódios de comprometimento de infraestrutura crítica por meio de invasão cibernética. O trabalho parte da constatação de que a crescente informatização das relações sociais, econômicas e estatais expôs infraestruturas basilares da sociedade a riscos sistêmicos inéditos, para os quais o ordenamento jurídico nacional ainda não apresenta resposta penal satisfatória. Para melhor compreensão, examina-se a dinâmica técnica do *ransomware*, sua arquitetura operacional e os impactos concretos criados sobre cadeias gerais de suprimento, segurança nacional e estabilidade econômica. Aprofunda-se também no marco jurídico internacional sobre cibercriminalidade, com destaque para a Convenção de Budapeste, recentemente incorporada ao ordenamento brasileiro. No plano interno, investiga-se a legislação vigente sobre internet e a própria norma penal já posta, demonstrando-se a fragmentação normativa e a insuficiência das figuras típicas atuais para abranger o desvalor global do ataque de *ransomware*. O estudo também enfrenta os desafios processuais centralizados nos aspectos probatórios relacionados à prova digital, à cadeia de custódia e à cooperação jurídica internacional, a fim de demonstrar que as consequências da carência legislativa ultrapassam o aspecto material da norma. Ao final, propõe-se a criação de um tipo penal autônomo específico (artigo 154-B) para o ataque de *ransomware* contra infraestruturas críticas, fundamentado na tutela de bens jurídicos sistêmicos, na política criminal contemporânea e nos compromissos internacionais assumidos pelo Brasil. Conclui-se que a ausência de tipificação própria compromete a prevenção, a repressão eficaz e a cooperação internacional, revelando a necessidade urgente de adequação legislativa ao enfrentamento da macrocriminalidade digital no país.

Palavras-chave: crimes cibernéticos; ataque de *ransomware*; infraestruturas críticas; legislação insuficiente; novo tipo penal.

ABSTRACT

This dissertation analyzes ransomware cyberattacks from the perspective of Brazilian Criminal Law, based on Colonial Pipeline case, which occurred in the United States in 2021 and is considered one of the most emblematic episodes of critical infrastructure compromise through cyberattacks. The work begins with the observation that the increasing computerization of social, economic, and state relations has exposed fundamental societal infrastructures to unprecedented systemic risks, for which the national legal system does not yet offer a satisfactory penal response. For better understanding, the technical dynamics of ransomware, its operational architecture, and the concrete impacts generated on general supply chains, national security, and economic stability are examined. Following this, the international legal framework on cybercrime is explored in depth, with emphasis on the Budapest Convention, recently incorporated into the Brazilian legal system. Domestically, the current legislation on the internet and the existing penal norms are investigated, demonstrating the normative fragmentation and the insufficiency of current typical figures to encompass the global harm of ransomware attacks. The study also addresses procedural challenges centered on evidentiary aspects related to digital evidence, chain of custody, and international legal cooperation, in order to demonstrate that the consequences of the legislative gap go beyond the material aspect of the law. Finally, it proposes the creation of a specific autonomous criminal offense (article 154-B) for ransomware attacks against critical infrastructure, based on the protection of systemic legal assets, contemporary criminal policy, and international commitments undertaken by Brazil. It concludes that the absence of a specific criminal offense compromises prevention, effective repression, and international cooperation, revealing the urgent need for legislative adaptation to address digital macro-criminality in the country.

Keywords: Cybercrimes; ransomware attacks; critical infrastructure; insufficient legislation; new criminal offense.

LISTA DE ABREVIATURAS E SIGLAS

ABNT – Associação Brasileira de Normas Técnicas

CD/DVD – Compact Disc / Digital Versatile Disc

CEO – Chief Executive Officer (Diretor-Executivo)

CFAA – Computer Fraud and Abuse Act

CIRCIA – Critical Infrastructure Act

CISA – Cybersecurity and Infrastructure Security Agency

CPP – Código de Processo Penal

CRI – Counter Ransomware Initiative

DHS – Department of Homeland Security

DRCI – Departamento de Recuperação de Ativos e Cooperação Jurídica Internacional

E-CIBER – Estratégia Nacional de Segurança Cibernética

END – Estratégia Nacional de Defesa

ENSIC – Estratégia Nacional de Segurança de Infraestruturas Críticas

FBI – Federal Bureau of Investigation

FISMA – Federal Information Security Modernization Act

FTK – Forensic Toolkit

GSI – Glossário de Segurança da Informação

HD – Hard Drive

IC – Instituto de Criminalística

IEC – International Electrotechnical Commission (Comissão Eletrotécnica Internacional)

ISO – International Organization for Standardization (Organização Internacional de Padronização)

ISO/IEC 27037 – Norma internacional de evidências digitais

LGPD – Lei Geral de Proteção de Dados

NICE – National Initiative for Cybersecurity Education

NSA – National Security Agency

OFAC – Office of Foreign Assets Control

OT – Tecnologia Operacional

PIX – Sistema de Pagamentos Instantâneos

PLANGIC – Plano de Gestão de Incidentes Cibernéticos da Administração Federal

PLANSIC – Plano Nacional de Segurança das Infraestruturas Críticas

PND – Política Nacional de Defesa

PNI – Política Nacional de Inteligência

PNSI – Política Nacional de Segurança da Informação

POP – Procedimento Operacional Padrão

PSDB – Partido da Social Democracia Brasileira

RAM – Random Access Memory (Memória volátil)

SENASP – Secretaria Nacional de Segurança Públic

STF – Supremo Tribunal Federal

STJ – Superior Tribunal de Justiça

TSA – Transportation Security Administration

VPN – Rede Privada Virtual

SUMÁRIO

INTRODUÇÃO

O advento da internet trouxe à população mundial a possibilidade de acesso ao conhecimento, praticamente em tempo real de acontecimentos ocorridos por todo o mundo – a famosa globalização.

Com extrema velocidade no fluxo da informação, a rede garante acesso rápido e quase que imediato, possibilitando a conexão instantânea e interatividade constante entre os usuários, e até mesmo não usuários.

Como afirma Klaus Martin Schwab[1], a sociedade se encontra na abertura de uma chamada quarta revolução industrial. Seu início, para o autor, deu-se na virada do século e baseia-se na revolução digital, sendo caracterizada por uma internet mais ubíqua e móvel, por sensores menores e mais poderosos, que se tornaram mais baratos, e, principalmente, pela inteligência artificial e aprendizagem automática.

Esse novo paradigma é também chamado de Indústria 4.0, termo justificado pelo nível de revolução que encara a organização das cadeias globais de valor. A rapidez dos avanços que estão ocorrendo não tem precedentes na história e interfere em quase todos os setores de todos os países[2].

Sabe-se, porém, que a evolução tecnológica também tem seus ônus, como por exemplo, a disponibilidade de novos mecanismos para o cometimento de crimes. Com esse quadro de popularização da informática, grande parte dos crimes conhecidos pelas legislações mundiais migraram para o mundo digital.

Na dinâmica de delitos praticados pelo computador ou com o auxílio deste, diferencia-se as infrações cibernéticas **próprias** (em que os terminais, arquivos, banco de dados e dispositivos informáticos em geral são atacados pelos criminosos, com o objetivo de causar danos diversos), dos delitos cibernéticos **impróprios** (quando o agente infrator se utiliza, para a prática/consumação de um determinado crime, de algum dispositivo informático)[3].

Dessa forma, um computador pode ser objeto (crime próprio) ou meio (crime impróprio) de um delito cibernético.

---

[1] SCHWAB, Klaus. **A quarta revolução industrial**. Tradução de Daniel Moreira Miranda. São Paulo: Edipro, 2016.
SCHWAB, Klaus; DAVIS, Nicholas. **Aplicando a Quarta Revolução Industrial**. Tradução de Daniel Moreira Miranda. São Paulo: Edipro, 2018.
[2]AFFONSO, Annibal. **Você está preparado para a quarta revolução industrial**. Disponível em: https://professorannibal.com.br/2017/05/09/voce-esta-preparado-para-a-quarta-revolucao-industrial/.
[3] OLIVEIRA, Anderson Soares Furtado. **Crime por Meios Eletrônicos**. Brasília: Universidade Gama Filho, 2009.

No presente trabalho acadêmico, tratar-se-á dos crimes próprios, especificamente os ataques cibernéticos de *ransomware*, modalidade em que a rede mundial de computadores se torna o alvo da conduta criminosa, demandando proteção ativa do Estado, partindo da premissa de que há, atualmente, a ausência de um sistema de normas desenhado objetivamente para esse tipo de transgressão.[4]

A escolha por falar dos crimes cometidos contra a própria rede mundial de computadores se justifica pelo aumento drástico de casos dessa natureza por todo o mundo, pelos impactos catastróficos de um delito bem sucedido, mas, principalmente, pela possibilidade, ainda existente, de enquadramento das condutas impróprias nos tipos penais já fixados no Código Penal Brasileiro, ao passo que quando a conduta é perpetrada com o fim de violar os dispositivos cibernéticos em si, não há norma específica que proteja esse bem, sendo, eventualmente, apreciado por analogias e inovações jurisprudenciais.

O que se tem é um desafio comum aos crimes dessa seara, qual seja, encontrar rastros eventualmente deixados pelo executor em um dispositivo informático repleto de dados diversos, inclusive falsos ou adulterados, que permita não só a percepção da conduta, a proteção do sistema, a identificação do agente e a sua correta e suficiente responsabilização, mas também a criação de mecanismos eficientes de proteção e contenção de danos.

Não menos importante também é a necessidade de se resguardar dados de terceiros, pessoas físicas, jurídicas ou até do próprio governo, que acabam por serem atingidos durante a prática criminosa, quando não são o verdadeiro alvo por trás do ataque.

Nos crimes impróprios, seria como dizer que um indivíduo que se utiliza da internet para invadir um banco de dados de um hospital e alterar os prontuários para um homicídio em massa, bem ou mal, poderia ser condenado pelo já existente artigo 121 (homicídio) do Código Penal[5], a despeito dos métodos inovadores utilizados. Há uma norma posta que criminaliza a conduta de "matar alguém", ainda que o agente se utilize de instrumentos desconhecidos pela lei.

Em contrapartida, quando se fala de invasão de banco de dados de uma infraestrutura crítica de um país com pedido de resgate, por exemplo, somos obrigados a encarar a dúvida crucial sobre a pluralidade de possibilidades de enquadramento do indivíduo (ou o grupo), vide

[4] A definição de crimes próprios e impróprios utilizada na presente produção acadêmica não se confunde com à classificação pertinente ao Código Penal Brasileiro, mas sim à divisão específica dos crimes cibernéticos estabelecida na doutrina.

[5] Art. 121. Matar alguém:
Pena - reclusão, de seis a vinte anos.

os tipos penais como os dos artigos 148[6] (sequestro), 159[7] (extorsão mediante sequestro) ou, ainda, 171[8] (estelionato) do mesmo diploma legal, os quais parecem se amoldar à conduta.

Apesar de parecer compatível sob o aspecto teórico, o bem jurídico tutelado pelo legislador nos dispositivos mencionados não se trata de sistemas informatizados ou de bancos de dados, ainda que, indiretamente, a vida, integridade física ou patrimônio de milhares de indivíduos estejam sendo violados.

Eis que surge o questionamento sobre qual crime tipificado pela lei penal realmente fora praticado e quem será o culpado.

Retrato da nebulosidade do tema é que, se a análise for mais profunda, há de se convir que não é possível identificar de maneira prática qual o verdadeiro bem jurídico a ser protegido pela norma. Na hipótese de um ataque a uma infraestrutura crítica – conceito que será explorado no segundo capítulo – está-se diante de um sequestro de banco de dados, extorsão para devolução, paralisação de um sistema basilar da sociedade e danos de natureza social, econômica, política e de segurança nacional.

Isto é, um único ato criminoso acarreta consequências capazes de violar diversos bens jurídicos simultaneamente.

Qual tipo penal protegeria todos os bens violados por um ataque cibernético criminoso? Na hipótese, seria necessária a invocação de leis penais, cíveis, econômicas, constitucionais e até de segurança nacional.

O debate está exatamente nesse tipo de entrave, que não está mais no plano futuro, mas sim no presente da sociedade brasileira.

Em palavras transparentes, a cada dia que passa as pessoas se enclausuram mais em casa e se valem da realidade virtual para trabalharem, se divertirem, socializarem, efetuarem negócios jurídicos como compras e vendas, acordos, investimentos e relacionamentos. Da mesma forma, agem as empresas e os órgãos estatais, os quais centralizam as suas atividades em sistemas informatizados capazes de amplificar a escala, celeridade e eficiência dos serviços prestados.

---

[6] Art. 148 - Privar alguém de sua liberdade, mediante sequestro ou cárcere privado:
Pena - reclusão, de um a três anos.

[7] Art. 159 - Sequestrar pessoa com o fim de obter, para si ou para outrem, qualquer vantagem, como condição ou preço do resgate:
Pena - reclusão, de oito a quinze anos.

[8] Art. 171 - Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento:
Pena - reclusão, de um a cinco anos, e multa, de quinhentos mil réis a dez contos de réis.

Em contrapartida, também utilizam a rede aqueles voltados ao ilícito, vide o que se vê em termos de *DeepWeb, Dark Web, Hackers, Malware* e proliferação de *Fake News*.

Naturalmente, a inquietude que surge na comunidade jurídica é de que maneira o Estado poderá se adaptar e se proteger de algo que não se domina e não se prevê, respeitando princípios constitucionais e se adaptando aos chamados "novos direitos"[9], quais sejam, direito à privacidade, à proteção de dados, ao acesso à informação e liberdade, não só de expressão[10], mantendo intacta, todavia, a efetividade e os ditames do procedimento penal estipulado em lei.

O enfoque do presente trabalho é analisar e responder se há, ou não, um real problema, a ser enfrentado pelo Estado, na falta de um enquadramento concreto do ataque cibernético de *ransomware*, considerando que hoje se vive a ausência de uma legislação prévia que comporte as condutas cibernéticas e norteie a sua investigação penal, avaliando quais os desafios atualmente encarados com a ausência do desenvolvimento dessa legislação e na adaptação à nova realidade.

Discutir o desenvolvimento de leis específicas para o ataque de *ransomware* não constitui apenas um exercício técnico de atualização legislativa, mas uma necessidade social, política e econômica inadiável em uma sociedade cuja infraestrutura passou a depender estruturalmente de sistemas digitais.

No plano social, a paralisação de hospitais, serviços públicos, sistemas de transporte, comunicação e abastecimento revela que os efeitos desse crime ultrapassam a esfera patrimonial e atingem diretamente a dignidade, a segurança e a própria continuidade da vida coletiva.

No plano político, a vulnerabilidade de infraestruturas críticas compromete a soberania estatal, expõe fragilidades institucionais e amplia a dependência externa em matéria de resposta a incidentes cibernéticos, deslocando o centro decisório para arenas transnacionais.

Já no plano econômico, os prejuízos derivados de ataques de *ransomware* atingem cadeias produtivas inteiras, desestabilizam mercados, afetam a confiança no ambiente digital e impõem custos sistêmicos que recaem não apenas sobre empresas, mas sobre o próprio Estado e a sociedade como um todo.

Neste ponto, importante lembrar a versatilidade de um ataque cibernético, na medida em que pode ser empregado desde fins comerciais a guerras, representando artefato com escala que, a depender de como é utilizado, pode vir a superar a potência bélica.

---

[9] BARBOSA, André. **Constitucionalismo digital e a Lei Geral de Proteção de Dados Pessoais**. Revista Jus Navigandi, Teresina, ano 23, n. 5515, 19 atrás. 2018.

[10]MENDES, Gilmar Ferreira; FERNANDES, Victor Oliveira. **Constitucionalismo digital e jurisdição constitucional: uma agenda de pesquisa para o caso brasileiro.** Revista Brasileira de Direito, Passo Fundo, v. 16, n. 1, p. 1-33, jan./abr. 2020.

Para tanto, partir-se-á de caso modelo: o ataque cibernético sofrido, em 2021, pelo sistema de oleodutos dos Estados Unidos, *Colonial Pipelin*e, oportunidade em que uma das maiores infraestruturas críticas americanas foi invadida por um grupo cibercriminoso, que ocasionou consequências drásticas à distribuição de combustível por todo o país e demais nações dependentes, acarretando prejuízos em todas os setores de insumos e energia não só da potência norte-americana, como do mundo.

O intuito é verificar, sob um aspecto penal e processual penal, como o Brasil se comportaria e se tem condições de lidar com ataques cibernéticos de grande escala (como o caso em comento), se possui mecanismos suficientes de proteção, procedimentos de investigação capazes de identificar os agentes responsáveis e se conta com legislação apta a criminalizá-los de maneira adequada.

A presente dissertação será dividida em quatro capítulos, para além do tópico preambular (Introdução) e Conclusão.

No Capítulo 1, será apresentado o caso *Colonial Pipeline*, que servirá como protótipo para as análises pretendidas. Trabalharemos como se procedera o ataque, quais as suas consequências cíveis e penais, os impactos econômicos e estruturais, bem como o percurso das investigações e a importância da proteção de infraestruturas críticas que sustentam não só um país, mas o mundo.

O recorte programado não contempla a metodologia de estudo de caso propriamente dita, mas a utilização de episódio prático como ponto de partida para a compreensão da discussão proposta e suas repercussões, na medida em que o escopo do trabalho não está nos desdobramentos do ataque americano, mas sim nas possíveis carências legais brasileiras (em diversas searas) que o ocorrido revela.

No Capítulo 2, tratar-se-á, de maneira geral, os conceitos que definem a conduta de *ransomware*, as etapas que compõem a arquitetura deste ataque e o marco jurídico internacional, com fins de examinar as inovações jurídicas da comunidade estrangeira sobre esse tipo de prática e como os países e as organizações têm administrado as necessárias proteções.

No Capítulo 3, partiremos para uma análise sob a perspectiva penal do ataque de *ransomware*, destrinchando as leis vigentes no Brasil que regulamentam a internet como um todo, em busca de compreender a criminalização da conduta na hipótese da ocorrência de um ataque da mesma natureza em infraestruturas críticas brasileiras. O escopo do tópico é estudar quais os mecanismos de proteção já existem, quais os órgãos responsáveis por administrar a intercorrência e que leis norteiam o enquadramento da conduta.

Por derradeiro, no Capítulo 4, será trabalhada a persecução penal do ataque de *ransomware* no Brasil e os desafios enfrentados em razão da ausência de tipificação específica. Utilizando como arranque o caso prático, serão analisados quais os instrumentos existem no Brasil que podem/são utilizados no processamento penal da invasão cibernética. Ainda neste capítulo, ante os obstáculos encarados pela carência de normas, será apresentado o produto da presente dissertação: a proposta de um tipo penal específico que criminaliza o ataque de *ransonware* a infraestruturas críticas brasileiras.

A finalidade desta produção acadêmica é, a partir de um caso real e de proporção mundial, demonstrar o nível de risco que acompanha a globalização e informatização dos sistemas estatais – o que deve ser objeto de debates imediatos –, com fins de preencher lacunas existentes não só no ordenamento jurídico brasileiro, em âmbito penal material, mas também penal processual, revelando a incapacidade que o país ainda possui de impedir um ataque de *ransomware*, de proteger os seus bancos de dados e indivíduos afetados, e, sobretudo, de responsabilizar os agentes criminosos, provocando as entidades a se debruçarem sobre a necessidade de desenvolvimento de novas leis e tecnologias capazes de fortalecer os muros virtuais da nação.

1. O CASO *COLONIAL PIPELINE*

Ao lado de WannaCry[11] e NotPetya[12], o ataque à *Colonial Pipeline Company* é considerado uma das invasões de *ransomware*[13] mais significativas e impactantes da história recente, especialmente devido às suas implicações nas infraestruturas críticas e nas cadeias de suprimento de combustível dos Estados Unidos[14].

A despeito de tantos outros casos importantes que poderiam ser mencionados, inclusive o mais recente contra a Prospect Medical Holdings[15], ocorrido em 2023, o ataque à *Colonial Pipeline* é um exemplo claro de como as invasões de *ransomware* podem não só causar grandes perdas financeiras, mas também afetar a vida cotidiana das pessoas e a segurança nacional de um país. A combinação de cibercriminalidade com infraestruturas críticas trouxe à tona a vulnerabilidade de setores essenciais frente a ameaças cibernéticas sofisticadas.

A *Colonial Pipeline Company*[16] é a maior operadora de oleodutos de combustível dos Estados Unidos e é a responsável por fornecer cerca de 45% (quarenta e cinco por cento) do combustível consumido desde o Golfo do México até a costa leste do país.

A companhia distribui mais de 100 (cem) milhões de galões de gasolina para consumidores por cerca de 14 estados, mantém 28 refinarias, aproximadamente 50 instalações militares e a maioria dos aeroportos[17].

---

[11] Ataque realizado contra o Sistema de Saúde do Reino Unido (NHS) – WannaCry, em maio de 2017. O ataque foi impulsionado por uma vulnerabilidade no sistema operacional Windows, conhecida como **EternalBlue**, que havia sido vazada pela NSA (Agência de Segurança Nacional dos EUA) e era utilizada para explorar sistemas desatualizados. O WannaCry se espalhou rapidamente por redes, criptografando arquivos e bloqueando o acesso aos sistemas. Atingiu empresas, governos e, principalmente, o setor de saúde, incluindo o Sistema Nacional de Saúde do Reino Unido (NHS), que teve muitos de seus serviços interrompidos, incluindo o atendimento em hospitais e clínicas. Acessado em: https://www.cisa.gov/news-events/alerts/2017/05/12/indicators-associated-wannacry-ransomware

[12] Referência de ciberataque com intenção geopolítica ocorrido em 2017, o NotPetya se espalhou rapidamente, afetando empresas globais, causando enormes prejuízos financeiros, especialmente para grandes corporações, como a Maersk e a Merck. Nesse caso, acredita-se que a real intenção era a destruição de dados e não propriamente a vantagem financeira. Acessado em: https://www.cisa.gov/news-events/alerts/2017/07/01/petya-ransomware

[13] Conceito e definições desenvolvidos no Capítulo 2

[14] DUDLEY, Renee; GOLDEN, Daniel. ***The Ransomware Hunting Team: A Band of Misfits' Improbable Crusade to Save the World from Cybercrime.*** New York: Macmillan, 2022.

[15] Ataque contra a rede de hospitais e clínicas dos Estados Unidos Prospect Medical Holdings, que resultou na interrupção de operações em diversos consultórios médicos, instalações e hospitais da rede. A empresa foi forçada a desligar temporariamente algumas de suas instalações ambulatoriais e a adotar procedimentos manuais enquanto a rede estava offline. A interrupção afetou a prestação de serviços médicos essenciais, resultando em atrasos no atendimento aos pacientes e desafios operacionais significativos para a organização. Acessado em: https://www.fiercehealthcare.com/providers/ongoing-cyberattack-prospect-medical-holdings-forces-facilities-offline-disrupts-services

[16] Hobbs, A. (2021). **The Colonial Pipeline Hack: Exposing Vulnerabilities in U.S. Cybersecurity**. Sage Publications. ISBN 978-1529789768

[17]BEERMAN, Jack; BERENT, David; FALTER, Zach; BHUNIA, Suman. **A review of Colonial Pipeline ransomware attack**. In: IEEE/ACM 23rd International Symposium on Cluster, Cloud and Internet Computing Workshops (CCGridW), 2023, Arizona. IEEE, 2023. Disponível

Mas, antes de adentrarmos ao caso em si, faz-se necessário entender melhor os aspectos conceituais de infraestruturas críticas e o que elas verdadeiramente representam.

Segundo as diretrizes da Estratégia Nacional de Defesa (END) e da Política Nacional de Defesa (PND) do Ministério da Defesa do Brasil[18], as infraestruturas críticas nacionais "*são instalações, serviços, bens e sistemas, virtuais ou físicos, que se forem incapacitados, destruídos ou tiverem desempenho extremamente degradado, provocarão sério impacto social, econômico, político, internacional ou à segurança nacional*".

O Decreto nº 9.573, de 22 de novembro de 2018, que aprovou a Política Nacional de Segurança de Infraestruturas Críticas, traz, em seu artigo 1º, as seguintes definições:

> Art. 1º A Política Nacional de Segurança de Infraestruturas Críticas - PNSIC tem por finalidade garantir a segurança e a resiliência das infraestruturas críticas do País e a continuidade da prestação de seus serviços.
> Parágrafo único. Para fins de implementação da PNSIC, considera-se:
> I - infraestruturas críticas - instalações, serviços, bens e sistemas cuja interrupção ou destruição, total ou parcial, provoque sério impacto social, ambiental, econômico, político, internacional ou à segurança do Estado e da sociedade;
> II - segurança de infraestruturas críticas - conjunto de medidas, de caráter preventivo e reativo, destinadas a preservar ou restabelecer a prestação dos serviços relacionados às infraestruturas críticas;
> III - interdependência de infraestruturas críticas - relação de dependência ou interferência de uma infraestrutura crítica em outra ou de uma área prioritária de infraestruturas críticas em outra; e
> IV - resiliência - capacidade de as infraestruturas críticas serem recuperadas após a ocorrência de situação adversa.

O Glossário de Segurança da Informação – GSI, instituído pela Portaria GSI/PR nº 03[19] da Presidência da República, inicialmente incluiu no referido conceito áreas de energia, comunicação, transportes, finanças e água, tendo, posteriormente, expandido para setores de biossegurança, bioproteção e defesa.

No que tange à segurança cibernética de infraestruturas críticas, o campo de maior relevância é a energia, na medida em que é fundamental para a operação e recuperação dos sistemas de informação. Contudo, importa destacar que nem todas as estruturas componentes

---

em:https://www.researchgate.net/profile/Lazarus-Gawazah/publication/383206534_To_Pay_or_Not_to_Pay-_The_US_Colonial_Pipeline_Ransomware_Attack/links/66c1b6bf8d007355925dd805/To-Pay-or-Not-to-Pay-The-US-Colonial-Pipeline-Ransomware-Attack.pdf Acesso em: 28 mar. 2025.

[18] BRASIL. Ministério da Defesa. **Estratégia Nacional de Defesa. Política Nacional de Defesa.** Brasília, DF: MD, 2020. Disponível em: https://www.gov.br/defesa/ptbr/assuntos/copy_of_estado-e-defesa/pnd_end_congresso_.pdf. Acesso em: 10 out. 2023.

[19] **BRASIL.** Presidência da República. **Glossário de Segurança da Informação. Portaria GSI/PR nº 93, de 18 de outubro de 2021.** Dispõe sobre a classificação das infraestruturas críticas nacionais e estabelece diretrizes para sua proteção. *Diário Oficial da União: seção 1*, Brasília, DF, 20 out. 2021. Disponível em: https://www.gov.br/gsi/pt-br/seguranca-da-informacao-e-cibernetica/glossario-de-seguranca-da-informacao-1 Acesso em: 28 mar 2025.

de um determinado setor são, necessariamente, consideradas críticas, ainda que o setor, de forma ampla, sim.[20]

Ou seja, é possível compreender que uma infraestrutura crítica representa um setor de subsistência de determinada comunidade, sem o qual resta prejudicada a manutenção das necessidades básicas dos indivíduos que integram aquele território e, consequentemente, a viabilidade das atividades estatais. Tais infraestruturas podem ser físicas ou virtuais, sendo as últimas as mais vulneráveis às invasões cibernéticas, conceito este que se aplica aos sistemas dos tribunais.

É por esse motivo que uma rede de oleodutos é um alvo robusto para um ataque dessa natureza e que não pode, em nenhuma hipótese, manter um sistema com arestas a serem aparadas. Além de ser uma infraestrutura crítica, é massivamente operado de maneira informatizada.

Consoante os ensinamentos de George Antaki, em sua obra "*Piping and Pipeline Engineering: Design, Construction, Maintenance, Integrity, and Repair*"[21], uma rede de oleodutos é uma infraestrutura de tubulações projetada para o transporte contínuo de produtos líquidos e gasosos (principalmente petróleo, gás natural e produtos refinados) de um ponto a outro, ao longo de grandes distâncias. Essas redes são essenciais para a distribuição de energia e combustíveis, conectando instalações de produção, refinarias, centros de distribuição e mercados de consumo.

Na prática, o principal objetivo de uma rede de oleodutos é transportar petróleo bruto, produtos refinados, como gasolina, diesel e querosene, e gás natural para os centros de consumo. O transporte por oleoduto é muito mais eficiente e econômico em comparação com métodos alternativos, como transporte rodoviário, ferroviário ou marítimo. Sem essas redes, as distâncias longas entre produtores e consumidores seriam muito mais difíceis de cobrir.

A importância dessa distribuição em larga escala está no fato de que setores industriais e comerciais dependem de uma oferta constante de combustíveis e energia para suas operações. Além disso, muitas indústrias petroquímicas dependem diretamente do petróleo e derivados para a fabricação de produtos como plásticos, fertilizantes e até medicamentos.

---

[20]**SOUZA, Carlos Eduardo de Oliveira.** ***A defesa das infraestruturas críticas brasileiras à luz dos normativos e dos objetivos do Exercício Guardião Cibernético: uma análise construtiva.*** 2021. 85 f. Trabalho de Conclusão de Curso (Bacharelado em Ciências Militares) — Escola de Guerra Naval, Rio de Janeiro, 2021. Disponível em: https://www.marinha.mil.br/egn/sites/www.marinha.mil.br.egn/files/TCM%20-%20Carlos%20Eduardo%20de%20Oliveira%20Souza.pdf. Acesso em: 28 mar. 2025.

[21] ANTAKI, G. A. **Piping and Pipeline Engineering: Design, Construction, Maintenance, Integrity, and Repair.** 1. ed. Boca Raton: CRC Press (Taylor & Francis Group), 2003. 564 p. ISBN 978-0824709648

Desse modo, a paralisação dos oleodutos pode causar atrasos na produção de bens e distribuição de mercadorias, impactando a cadeia de suprimentos e o comércio mundial. Além disso, uma interrupção na rede pode aumentar os custos de transporte e, consequentemente, inflacionar os preços para o consumidor final, prejudicando a economia e o poder de compra da população.

Os danos de uma paralisação afetam também os mercados globais, eis que, como muitas dessas redes de oleodutos atravessam fronteiras e conectam diferentes mercados internacionais, a interrupção das operações impactam outros países que dependem da distribuição e geram instabilidade nos preços globais do petróleo. Uma redução na oferta de petróleo ou gás de regiões estratégicas pode elevar os preços globalmente, impactando economias que dependem da importação de energia.

A energia, por sua vez, como pudemos perceber, é o que move o mundo.

A segurança energética de um país está intimamente ligada à estabilidade de suas redes de oleodutos. Quando esses sistemas funcionam bem, o fornecimento de energia é fiável e seguro, o que é crucial para a soberania nacional e a estabilidade política.

Percebe-se que as redes de oleodutos são infraestruturas basilares, motivo pelo qual qualquer interrupção nas operações pode ser vista como um risco à segurança nacional, pois todo país possui dependência do transporte contínuo de energia para o funcionamento de hospitais, instalações militares, empresas, governos inteiros e, consequentemente, a própria rede mundial de computadores.

Por conseguinte, a paralisação de uma rede de oleodutos pode enfraquecer a segurança de um país, tornando-o vulnerável a interrupções externas, representando implicações geopolíticas**,** já que os países podem ser forçados a buscar fontes alternativas de energia ou a envolver-se em negociações diplomáticas em busca de fontes estrangeiras.

De maneira mais realista e palpável. Explica-se.

Interromper o fornecimento de energia de um país – ou para países – significa escassez imediata de combustível. Isso afeta todos que possuem veículos automotores, indústrias que dependem de transporte para operações diárias, a distribuição de alimentos, roupas e utensílios para supermercados e demais estabelecimentos, o transporte de suprimentos médicos como medicamentos e oxigênio para centros de saúde, acarreta restrição do transporte público, aumento dos preços por desregulação do binômio oferta e demanda, paralisação de serviços de emergência como ambulâncias e polícias, além da possibilidade de revolta popular com protestos e saques.

Em suma, a rede de oleodutos é essencial para garantir uma distribuição eficiente de energia e combustível que sustentam toda a economia e a segurança global.

É por esse motivo que esse sistema representa uma infraestrutura crítica de um país e um ataque de *ransomware* pode significar tragédia eventualmente irreparável.

O caso do ataque à *Colonial Pipeline* aconteceu em 07 maio de 2021 e foi realizado pelo grupo *hacker DarkSid*, conhecido por atacar grandes empresas e pedir resgates elevados. O ataque acabou por contrariar todas as simulações já realizadas, durante anos, pela área pública e privada dos Estados Unidos, *demonstrando que a realidade é bem distinta dos "jogos de guerra"*[22] promovidos em treinamentos.

Todas as informações coletadas para esta dissertação foram extraídas dos sítios eletrônicos do FBI (*Federal Bureau of Investigation)*, de renomados jornais e revistas americanas (*New York Times*, *BBC News*, *To Pay* ou *Not To Pay*, *CBS News*, etc...), dos informativos da própria *Colonial Pipeline Company* e de produções acadêmicas específicas sobre o caso.

Segundo o FBI, o grupo conseguiu invadir[23] a rede por intermédio de credenciais de VPN (Rede privada virtual) comprometidas, utilizadas por um empregado da companhia, provavelmente obtidas por meio de um ataque de *phishing* ou reconhecimento de vulnerabilidades em um sistema desatualizado e desprotegido, que permitiu implantar o *ransomware* e criptografar os dados da empresa.

Phishing, por sua vez, é, segundo o Instituto Nacional de Padrões e Tecnologias dos Estados Unidos (*National Institute of Standards and Technology*) "*uma técnica para tentar adquirir dados sensíveis, como números de contas bancárias, dados de login, cartão de crédito e outras credenciais, por meio de uma solicitação fraudulenta por e-mail ou site, em que o autor se faz passar por empresa legítima*".[24]

Isto é, algum dos funcionários da companhia foi "pescado" por intermédio dessa artimanha e acabou por abrir uma porta virtual aos sistemas da empresa, permitindo, ainda que fosse contra a sua vontade (não há indícios de participação), a invasão do grupo criminoso.

---

[22] SANGER, David E.; PERLROTH, Nicole. **Pipeline attack yields urgent lessons about U.S. cybersecurity: the hack underscored how vulnerable government and industry are to even basic assaults on computer networks.** New York Times, New York, 14 May 2021. Disponível em: https://www.nytimes.com/2021/05/14/us/politics/pipelinehack.html. Acesso em: 13 jan 2025.

[23] GAWAZAH, Lazarus; RONDLA, Arjun; BALHARETH, Mohammad Saleh A. **To Pay or Not to Pay: The US Colonial Pipeline Ransomware Attack.** Disponível em: https://www.researchgate.net/publication/383206534_To_Pay_or_Not_to_Pay-_The_US_Colonial_Pipeline_Ransomware_Attack. Acesso em: 28 mar 2025

[24] https://csrc.nist.gov/glossary/term/phishing

Com a entrada, o sistema de faturamento ficou absolutamente comprometido, então a *Colonial Pipeline* foi forçada a fechar toda a sua rede de oleodutos como medida de precaução. O fechamento imediatamente interrompeu o fornecimento de combustível em todo o sudeste dos Estados Unidos.

Nos dias seguintes, a situação se agravou rapidamente – postos de gasolina secaram, companhias aéreas redirecionaram voos e o governo dos EUA declarou emergência regional para manter o combustível fluindo. Como um dos oleodutos mais cruciais do mundo permaneceu *offline*, o ataque expôs vulnerabilidades na infraestrutura de energia envelhecida da América.

Conforme já mencionado, grande parte dos ataques cibernéticos tem início pela exploração de engenharia social, isto é, pela manipulação psicológica do usuário para que ele, inadvertidamente, forneça acesso ou execute ações que comprometam o sistema. Por esse motivo, ambientes excessivamente automatizados tendem a ser mais vulneráveis, pois reduzem a intervenção humana crítica que poderia identificar comportamentos anômalos. Em contrapartida, sistemas informatizados muitas vezes precisam ser complementados por mecanismos físicos de controle e auditabilidade, capazes de registrar e monitorar ações de maneira independente do ambiente digital, aumentando a capacidade de detecção e resposta a incidentes.

O ataque paralisou 5.500 (cinco mil e quinhentas) milhas de oleodutos e levou ao fechamento temporário de terminais de distribuição e estações de bombeamento, o que fez a *Colonial Pipeline* enfrentar dificuldade para retomar as operações ante a escassez de combustível, aumento de preços e quebra da cadeia de suprimentos de energia.[25]

Como será aprofundado no capítulo seguinte, os ataques cibernéticos não são praticados apenas com o intuito de paralisar e inviabilizar sistemas, mas sim, em sua grande maioria, com o objetivo claro de obtenção de vantagens financeiras, as quais, inclusive, poderão ser utilizadas como fonte de investimento para futuros ataques ou, ainda, como financiamento de outros crimes cometidos pelo grupo.

Portanto, após a invasão, no curso da extorsão, o grupo *DarkSide* exigiu um resgate de US$ 4,4 milhões (quatro milhões e quatrocentos mil dólares) em *bitcoin* para liberar o sistema da empresa, valor este que foi de fato pago.

---

[25]COLONIAL PIPELINE COMPANY. **About Us.** ***[S.l.]: Colonial Pipeline***, s.d. Disponível em: https://www.colpipe.com/about-us/. Acesso em: 20 jun. 2025.

O CEO da Companhia, Joseph Blount[26], e sua equipe de liderança enfrentaram uma tomada de decisão agonizante após o ataque: pagar o resgate pleiteado pelo *DarkSide* ou recusá-lo e tentar restaurar os sistemas sem as ferramentas de "descriptografia", que são conhecidas, e só podem ser disponibilizadas, pelos "donos" do ataque.

Em depoimento ao Senado norte-americano[27], segundo informações veiculadas pelos tabloides, Joseph Blount, afirmou que a decisão de pagar o resgate foi tomada diante da incerteza sobre o tempo de restauração dos sistemas, após consultas com especialistas em segurança cibernética e assessores jurídicos, embora soubesse que o FBI, em suas diretrizes gerais, desencoraja o pagamento de resgates. Com o passar das horas, o oleoduto permaneceu fechado e o pânico se intensificou, obrigando a equipe de liderança a, após deliberações, concluir que a opção de menor dano seria arcar com o resgate, obtendo a ferramenta (chave) de "descriptografia" rapidamente e retomando as entregas de combustível para mitigar os crescentes danos econômicos e interrupções[28].

O pagamento de US$ 4,4 (quatro milhões e quatrocentos mil dólares) em *bitcoin* foi feito em 08 de maio, cerca de 24 horas após o ataque inicial.

Em um canal de comunicação seguro com o *DarkSide*, os *hackers* forneceram à *Colonial Company* a chave capaz de desbloquear seus sistemas. Embora as operações tenham sido restauradas em questão de dias, o incidente gerou indignação nacional e perguntas difíceis para os gestores da companhia[29].

De acordo com as informações fornecidas pelo sítio eletrônico oficial do FBI[30], em 07 de junho de 2021, a agência apreendeu com sucesso parte dos lucros criminosos da carteira de *bitcoin*, cerca de US$ 2,3 (dois milhões e trezentos mil dólares), que os agentes do *DarkSide* usaram para coletar o pagamento recebido no ataque.

---

[26]Brewer, R. **Colonial Pipeline CEO defends $4.4 million ransom payment to hackers.** CBS News. https://www.cbsnews.com/news/colonial-pipeline-ceo-defends-ransompayment-to-hackers/.
Gandel, S. **The Colonial pipeline ransomware hackers had a secret weapon: Cyber insurance firms.** CBS News. https://www.cbsnews.com/news/colonial-pipelineransomware-attack-cyber-insurance/.

[27] EATON, Collin; VOLZ, Dustin. **Colonial Pipeline CEO Tells Why He Paid Hackers a $4.4 Million Ransom.** The Wall Street Journal, New York, 19 maio 2021.
BOGAGE, Jacob. **Colonial Pipeline CEO says paying $4.4 million ransom was 'the right thing to do for the country'.** The Washington Post, Washington, 19 maio 2021.
REUTERS. **Colonial Pipeline CEO acknowledges paying hackers to restore pipeline.** 19 maio 2021.

[28] KONRAD, A. **U.S. recovers millions in cryptocurrency paid to Colonial Pipeline ransomware hackers.** CNBC. Disponível em: https://www.cnbc.com/2021/06/07/us-recovers-millions-incryptocurrency-paid-to-colonial-pipeline-ransomware-hackers.html. Acessado em: 28 out 2025.

[29]https://www.fbi.gov/news/press-releases/fbi-deputy-director-paul-abbates-remarks-at-press-conference-regarding-the-ransomware-attack-on-colonial-pipeline

[30]https://www.fbi.gov/news/press-releases/fbi-deputy-director-paul-abbates-remarks-at-press-conference-regarding-the-ransomware-attack-on-colonial-pipeline

A variante do *ransomware DarkSide* é uma das mais de 100 variantes de *ransomware* que o FBI já estava investigando desde o ano de 2020, sendo que os seus desenvolvedores comercializam os *malwares* para afiliados criminosos, que então conduzem ataques e compartilham uma porcentagem dos lucros com os criadores desses programas.

No caso da *Colonial Pipeline*, o FBI identificou mais de 90 (noventa) vítimas em vários setores de infraestrutura crítica dos Estados Unidos, incluindo o setor de manufatura, jurídico, seguros, assistência médica e energia.

Ao perseguir os rastros do valor pago, com base na investigação desenvolvida, o FBI localizou a carteira de moeda virtual que os agentes do *DarkSide* usaram para coletar o pagamento e, assim, as verbas das vítimas foram apreendidas, impedindo que os integrantes do grupo criminoso as usassem.

Para tanto, declarou a agência de investigação que foi necessária a atuação do departamento em conjunto com parceiros da indústria privada e também de outras entidades governamentais para que fosse possível expor e combater a ferramenta cibernética de *ransomware*.

Os Estados Unidos já possuíam tecnologias desenvolvidas em prol da remoção de *backdoors*[31] maliciosos que eventualmente são instalados nas redes de clientes da *Microsoft*, contudo, no âmbito do caso da *Colonial Pipeline*, a riqueza das investigações e dos instrumentos utilizados para repreender a conduta e reaver os valores obtidos ensejou um aprimoramento americano, sobretudo ao se considerar que a reestruturação de um setor basilar para a subsistência mundial dependia da atuação rápida e eficaz dos órgãos responsáveis.

Houve operações prévias – *Gameover Zeus* (2014)[32], *Avalanche* (2016)[33] e *Kelihos* (2017)[34] – que já demonstravam que havia, desde pelo menos 2014, um modelo técnico maduro de desarticulação de *botnets*, baseado em cooperação internacional para apreensão coordenada de infraestrutura criminosa. No entanto, foi somente após o ataque à Colonial Pipeline, em 2021, que esse conhecimento acumulado ganhou centralidade política e estratégica no enfrentamento do *ransomware*.

---

[31] Backdoor é um método de contornar os mecanismos de autenticação de um sistema computacional, permitindo que um atacante (ou o próprio desenvolvedor) acesse remotamente o sistema sem ser detectado. (STALLINGS, William. *Criptografia e Segurança de Redes*, 6ª ed. Pearson, 2018)

[32] https://www.justice.gov/archives/opa/pr/us-leads-multi-national-action-against-gameover-zeus-botnet-and-cryptolocker-ransomware#:~:text=The%20Justice%20Department%20today%20announced%20a%20multi-national%20effort,Omaha%2C%20Nebraska%2C%20against%20an%20administrator%20of%20the%20botnet.

[33] https://www.europol.europa.eu/media-press/newsroom/news/%e2%80%98avalanche%e2%80%99-network-dismantled-in-international-cyber-operation#:~:text=On%2030%20November%202016%2C%20after%20more%20than%20four,an%20international%20criminal%20infrastructure%20platform%20known%20as%20%E2%80%98Avalanche%E2%80%99.

[34] https://www.justice.gov/archives/opa/pr/justice-department-announces-actions-dismantle-kelihos-botnet-0

O incidente, que afetou diretamente a maior rede de oleodutos dos Estados Unidos, revelou a dependência crítica de setores essenciais e expôs o potencial de colapso nacional decorrente de ataques cibernéticos. A partir dele, a resposta governamental passou a integrar, de forma sistemática, não apenas técnicas já consolidadas de desmantelamento de *botnets*, mas também uma política pública mais agressiva de coordenação interagências, priorização de rastreamento financeiro, cooperação internacional estruturada e tratamento do *ransomware* como ameaça estratégica à segurança nacional.[35]

Assim, o caso *Colonial Pipeline* não criou novas técnicas operacionais, mas funcionou como um catalisador institucional, elevando o padrão de resposta estatal e abrindo caminho para operações mais amplas e articuladas – como a disrupção do *Qakbot* em 2023[36], em um ambiente em que o combate ao *ransomware* passou a ser prioridade global.[37]

Retrato da união de esforços foi o desenvolvimento da *National Cyber Investigative Joint Task Force*, uma força-tarefa que reúne a comunidade de inteligência e agências de segurança cibernética para uma abordagem de todo o governo contra essas ameaças.

A estrutura[38] foi criada para elevar a investigação cibernética dos Estados Unidos e é formada por várias agências governamentais, com o objetivo de combater ameaças cibernéticas contra os EUA e proteger infraestruturas críticas. Ela foi desenvolvida em 2008, sendo liderada pelo FBI e contando com a colaboração de mais de 30 (trinta) parceiros federais, incluindo organizações de inteligência e segurança nacional.

Esse setor de investigação é responsável por centralizar, coordenar e integrar os esforços de diferentes agências, como FBI[39], NSA (National Security Agency), CISA (Cybersecurity and Infrastructure Security Agency), DHS (Departamento of Homeland Security)[40] e *Secret Service*, para identificar e investigar a ameaça cibernética maliciosa que possa representar riscos à sociedade, economia e segurança nacional do país, compartilhando as informações e inteligência em tempo real para combater as invasões.

---

[35] LUBIN, Asaf. Cyber Plungers: **Colonial Pipeline and the Case for an Omnibus Cybersecurity Legislation.** Georgia Law Review, v. 57, p. 1605-1674, 2023. Disponível em: https://www.repository.law.indiana.edu/facpub/3082/Acesso em: 12 nov. 2025.

[36]https://www.justice.gov/usao-cdca/pr/qakbot-malware-disrupted-international-cyber-takedown#:~:text=LOS%20ANGELES%20%E2%80%93%20The%20Justice%20Department%20today%20announced,known%20as%20Qakbot%20and%20take%20down%20its%20infrastructure.

[37] BELLAMKONDA, Srikanth. ***Ransomware Attacks on Critical Infrastructure: A Study of the Colonial Pipeline Incident.*** International Journal of Research in Computer Applications and Information Technology, v. 7, n. 2, p. 1423-1433, 2024. Disponível em: https://iaeme.com/MasterAdmin/Journal_uploads/IJRCAIT/VOLUME_7_ISSUE_2/IJRCAIT_07_02_110.pdf. Acesso em: 12 nov. 2025.

[38] https://www.fbi.gov/investigate/cyber/national-cyber-investigative-joint-task-force

[39] https://www.infragard.org

[40] https://www.dhs.gov/topic/cybersecurity

A dinâmica da força-tarefa se mostra bastante interessante, na medida em que as agências envolvidas possuem aptidões específicas e funções definidas em prol da rápida resposta aos ataques, identificação dos envolvidos, rastreio do dinheiro e recuperação dos dados.

Por exemplo, enquanto o FBI lidera a atuação, a NSA é responsável por fornecer a inteligência e o suporte técnico para a viabilização dos trabalhos (programas de computador e instrumentos cibernéticos capazes de permitir que os agentes ingressem nas máquinas atacadas, disputem o domínio com o *malware* criminoso e proteja os dados). Por outro lado, a CISA se empenha na proteção das infraestruturas críticas, enquanto o DHS trabalha na garantia da segurança nacional.

O serviço secreto e outras agências de aplicação da lei auxiliam na identificação e prisão dos criminosos envolvidos.

Por intermédio dessa cadeia de trabalho, o estado americano conseguiu, no ataque à *Colonial Pipeline*, privar o grupo cibercriminoso do objeto de sua atividade – seus rendimentos financeiros e financiamento para a manutenção de outros ataques. Para criminosos cibernéticos motivados pela captação de proveitos econômicos fáceis, especialmente aqueles localizados no exterior, o corte do acesso à receita é uma das consequências mais eficazes que podem ser impostas.

No mínimo, podemos perceber que a atuação exitosa dos Estados Unidos diante do caso apresentado se deve à infinidade de projetos e programas desenvolvidos para a capacitação de agentes na proteção contra ataques cibernéticos.

Como exemplo, a própria CISA[41] oferece treinamentos, recursos e orientações técnicas para os profissionais de cibersegurança, desenvolvendo exercícios simulados de ataques que preparam os seus agentes para cenários realistas.

A NICE (*National Initiative for Cybersecurity Education)*[42], por sua vez, é um programa do já mencionado Instituto Nacional de Padrões e Tecnologias que representa uma força de trabalho qualificada para a área de segurança virtual, mantendo parcerias com universidades e empresas.

Além disso, há o *CyberCorps*[43], que é um programa para financiar estudantes em troca de serviços no governo federal, estadual e local, em busca da qualificação de profissionais desde o início de suas carreiras.

---

[41] https://www.cisa.gov/
[42] https://www.nist.gov/itl/applied-cybersecurity/nice
[43] https://sfs.opm.gov/

Para o governo americano, a cibersegurança é uma prioridade nacional.

Embora episódios anteriores já demonstrassem a relevância crescente do *ransomware*, foi a paralisação temporária do maior oleoduto do país que expôs, de modo incontornável, a fragilidade das infraestruturas críticas norte-americanas e os riscos sistêmicos associados aos ataques cibernéticos. A partir desse incidente, observou-se uma reorientação profunda da postura estatal, marcada pela adoção de novas diretrizes regulatórias, reformas legislativas, integração interagências e fortalecimento da cooperação internacional.

A primeira resposta imediata após o caso veio da *Transportation Security Administration* (TSA)[44], que, pela primeira vez, emitiu diretivas obrigatórias de cibersegurança para operadores de dutos, impondo a designação de coordenadores de segurança cibernética disponíveis 24 horas, a notificação compulsória de incidentes relevantes à CISA, a realização de auditorias e a adoção de planos formais de resposta a ocorrências. Tais medidas romperam com a lógica anterior, eminentemente voluntária, para inaugurar um regime regulatório impositivo na proteção de infraestrutura energética.

No plano legislativo, o ataque impulsionou a aprovação da *Cyber Incident Reporting* for *Critical Infrastructure Act* (CIRCIA)[45], em 2022, que estabeleceu obrigações federais de comunicação de incidentes de segurança cibernética no prazo de 72 horas e de pagamentos de resgate em 24 horas para entidades de infraestrutura crítica. Tal legislação fortaleceu a capacidade federal de supervisão, ampliou a transparência do setor privado e permitiu respostas mais coordenadas e tempestivas.

Outra consequência direta foi a edição da *Executive Order 14028 – Improving the Nation's Cybersecurity*[46], promulgada pelo Presidente Joe Biden poucos dias após o ataque. A ordem executiva determinou a criação do *Cyber Safety Review Board*[47], estabeleceu padrões de segurança para *softwares* utilizados pelo governo federal e ampliou programas de compartilhamento de informações entre o setor público e o setor privado. O ataque levou o

---

[44] **UNITED STATES. Transportation Security Administration.** *Security Directive Pipeline-2021-01 (SD-01) and Pipeline-2021-02 (SD-02): Enhancing Pipeline Cybersecurity Requirements*. Washington, D.C., 2021. Disponível em: https://www.tsa.gov. Acesso em: 12 nov. 2025.

[45] **UNITED STATES. Congress.** *Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA)*. Washington, D.C., 2022. Disponível em: https://www.congress.gov/bill/117th-congress/senate-bill/3600. Acesso em: 12 nov. 2025.

[46] **UNITED STATES. The White House.** *Executive Order 14028: Improving the Nation's Cybersecurity*. Washington, D.C., 12 may 2021. Disponível em: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/. Acesso em: 12 nov. 2025.

[47] UNITED STATES. Department of Homeland Security; Cybersecurity and Infrastructure Security Agency. **Cyber Safety Review Board FAQs**. January 24 2024. Disponível em: https://www.cisa.gov/sites/default/files/2024-01/CSRB%20FAQs%202024.01.24_508c.pdf. Acesso em: 18 nov. 2025.

governo a adotar uma abordagem abrangente e transversal para tratar o *ransomware* como ameaça.

A consolidação do modelo de coordenação interagências permitiu o avanço de iniciativas como a *Counter Ransomware Initiative* (CRI)[48], que reúne diversos países em um esforço internacional de combate ao *ransomware*, e ampliou o padrão de governança cibernética global.

O Brasil inclusive passou a integrar formalmente o CRI no ano de 2022, conforme o *Joint Statement* da Casa Branca de 1 de novembro de 2022[49], que lista o país entre os membros participantes.

Dessa forma, o ataque à *Colonial Pipeline* não apenas expôs os riscos concretos à continuidade de serviços essenciais, como também promoveu mudanças estruturais na política cibernética norte-americana, servindo como impulsionador para reformas regulatórias, legislativas e institucionais que moldam a atual resposta estatal ao *ransomware*.

No que tange às consequências práticas do ataque, o autor Taiwo Justice Olorunlana[50] analisou os principais danos sofridos pelos Estados Unidos, os quais se concentraram no aumento dos preços dos combustíveis, escassez de gasolina, superlotação de postos de abastecimento, alto custo do resgate, prejuízo operacional e impacto na cadeia de suprimentos.

Com o ataque de *ransomware*, o preço médio do galão de gasolina nos Estados Unidos ultrapassou US$ 3,00 (três dólares) pela primeira vez desde 2014, sendo que, na Costa Leste, o aumento chegou a 6,4% (seis vírgula quatro porcento) em poucos dias[51].

A paralisação gerou um pânico generalizado, o que fez com que os consumidores esgotassem os estoques em diversos estados. Mais de 15 (quinze) mil postos de gasolina ficaram sem combustível, especialmente na Geórgia, Carolina do Norte e Virgínia.

---

[48] UNITED STATES. The White House. **Fact Sheet: Biden-Harris Administration Convenes Fourth Global Gathering to Counter Ransomware.** Washington, D.C.: The White House, 02 out. 2024. Disponível em: https://www.presidency.ucsb.edu/documents/fact-sheet-biden-harris-administration-convenes-fourth-global-gathering-counter-ransomware. Acesso em: 18 nov. 2025.

[49] https://eucyberdirect.eu/atlas/sources/international-counter-ransomware-initiative-2022-joint-statement

[50] OLORUNLANA, Taiwo Justice; MOHAMMED, Hamdiya. ***Analysis of the Colonial Pipeline Cybersecurity Incident. International Journal of Science, Architecture, Technology, and Environment,*** v. 2, n. 4, abr. 2025. DOI: 10.63680/jngh0767as.

[51] BEERMAN, Jack; BERENT, David; FALTER, Zach; BHUNIA, Suman. **A Review of Colonial Pipeline Ransomware Attack.** In: IEEE/ACM 23rd International Symposium on Cluster, Cloud and Internet Computing Workshops (CCGridW)**,** 2023, Bangalore, Índia.

Sob a perspectiva penal, após o ataque à rede de oleodutos norte-americana, devido à forte pressão do governo dos Estados Unidos, o grupo *DarkSide* anunciou ter encerrado as suas atividades[52], tendo, supostamente, perdido o acesso à sua própria estrutura de *ransomware.*

Consoante analisam Chad Whelan, David Bright e James Martins, especialistas em criminologia com foco em redes criminosas, no artigo "*Reconceptualising organised (cyber)crime: The case of ransomware" publicado no Jornal de Criminologia da Sage Journals*[53], *n*ão raro, grupos *hackers* se dissolvem, como forma de despistar as buscas policiais e evitar os holofotes, mas reaparecem em momentos posteriores com nomes diferentes, a fim de realizar novos ataques sem perigo de fácil rastreio.

Ao final, em novembro de 2021, a *Europol*[54] anunciou a prisão de um suspeito ligado ao grupo na Polônia e outro na Romênia. Em 2022, o *Secret Service*[55] do Estados Unidos prendeu um dos integrantes russos do grupo.

Até a produção deste trabalho acadêmico, diante das pesquisas realizadas, a maioria dos membros segue foragida ou realocada em outros grupos de *ransomware*, o que demonstra que, mesmo com o emprego de esforços e investimentos na proporção realizada pelo país norte-americano, a identificação dos autores do ataque ainda é ponto sensível.

No que diz respeito ao processamento penal dos indivíduos capturados, não há informações amplamente divulgadas e confiáveis, considerando a confidencialidade dos processos e a cooperação internacional, de modo que não se sabe o *status* da responsabilização criminal dos agentes.

Assim, apresentado o caso referência, é de suma importância que compreendamos melhor como se desenvolve um ataque de *ransomware*.

---

[52] *The New York Times.* "Hacking Group Behind Colonial Pipeline Attack Says It Is Shutting Down". Disponível em: https://www.nytimes.com/2021/05/14/us/politics/darkside-colonial-pipeline-hack.html. Acesso em: 29 mar 2025

[53] WHELAN, Chad; BRIGHT, David; MARTIN, James. ***Reconceptualising organised (cyber)crime: The case of ransomware.*** Journal of Criminology, v. 57, n. 1, p. 45-61, 2024. Disponível em: https://journals.sagepub.com/doi/10.1177/26338076231199793. Acesso em: 18 de nov de 2025,

[54] Ransomware affiliate arrested for extorting companies in the US and South Korea". Disponível em: https://www.europol.europa.eu/newsroom/news/ransomware-affiliate-arrested-for-extorting-companies-in-us-and-south-korea. Acesso em: 28 mar 2025

[55] SHEA, Chris. **White House: Arrested Russian hacker was behind Colonial Pipeline attack.** *The Record*, 14 jan. 2022. Disponível em: https://therecord.media/biden-official-one-of-arrested-russian-hackers-carried-out-the-colonial-pipeline-attack. Acesso em: 28 mar. 2025.

2. TRATANDO GENERICAMENTE DA CIBERCRIMINALIDADE

2.1. O “crime” de *ransomware*

O século XXI é tido como a era das grandes revoluções tecnológicas. Hoje, vivemos uma realidade antes pouco imaginada, na qual uma rede global de computadores é capaz de interconectar pessoas e outras redes locais, regionais e internacionais em um mesmo sistema, permitindo o acesso por intermédio de portas virtuais abertas através de credenciais digitais, como no nosso caso prático modelo.

Está-se diante da dominância da Internet.

Naturalmente, como já exposto, com o avanço dessa tecnologia, surge também o temor quanto ao seu controle, sobretudo quando as condutas criminosas são praticadas dentro da própria rede mundial de computadores, configurando a mencionada infração cibernética própria.

Em termos de responsabilidade penal, a legislação brasileira já prevê a punição para alguns crimes cibernéticos. Ocorre que, a preocupação persistente é com as práticas que não possuem qualquer normatização e, muito menos, responsabilização penal, ainda que tímida, tais como ataques cibernéticos voltados ao sequestro de banco de dados, falsidade ideológica virtual, roubos de informações e paralisação de infraestruturas críticas.

A inteligência artificial tem sido empregada para aumentar a eficácia de ataques cibernéticos, como aqueles realizados por *bots*[56], isto é, programas de computador desenvolvidos para executar tarefas repetidas vezes, de forma automatizada, como se um humano fosse.

Significa dizer que um computador recebe um comando para realizar determinada tarefa exatamente como um indivíduo deveria fazê-la, porém em escalas humanamente impossíveis e em um curtíssimo espaço de tempo.

Ao contrário de depender da implementação de um ataque manual, atualmente os grupos se utilizam das inteligências artificiais para criarem programas que localizam, automaticamente, as vulnerabilidades de um sistema de segurança[57], utilizando justamente o sistema de *bots.*

---

[56] Abreviação da palavra “robô”.

[57] RUSSELL, Stuart; NORVIG, Peter. **Artificial Intelligence: A Modern Approach.** 4ª ed. Pearson, 2021. Disponível em: https://dl.ebooksworld.ir/books/Artificial.Intelligence.A.Modern.Approach.4th.Edition.Peter.Norvig.%20Stuart.Russell.Pearson.9780134610993.EBooksWorld.ir.pdf. Acessado em: 14 set 2025.

É dessa maneira que um ataque se torna mais eficiente e perigoso, na medida em que há um estudo prévio e o desenvolvimento da maneira ideal para que a invasão não seja descoberta e ainda atinja exatamente o objetivo pretendido.

A execução desse avançado sistema informatizado se revela como mecanismo estrutural das modalidades criminosas mais comuns no cenário atual[58].

A título de exemplo, a inteligência artificial tem sido empregada como facilitadora no roubo de dados pessoais, que é uma prática recorrente em ataques cibernéticos. Os criminosos, por intermédio de *bots* vasculham grande volume de dados na internet para identificar informações pessoais e financeiras. Por meio de algoritmos de aprendizado de máquina, torna-se possível a análise imediata de informações e a fixação de padrões de comportamento, o que viabiliza o desenvolvimento de técnicas mais eficazes de engenharia social, como o *phishing*[59], que, ao que tudo indica, foi a técnica utilizada para a invasão à *Colonial Pipeline*.

Neste tipo de ataque, dados são disponibilizados sem que os alvos percebam e os crimes sejam cometidos.

O que se tem é que, com o grande valor gerado pela informação na competitividade de mercado, esta se tornou um alvo constante de criminosos, que buscam comprometer a imagem não só de indivíduos, mas também de empresas e órgãos, visando a rápida obtenção de benefícios de alta importância socioeconômica.

Portanto, os ataques podem ser descritos como qualquer tentativa de abusar da vulnerabilidade de sistemas e usuários para acessar dados e processos confidenciais. Os objetivos, geralmente, são de acesso a informações privilegiadas, vazamento, extorsão (sequestro de dados), venda de dados para partes interessadas, falsidade ideológica ou, ainda, a disseminação de informações inverídicas.

As ameaças cibernéticas, com relação ao seu funcionamento, podem ser separadas em dois grupos: ataques externos, que utilizam brechas em aplicações e dispositivos para acessar áreas restritas com força bruta, e ataques internos, em que os criminosos utilizam táticas para acessar de forma legítima (permitida) o ambiente protegido.[60]

Seja qual for a motivação, os cibercriminosos se aproveitam do anonimato e da dificuldade de rastreamento de técnicas invasivas para obterem vantagem e colocarem suas vítimas em situações de extrema insegurança e vulnerabilidade.

---

[58] CHEN, Thomas M.; JAJODIA, Sushil. **Cybersecurity: Principles and Practice.** 3ª ed. Springer, 2021.
[59] BACH, Sirlei Lourdes. **Contribuição do Hacker para o desenvolvimento da informática.** 2001. 135 f. Tese (Doutorado) - Curso de Ciência da Computação, Universidade Federal de Santa Catarina, Florianopolis, 2001.
[60]SILVA, Marco Aurélio Barbosa da. **Cibercrimes: Aspectos Jurídicos e Técnicos**. 2ª ed. São Paulo: Revista dos Tribunais, 2017.

A preparação do Estado para a proteção dos dados pessoais é nebulosa, afinal, os ataques cibernéticos podem acarretar perda financeira, interrupção de serviços e operações, roubo e exposição de dados pessoais, perda de confiança, danos à reputação, riscos à segurança nacional, danos psicológicos, perda de propriedade intelectual e, inclusive, um aumento nos custos da implementação da segurança, não só em âmbito particular como público em geral.

Significa dizer que, um ataque cibernético atinge tanto pessoas físicas, como pessoas jurídicas e o próprio Estado, criando uma esfera de desproteção em torno de toda uma sociedade.

Atualmente, há escasso amparo na vida real que assegure aos indivíduos que seus dados não serão corrompidos, quiçá perdidos, em um desses ataques. Os especialistas em tecnologia, em tese, são responsáveis por entregarem as ferramentas necessárias para a competitividade moderna, mas, ao mesmo tempo, o Estado deve ser o garantidor de que elas possam ser usadas com segurança e eficiência.

Neste liame, os agentes criminosos se utilizam de programas de computador desenvolvidos para a invasão dos terminais detentores dos dados almejados. Esses programas são chamados de *malware*, popularmente conhecidos como vírus de computador.

O *Malware*, ou *software* malicioso, é qualquer tipo de código furtivo instalado em um dispositivo (computador, smartphone, entre outros) que passa a executar ações localmente sem o conhecimento do usuário. Geralmente, eles são instalados não intencionalmente, disfarçados de outros arquivos ou embutidos em aplicações de terceiros. A partir do momento em que são ativados, agem automaticamente, realizando funções diversas. Os *malwares* podem ser utilizados para espionar uso de sistemas, interceptar comunicações, registrar teclas digitadas, captar e enviar dados ou até diminuir a capacidade de processamento da máquina.

A categoria de *malwares* que mais se popularizou nos últimos tempos foi, justamente, o *ransomware*[61]. Esse código bastante especializado tem como função criptografar dados a que tem acesso a partir do dispositivo em que foi instalado – que pode ir do disco local da máquina até bancos na nuvem – com fins de extorquir digitalmente os alvos.

Existem duas formas de extorsão por *ransomware*, quais sejam, as que criptografam, ofuscam ou impedem o acesso aos arquivos, e aquelas não modificam os dados, mas restringem o acesso ou bloqueiam os usuários dos sistemas.

---

[61] FORNASIER, Mateus de Oliveira; SPINATO, Tiago Protti; RIBEIRO, Fernanda Lencina. **Ransomware e cibersegurança: a informação ameaçada por ataques a dados.** Revista Thesis Juris–RTJ, São Paulo, v. 9, n. 1, p. 208-236, jan./jun. 2020. http://doi.org/10.5585/rtj.v9i1.16739

O *ransomware* teve origem a partir de um código malicioso chamado de AIDS Trojan, também conhecido como *PC Cyborg*, desenvolvido em 1989 por Joseph L. Popp Jr., um biólogo evolucionista. O AIDS original é o famigerado "cavalo de Troia" (trojan), conhecido até mesmo por aqueles que não possuem afinidade com a área da tecnologia da informação[62].

Esse código era distribuído em disquetes e era capaz de embaralhar os nomes dos arquivos armazenados no computador invadido por meio de criptografia, o que impedia a identificação e o acesso dos usuários aos referidos documentos, colocando toda a máquina em posse do invasor, ainda que a longas distâncias.[63]

Desse modo, o objetivo de um ataque de *ransomware*, desde os primeiros episódios identificados ainda nos anos 90, é impedir o acesso da pessoa, órgão ou empresa às suas próprias informações e também a dados de usuários, algo que inviabiliza a produtividade na era digital e pode acarretar vazamentos sérios.

Quando bem-sucedido, o agente criminoso exige, inclusive, uma compensação em dinheiro (geralmente, criptomoedas, ou serviços de voucher pré-pagos como MoneyPak, Ukash, etc) para devolver o acesso aos dados – daí o nome *ransom*, que significa "resgate", na língua inglesa.[64]

Como consectário lógico, podemos dizer que os grupos criminosos optam pelo recebimento em moedas virtuais justamente pelo maior anonimato e facilidade na realização de transações nacionais e internacionais, dificultando o rastreio financeiro e viabilizando atos, por exemplo, de lavagem de dinheiro.

Isto é, por meio de um programa, os agentes criminosos invadem determinado sistema, instalam um *ransomware*, bloqueiam/ocultam os dados alocados na máquina e somente os liberam após o pagamento do resgate, servindo como um sequestro de informações.

Atualmente, toda a sociedade funciona a partir de sistemas computadorizados, de modo que qualquer estabelecimento, órgão ou pessoa se torna potencial vítima de ataques dessa natureza, não se sabendo, sequer, se os dados indisponibilizados pelos criminosos durante o "crime" serão devolvidos de forma intacta ou se serão mal utilizados em atos subsequentes.

---

[62] https://www.sdxcentral.com/search/?q=aids+trojan#/?q=aids%20trojan&orderby=recent

[63] BATES, Jim. **Trojan Horse: AIDS Information Introductory Diskette Version 2.0**. *Virus Bulletin*, Oxfordshire, v. 2, n. 1, p. 3-5, jan. 1990. Disponível em: https://www.virusbulletin.com/uploads/pdf/magazine/1990/199001.pdf. Acesso em: 15 jan. 2025.

[64] WENDT, Emerson; GUEIROS, Guilherme. **Ransomware 360°: Abordagens Multidisciplinares da Extorsão Criptoviral.** 1. ed. São Paulo: Opice Blum Academy, 2021.

As ameaças de *ransomware* não estão limitadas a nenhuma área geográfica ou sistema de operação em particular e podem atuar desde dispositivos de *Android* até *iOS* ou *Windows*, os quais são os mais utilizados na atual sociedade da informação.

Assim como nos primórdios, quando os navios eram saqueados, hoje, os criminosos, com a pretensão obscura de subtrair dados e, por meio destes, praticar enormes fraudes, estelionatos, entre outros delitos, navegam pela rede mundial de computadores em busca de novas vítimas.

A engenharia social, que é o conjunto de técnicas usadas por criminosos para manipular pessoas, explorando aspectos psicológicos e comportamentais, a fim de obter informações, acesso ou vantagens, pode englobar todos os tipos de ataques, mas também tem suas características próprias. A maior vulnerabilidade dos sistemas está exatamente nesta vítima, que naquele contexto figura como usuário.

A invasão forçada a computadores de terceiros gera, de pronto, uma enorme comoção, eis que a vítima, geralmente, percebe de imediato que algo está incorreto e aciona mecanismos de proteção com fins de impedir a entrada de usuários desconhecidos. É essa a função dos programas de antivírus que normalmente são instalados logo após a compra de computadores.

Por esse motivo, os ataques mais comuns não buscam fazer a entrada pela "força bruta", mas, sim, ludibriar as pessoas, para que elas concedam acesso sem perceberem, o que por si só já pode significar uma dificuldade na responsabilização do agente[65], já que ele camufla a sua entrada no sistema.

Foi a modalidade aparentemente utilizada na invasão do caso *Colonial Pipeline.*

Por outro lado, a "força bruta" ainda é utilizada em casos em que o *ransomware* também pode ser praticado em formato de negação de serviço.

Neste formato, o criminoso utiliza um grande número de dispositivos cooptados por *malwares* para fazer um volume de acesso superior ao que o servidor da empresa ou órgão suporta. No cenário, o sistema fica abarrotado e acaba sendo desconectado, o que expõe uma brecha para invasões ou o comprometimento de produtos digitais disponibilizados pelo alvo.

Em termos práticos, podemos dizer que esse mecanismo é como um ataque a um país por meio de um exército inteiro, situação em que há investidas por todos os lados, até que o país atacado, sem força de repressão, recue e abra espaços para uma invasão completa e a tomada do território.

---

[65] CLARKE, Richard; KNAKE, Robert. **Cyber War: The Next Threat to National Security and What to Do About It.** Nova York: HarperCollins, 2010.

Indubitavelmente, a compreensão sobre as modalidades de ataque permite a criação de obstáculos a práticas dessa natureza, sobretudo ao se considerar que, após praticada a conduta, mais difícil se torna o rastreamento de seus autores.

Há instituições que, em busca de implementarem métodos capazes, ao menos, de dificultar invasões, propõem debates quanto à utilização de vias únicas de acesso à serviços públicos digitais pelo usuário, com fins de proteger os dados manuseados, o alcance às informações alocadas no sistema e proporcionar uma real barreira virtual ao acesso.[66]

2.2. A arquitetura do ataque

Não obstante o presente trabalho acadêmico seja direcionado ao estudo jurídico do ataque de *ransomware* e ao tratamento dado à modalidade pelo Estado Brasileiro na esfera penal, torna-se impossível a análise profunda da investigação e criminalização da conduta sem que saibamos a arquitetura de um ataque de *ransomware,* inclusive para que se possa, ao final da pesquisa, identificar como se pode trabalhar para sanar as dificuldades enfrentadas.

Uma invasão dessa natureza perpassa por, basicamente, 08 (oito) fases, que foram desenvolvidas a partir de uma análise consolidada por especialistas em segurança cibernética, pesquisadores e empresas de segurança, havendo ainda, divergências quanto à nomeação dessas etapas.

Bruce Schneier[67], em seus livros "*Applied Cryptography*"[68] e "*Secrets and Lies: Digital Security in a Networked World*"[69], e Eugene Kaspersky, fundador da *Kaspersky Lab* (empresa de segurança cibernética), auxiliaram na estruturação das etapas do ataque juntamente com organizações como a *Mitre Attack Framework* e a NIST (*National Institute of Standard and Technology*).

Para essas referências do universo digital, o ataque de r*ansomware* segue um processo estruturado em que passa por: 1) Reconhecimento; 2) Infecção; 3) Execução; 4) Proliferação; 5) Exfiltração; 6) Criptografia; 7) Extorsão e 8) Resultado.[70]

---

[66] MARTINS, João Pedro; SILVA, Ana Carolina; PEREIRA, Lucas. ***Ransomware attacks and the protection layer on government systems.*** *Núcleo do Conhecimento*, [S.l.], 30 mar. 2022. Disponível em: https://www.nucleodoconhecimento.com.br/technology-en/ransomware-attacks. Acesso em: 28 mar. 2025.
[67] https://www.schneier.com/books/applied-cryptography/
[68] SCHNEIER, Bruce. **Applied Cryptography: Protocols, Algorithms, and Source Code in C.** 2. ed. New York: John Wiley & Sons, 1996. ISBN 978-1119096726.
[69] SCHNEIER, Bruce. **Secrets and Lies: Digital Security in a Networked World.** New York: John Wiley & Sons, 2000. ISBN 978-1119092438.
[70] https://attack.mitre.org/

Os autores norte-americanos Allan Liska e Timothy Gallo tratam as fases do ataque na obra "*Ransomware:* Defendendo-se da Extorsão Digital"[71], livro traduzido para o português por Lúcia A. Kinoshita, ocasião em que as sintetizam em 05 (cinco) etapas: 1) Implantação; 2) Instalação; 3) Comando e Controle; 4) Destruição e 5) Extorsão.

Com o intuito de manter a didática e acessibilidade da presente produção acadêmica, serão utilizadas ambas as denominações.[72]

Na primeira fase do ataque, Reconhecimento *(Reconnaissance),* o invasor realiza uma coleta de informações sobre o alvo, buscando pontos fracos na infraestrutura e na rede. Nessa fase, são usadas técnicas como engenharia social (tipo *phishing*), análise de sistemas desatualizados ou vulnerabilidades de *softwares* para mapear o ambiente e escolher o alvo mais vulnerável.

Na fase da Infecção/Implantação (*Inicial Acces/Deployment*), após o reconhecimento, o atacante implanta o *malware* no sistema da vítima. Isso pode ocorrer através de um anexo de e-mail, um *link* malicioso ou uma vulnerabilidade de *software* não corrigida, que são as portas virtuais abertas. O *malware* é instalado de forma furtiva, preparando o terreno para a execução do ataque.

Ato contínuo, inaugura-se a etapa de Execução/Instalação (*Execution/Installation*), oportunidade em que o *ransomware* é executado no sistema e instalado. O *malware* tenta garantir persistência, o que significa que ele toma medidas para se manter ativo, mesmo após reinicializações do sistema. Isso pode envolver a modificação de configurações ou a desativação de mecanismos de segurança (como antivírus e *firewalls*).

Uma vez instalado, é iniciada a fase de Proliferação/Comando (*Lateral Movement/Command*). O *ransomware* começa a se espalhar dentro da rede ou sistema, explorando vulnerabilidades adicionais. Nesta fase, o atacante pode usar o *malware* para emitir

---

[71] LISKA, Allan; GALLO, Timothy. ***Ransomware: Defendendo-se da Extorsão Digital.*** Tradução de Lúcia A. Kinoshita. 1. ed. São Paulo: Novatec, 2017. ISBN 978-85-7522-551-6. Disponível em: https://books.google.com.br/books?hl=pt-BR&lr=&id=gf6ZDwAAQBAJ&oi=fnd&pg=PT4&dq=tudo+sobre+ransomware&ots=SG-jELbn2D&sig=psdr924270DhngNSeEOQwoWbuRc&redir_esc=y#v=onepage&q=tudo%20sobre%20ransomware&f=false

[72] LISKA, Allan; GALLO, Timothy. **Ransomware: Defendendo-se da Extorsão Digital.** Tradução de Lúcia A. Kinoshita. 1. ed. São Paulo: Novatec, 2017. ISBN 978-85-7522-551-6. Disponível em: https://books.google.com.br/books?hl=pt-BR&lr=&id=gf6ZDwAAQBAJ&oi=fnd&pg=PT4&dq=tudo+sobre+ransomware&ots=SG-jELbn2D&sig=psdr924270DhngNSeEOQwoWbuRc&redir_esc=y#v=onepage&q=tudo%20sobre%20ransomware&f=false

SCHNEIER, Bruce. **Applied Cryptography: Protocols, Algorithms, and Source Code in C.** 2. ed. New York: John Wiley & Sons, 1996. ISBN 978-1119096726.

SCHNEIER, Bruce. **Secrets and Lies: Digital Security in a Networked World.** New York: John Wiley & Sons, 2000. ISBN 978-1119092438.

comandos remotos, garantindo controle sobre mais máquinas na rede. O objetivo é maximizar o impacto e garantir que o *ransomware* alcance o maior número possível de dispositivos.

Estabelecido o controle, o *ransomware* pode, antes de criptografar os arquivos, passar pela fase de Exfiltração/Destruição (*Data Exfiltration/Destruction*), ocasião em que dados sensíveis da vítima são roubados para aumentar o poder de extorsão. O atacante pode usar esses dados para ameaçar a divulgação pública ou venda de informações confidenciais. A destruição pode ocorrer em forma de criptografia ou exclusão de arquivos críticos para interromper o funcionamento do sistema.

A fase de Criptografia (*Encryption*) é aquela em que fatalmente o *ransomware* criptografa os arquivos da vítima, tornando-os inacessíveis. Os atacantes substituem a extensão dos arquivos criptografados, deixando uma mensagem com instruções sobre o resgate, onde o pagamento é solicitado para fornecer a chave de "descriptografia".

Essa etapa do ataque consiste na utilização de fórmulas matemáticas complexas que, literalmente, embaralham o conteúdo da informação, tornando-a ilegível, e somente o código correto (chave) é capaz de "destrancar" o texto. É essa propriedade, por exemplo, que inviabiliza de fato a operação de empresas, paralisa infraestruturas críticas e impede a restauração célere de sistemas.

Os invasores passam a exigir o pagamento do resgate, perfazendo a etapa da Extorsão (*Extortion*). Normalmente, o pagamento é solicitado em criptomoedas, cuja principal característica é a dificuldade de se rastrear. Se o pagamento não for feito, o atacante pode ameaçar a divulgação dos dados roubados, a venda a terceiros ou a destruição definitiva das informações.

Por fim, consagra-se a etapa do Resultado (*Post-Attack Actions*). Após o ataque, a vítima precisará lidar com as consequências. O pagamento do resgate pode liberar os arquivos, mas não há garantias de que os dados serão devolvidos ou que os atacantes não retornarão. A vítima também pode optar por não pagar, o que pode resultar na perda permanente dos dados. Ainda, pode-se tentar recuperar os dados por meio de *backups*, se disponíveis.

William Stallings[73] define a realização de *backups* como sendo uma das medidas mais essenciais de resiliência institucional frente a ataques de *ransomware*, uma vez que consiste na criação de cópias de segurança dos dados e sistemas críticos, armazenadas de forma redundante e, preferencialmente, isolada da rede principal.

[73] STALLINGS, William. ***Cryptography and Network Security: Principles and Practice*.** 8. ed. Boston: Pearson, 2023.

A partir das etapas do ataque já é possível perceber os maiores desafios encarados quando o assunto é *ransomware:* a) a identificação dos invasores, que estão mascarados pelo *malware* implantado; b) impedir que a invasão aconteça ou prossiga, já que os mecanismos de segurança são desativados e o acesso passa a ser impedido pela criptografia imposta aos arquivos; e c) resgatar os dados intactos (os seus e os dos outros), contendo eventuais danos com repercussão na vida real.

2.3. O marco jurídico internacional no contexto dos crimes cibernéticos

A era da informação deu início a movimentações internacionais em busca de se estabelecer a abordagem a ser conferida às condutas ilícitas praticadas no espaço cibernético, na medida em que essas novas atividades transcendem as fronteiras tradicionais e modificam o panorama jurídico já conhecido.

Uma vez ultrapassados os limites geográficos da conduta, surgem novas percepções quanto à delimitação da jurisdição e competência no tratamento dos crimes cibernéticos, o que praticamente obriga a promoção de cooperação jurisdicional entre os países no desenvolvimento de políticas criminais.

Como observa Paulo Abrão Pires Júnior[74], a realização efetiva da justiça em um cenário global marcado por intensa interconectividade exige uma postura mais cooperativa e proativa por parte dos Estados. A crescente complexidade das relações jurídicas contemporâneas – que frequentemente ultrapassam limites territoriais e desafiam a atuação isolada das jurisdições soberanas – evidencia a indispensabilidade de mecanismos sólidos de cooperação internacional. Tal articulação entre nações não apenas reforça a capacidade estatal de responder a conflitos transnacionais, como também assegura que as demandas de justiça formuladas por indivíduos e pela coletividade sejam atendidas de maneira integral, coordenada e eficiente.

Assim, uma persecução penal eficaz, que pode alcançar múltiplas jurisdições, também pode exigir diligências que vão além daquelas abarcadas pelo país onde ocorreu o ataque. Dessa forma, é imprescindível a interação entre nações e estados com fins de lidar com as consequências, também múltiplas, de uma conduta dessa natureza.

Nesse cenário, é primordial compreender a importância da cooperação jurídica em matéria penal, a imprescindibilidade da existência de legislações harmônicas e a necessária

[74] PIRES JÚNIOR, Paulo Abrão. **O papel da cooperação jurídica internacional. In: Manual de cooperação jurídica internacional e recuperação de ativos.** Secretaria Nacional da Justiça. 2. ed. Brasília, 2012, p. 17.

aplicação coordenada da lei ante os desafios enfrentados pela persecução penal dos crimes cibernéticos. Por isso, se torna indiscutível a importância da assinatura de acordos multilaterais entre países, que facilitam a cooperação internacional.

Japiassu[75] ensina que o Direito Penal Internacional constitui o ramo jurídico responsável por definir os crimes de natureza internacional e estabelecer as sanções correspondentes, disciplinando, ainda, temas sensíveis como a extraterritorialidade da lei penal, as imunidades de agentes internacionalmente protegidos e os múltiplos mecanismos de cooperação penal entre Estados. A ele compete também regular a transferência de processos e de pessoas presas ou condenadas, a extradição, os critérios para reconhecimento e execução de penas estrangeiras e a própria estruturação e funcionamento de tribunais penais de alcance internacional ou regional.

Em sentido amplo, o autor assinala que esse campo normativo abarca toda e qualquer problemática criminal envolvendo indivíduos cuja repercussão se projete para além das fronteiras estatais.

Nessa perspectiva, o Direito Penal Internacional não se restringe ao tratamento dos delitos transnacionais — tradicionalmente vinculados ao Direito Penal interno —, mas também incorpora, de modo indissociável, os instrumentos e procedimentos de cooperação penal internacional, usualmente analisados no âmbito do Direito Processual Penal, revelando sua natureza transversal e essencialmente integrada.

Nas palavras de Bechara[76], a cooperação jurídica penal internacional se define como o conjunto de medidas que estabelecem as diretrizes para a interação entre dois ou mais Estados, ou até mesmo entre Estados e tribunais internacionais, com o objetivo de suprir as restrições territoriais impostas pela soberania. Essa necessidade surge em decorrência das limitações inerentes à autonomia estatal.

No contexto dos crimes cibernéticos, as autoridades responsáveis pela persecução penal têm identificado[77], de forma cada vez mais evidente, a necessidade de acessar diligências e elementos probatórios situados além dos limites de suas próprias jurisdições. Trata-se de uma demanda que decorre diretamente da natureza transfronteiriça de inúmeros delitos

---

[75] GUEIROS, Artur; JAPIASSÚ, Carlos Eduardo. **Direito penal: volume único.** São Paulo: Atlas, 2018.
[76] BECHARA, Fábio Ramazzini; FLORES, Dímitri Molina. **Crimes cibernéticos: qual é o lugar do crime para fins de aplicação da pena e determinação da competência jurisdicional.** Revista Direito Mackenzie, v. 13, n. 2, p. 1-21, 2019.
[77] MINISTÉRIO DA JUSTIÇA. **Manual de Cooperação Jurídica Internacional. Matéria Penal e Recuperação de Ativos**. 4. ed. Brasília, 2019. Disponível em: https://www.gov.br/mj/pt-br/assuntos/sua-protecao/lavagemdedinheiro/institucional-2/publicacoes/manuais/cooperacao-juridica-internacional-em-materia-penal/manualpenalonline-final-2.pdf. Acesso em: 18 de nov de 2025.

contemporâneos, exigindo a obtenção de informações no exterior para a adequada elucidação tanto da autoria quanto da materialidade das infrações que extrapolam o alcance das fronteiras nacionais.

E para além disso, a cooperação internacional não se volta apenas ao auxílio na persecução como também na própria proteção estatal contra os delitos virtuais. Os Estados Unidos e os países europeus se tornaram precursores no desenvolvimento de normativas e regulamentos voltados à repressão dessas condutas.

Diante disso, torna-se essencial que a produção acadêmica se aprofunde na análise dos documentos normativos elaborados pela comunidade internacional, com o objetivo de compreender os parâmetros firmados por países cujos sistemas jurídicos apresentam maior grau de maturidade e que enfrentam essas modalidades criminosas há mais tempo que o Brasil.

Tratam-se aqui de normas desenvolvidas pelas grandes potências mundiais e não apenas diretrizes práticas a serem utilizadas na ocasião de um ataque.

Nos Estados Unidos, a legislação federal é a principal fonte de regulação sobre crimes cibernéticos. A *Computer Fraud and Abuse Act* (CFAA)[78], aprovada em 1986, é uma das normas mais relevantes nesse contexto, tendo sido alterada em diversas ocasiões para acompanhar a evolução tecnológica. Essa lei estabelece sanções para o acesso não autorizado a sistemas computacionais, danos a dispositivos eletrônicos e divulgação indevida de informações confidenciais.

Além disso, a *Federal Information Security Modernization Act* (FISMA)[79] impõe às agências federais a obrigação de proteger seus sistemas contra ameaças cibernéticas, impondo padrões rigorosos de segurança. No campo penal, assim como no Brasil, as leis contra a lavagem de dinheiro também punem a ocultação da origem de bens ilícitos, o que pode abranger situações em que há pagamento de resgate a grupos criminosos.

Nesse sentido, o *USA Patriot Act*[80] veda o fornecimento consciente de apoio material a organizações terroristas, o que pode incluir pagamentos de resgates em determinadas circunstâncias. Complementarmente, o *Office of Foreign Assets Control* (OFAC)[81], vinculado

---

[78] ESTADOS UNIDOS. **Computer Fraud and Abuse Act** *(CFAA)*. Public Law 99-474, 100 Stat. 1213, 16 out. 1986 (18 U.S.C. § 1030). Disponível em: https://www.govinfo.gov/app/details/STATUTE-100/STATUTE-100-Pg1213. Acesso em: 20 jun. 2025.

[79] ESTADOS UNIDOS. **Federal Information Security Modernization Act of 2014 (FISMA).** Public Law 113-283, 18 dez. 2014 (atualização da Federal Information Security Management Act de 2002). Disponível em: https://csrc.nist.gov/topics/laws-and-regulations/laws/fisma. Acesso em: 20 jun. 2025.

[80] ESTADOS UNIDOS. **Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act)**. Public Law 107-56, 02 out. 2001.

[81] ESTADOS UNIDOS. **Office of Foreign Assets Control — Department of the Treasury.** Orientações sobre pagamento de resgates relacionados a entidades sancionadas. Disponível no site do Departamento do Tesouro. Acesso em: 20 jun. 2025.

ao Departamento do Tesouro, emitiu orientações segundo as quais o pagamento a determinados grupos de cibercriminosos pode ser considerado ilegal, dependendo de sua vinculação com entidades sancionadas.

Outra medida relevante é a própria *Cyber Incident Reporting for Critical Infrastructure Act* (CIRCIA)[82], de 2022, criada após o ataque à *Colonial Pipeline*, que obriga entidades operadoras de infraestrutura crítica a reportarem incidentes cibernéticos às autoridades reguladoras, incluindo ataques por *ransomware*.

Além das medidas de natureza penal, a legislação norte-americana também admite a responsabilização civil dos autores de tais ataques, bem como de terceiros eventualmente envolvidos, como seguradoras, dependendo do caso concreto.

No Reino Unido, a principal norma aplicável é o *Computer Misuse Act*[83], que guarda muitas semelhanças com a legislação estadunidense. Essa lei pune o acesso não autorizado a sistemas de computador, a disseminação de vírus ou *malware* e prevê sanções para crimes como espionagem industrial e o roubo de informações comerciais sigilosas.

Na Alemanha, as condutas criminosas relacionadas ao uso indevido de sistemas de informação estão tipificadas no Código Penal (Strafgesetzbuch)[84]. O parágrafo 202a prevê punição para quem obtém ou tenta obter acesso indevido a dados eletrônicos ou compromete o funcionamento de sistemas computacionais, com penas que podem chegar a dois anos de reclusão.

Dessa forma, observa-se uma tendência de compatibilidade e alinhamento entre os sistemas jurídicos das principais potências globais, que têm promovido reformas legislativas e ações coordenadas para combater com maior eficiência os crimes cibernéticos, em especial os ataques de *ransomware*.

No âmbito dos tratados e convenções internacionais em que os crimes cibernéticos já são objeto de deliberações, se destacam o Protocolo de Assistência Jurídica Mútua em Assuntos penais do Mercosul, a Convenção Interamericana sobre assistência mútua em matéria penal (Convenção da OEA) e, de forma mais significativa, a Convenção sobre Cibercrime, também conhecida como Convenção de Budapeste.

---

[82] ESTADOS UNIDOS. **Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA).** Public Law 117-103, 15 dez. 2022.

[83] REINO UNIDO. ***Computer Misuse Act 1990.*** Cap. 18. Londres: Secretaria de Estado do Reino Unido, 1990. Disponível em: https://www.legislation.gov.uk/ukpga/1990/18. Acesso em: 20 jun. 2025.

[84] ALEMANHA. ***Strafgesetzbuch (StGB) – Código Penal Alemão,* §§ 202a–b, 303a–b**. Disponível em: https://www.gesetze-im-internet.de/englisch_stgb/. Acesso em: 20 jun. 2025.

O Protocolo de Assistência Jurídica Mútua em Assuntos Penais do Mercosul foi firmado em San Luis, na Argentina, em 13 de junho de 1996, aprovado pelo Conselho do Mercado Comum (Decisão 02/96) e promulgado no Brasil pelo Decreto nº 3.468, de 17 de maio de 2000.

A normativa constitui um dos pilares da integração jurídica entre os Estados-Partes, em conformidade com o Tratado de Assunção e foi elaborado com o propósito de harmonizar a legislação penal e processual penal dos países integrantes, fortalecendo a resposta conjunta frente às atividades criminosas de natureza transnacional, reconhecendo que a cooperação jurídica em matéria penal é essencial para aprofundar os objetivos comuns e assegurar a efetividade do processo de integração regional.[85]

Sua finalidade central consiste em reduzir entraves burocráticos decorrentes de prerrogativas soberanas, estabelecendo um mecanismo de cooperação direta entre as autoridades competentes dos Estados-Partes. A premissa inicial é de que inúmeras modalidades contemporâneas de criminalidade transnacional – notadamente aquelas que envolvem fluxo de capitais, dados e pessoas – distribuem suas evidências e efeitos por diferentes países, o que demanda um sistema célere e desburocratizado de auxílio mútuo para a obtenção de informações e provas.[86]

No mesmo sentido, a Convenção Interamericana sobre Assistência Mútua em Matéria Penal, firmada na Assembleia Geral da Organização dos Estados Americanos em 1992, em Nassau, e internalizada no Brasil pelo Decreto nº 6.340/2008, representa um marco na consolidação da cooperação penal entre os Estados americanos – incluindo os do Mercosul, com exceção do Uruguai.

Segundo a análise de Sandro Trotta, seu objetivo primordial é propiciar soluções coordenadas para questões jurídicas, políticas e econômicas que emergem entre os países do continente, estabelecendo a obrigatoriedade de assistência recíproca em investigações, processos e procedimentos criminais relativos a delitos de competência do Estado requerente no momento da solicitação.

A Convenção não autoriza o exercício de jurisdição ou funções próprias de autoridades nacionais por agentes do estado estrangeiro, preservando a soberania de cada país, e também veda aos particulares qualquer pretensão de obter, excluir ou impedir a produção de provas no âmbito desses pedidos de auxílio.

---

[85] GUIDI, Guilherme Berti de Campos; REZEK, Op. Cit. p.276-288, p. 279.
[86] TROTTA, Sandro Brescovit; FERREIRA, Luciano Vaz. **Cooperação jurídica internacional em matéria penal: contornos históricos.** Sistema Penal & Violência, v. 5, n. 1, 2013.

Destaca-se, ainda, que há um Acordo de Assistência Judiciária em Matéria Penal entre Brasil e Estados Unidos da América (MLAT)[87], firmado em 14 de outubro de 1997 e em vigor desde 2001, que se trata de instrumento cooperativo destinado a uniformizar procedimentos e mitigar obstáculos ao trânsito internacional de pessoas, bens e provas no contexto de investigações e ações penais. Seu propósito é facilitar a atuação das autoridades encarregadas da persecução criminal em ambos os países, contemplando atividades que vão desde a investigação preliminar até a ação penal e a prevenção do crime, fortalecendo a troca de informações e o apoio jurídico recíproco.

Entretanto, é a Convenção de Budapeste que ainda representa a regulamentação mais moderna e completa que se tem na atualidade no que concerne a ataques cibernéticos e outros delitos virtuais.

Isabela Donza Corrêa e João Araújo Monteiro Neto[88] analisaram, no bojo do artigo "A adesão do Brasil à Convenção de Budapeste e o enfrentamento do Cibercrime: entre a Cooperação Internacional e a expansão do Direito Penal", a repercussão do tratado internacional sobre Direito Penal e Processual Penal no tratamento das práticas virtuais.

Como mencionado pelos autores, em 2023, o Governo Federal Brasileiro[89] promulgou, por meio do Decreto nº 11.491[90], publicado no Diário Oficial da União no dia 12 de abril de 2023, a absorção pelo país da convenção sobre o crime cibernético, firmada em Budapeste. O Brasil, ao aceitar o convite do Conselho da Europa, passou a ser um dos países que aderiram ao instrumento internacional multilateral, fortalecendo, assim, os laços de cooperação com parceiros estratégicos no enfrentamento aos crimes cibernéticos.

A Convenção de Budapeste[91] foi firmada em 2001 no âmbito do Conselho da Europa e constitui o primeiro e mais abrangente tratado internacional voltado especificamente ao enfrentamento dos crimes cibernéticos. Com a adesão de mais de 60 países, a convenção

---

[87] BRASIL. Decreto N° 3.810, de 2 de maio de 2001, **Acordo de Assistência Judiciária em Matéria Penal entre Brasil e Estados Unidos.** Disponível em http://www.planalto.gov.br/ccivil_03/decreto/2001/D3810.htm Acesso em: 18 de nov de 2025.

[88] CORRÊA, Isadora Donza; MONTEIRO NETO, João Araújo. **A adesão do Brasil à Convenção de Budapeste e o enfrentamento do Cibercrime: entre a Cooperação Internacional e a expansão do Direito Penal.** Revista Brasileira de Direito e Tecnologia da Informação, v. 1, n. 16, 2023. Disponível em: https://revista.direitoeti.com.br/RBTI/article/view/160. Acesso em: 20 jun. 2025.

[89] https://www.gov.br/mj/pt-br/assuntos/noticias/convencao-de-budapeste-e-promulgada-no-brasil#:~:text=Por%20meio%20da%20denominada%20Conven%C3%A7%C3%A3o,digitais%20armazenadas%20em%20outros%20pa%C3%ADses.

[90] BRASIL. **Decreto nº 11.491, de 12 de abril de 2023.** Promulga a Convenção sobre o Crime Cibernético. Diário Oficial da União, 13 abr. 2023. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/d11491.htm e https://legis.senado.leg.br/norma/36966539. Acesso em: 20 jun. 2025.

[91] CONSELHO DA EUROPA. **Convenção sobre o crime cibernético (Convenção de Budapeste).** Budapeste, 23 nov. 2001. Disponível em: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561. Acesso em: 20 jun. 2025.

representa um marco no esforço de harmonização normativa em matéria penal e processual penal no contexto digital, estabelecendo parâmetros comuns para a criminalização de condutas típicas da criminalidade informática.

O tratado foi idealizado pelo próprio Conselho Europeu e emergiu da necessidade premente de promover uma resposta penal coordenada entre os Estados signatários, diante do crescimento exponencial de delitos praticados por meio da internet e outras tecnologias da informação.

Consoante Donza e Monteiro, a elaboração se deu como resposta à complexidade crescente dos cibercrimes, que, por sua natureza transnacional, exigem mais do que instrumentos legais internos – demandam mecanismos eficazes de cooperação internacional e intercâmbio célere de informações entre autoridades competentes.

Nesse cenário, a Convenção de Budapeste surge não apenas como instrumento jurídico, mas como expressão de uma política criminal supranacional voltada à tutela da sociedade frente à sofisticação e capilaridade da criminalidade digital.

Ao promover a harmonização legislativa entre os ordenamentos jurídicos nacionais, a convenção propõe a mitigação dos entraves normativos e operacionais que historicamente dificultam a persecução penal em casos de crimes cibernéticos, além de fomentar um modelo de cooperação baseado na confiança recíproca, agilidade procedimental e convergência regulatória.

Com a adesão do Brasil, as autoridades podem contar com mais um recurso nas investigações de crimes cibernéticos, assim como de outras infrações penais, que demandem a obtenção de provas eletrônicas/digitais armazenadas em outros países. Portanto, prevê-se uma cooperação “mais intensa, rápida e eficaz”.

Um dos maiores desafios é que, no âmbito do Direito Penal aplicado aos delitos informáticos, é importante reconhecer que, ainda que determinado material esteja hospedado em servidor localizado fora do território nacional, os efeitos jurídicos se produzem no local onde o conteúdo é acessado, em conformidade com o princípio da territorialidade mitigada. Essa constatação demanda a reinterpretação clássica dos critérios de jurisdição, principalmente no contexto digital.

Bertrand de La Chapelle e Paul Fehlinger[92] afirmam que podemos identificar três níveis distintos de jurisdição na internet. O primeiro é o espaço físico, no qual os indivíduos

[92] DE LA CHAPELLE, Bertrand; FEHLINGER, Paul. ***Internet & Jurisdiction: Jurisdiction on the Internet: From Legal Arms Race to Transnational Cooperation.*** Internet & Jurisdiction Global Policy Network, abril 2016.

estão vinculados ao território que ocupam e, portanto, sujeitos à legislação ali vigente. O segundo, refere-se à jurisdição dos provedores de acesso, em que a relação se estabelece com base na localização da infraestrutura e na legislação do país onde esse provedor está sediado. O terceiro nível, por sua vez, é aquele das comunidades e domínios virtuais, que operam de modo transnacional, à margem de fronteiras geográficas e, muitas vezes, de regulamentações estatais tradicionais, o que desafia os paradigmas clássicos do Direito Penal e Processo Penal.

Diante dessa complexidade, a Convenção de Budapeste emerge como esperança institucional da comunidade internacional à necessidade de uniformização das legislações substantivas penais relativas aos delitos informáticos. Seu escopo ultrapassa a simples tipificação penal, abrangendo também a necessária modernização das normas processuais penais dos Estados signatários.

Ao propor instrumentos jurídicos que conferem poderes efetivos de investigação e persecução penal, a Convenção assegura um modelo capaz de enfrentar não apenas os crimes cometidos por meio de sistemas informatizados, mas também aqueles em que os elementos probatórios estejam vinculados a meios eletrônicos. Portanto, se revela como um marco normativo voltado à superação das limitações territoriais do Direito Penal contemporâneo, à luz de um ciberespaço globalizado e tecnicamente dinâmico.

Para André Zaca Furquim, coordenador-geral de Cooperação Jurídica Internacional em Matéria Penal do Ministério da Justiça e Segurança Pública[93], em seu comunicado oficial sobre a adesão, há uma expectativa de que a Convenção de Budapeste irá, gradativamente, elevar o número de pedidos de cooperação jurídica internacional. Em trecho do seu pronunciamento, afirmou

> Considerando que as investigações operadas no Brasil demandam, cada vez mais, provas eletrônicas que se encontram em outros países, esta Convenção irá facilitar e, portanto, encorajar os investigadores brasileiros a utilizar tal estratégia.

A diretora do Departamento de Recuperação de Ativos e Cooperação Jurídica Internacional (DRCI) do MJSP, Carolina Yumi também expressou opinião no sentido de que

> A integral implementação da Convenção de Budapeste no Brasil trará resultados positivos ao país, uma vez que ensejará a modernização de normativos e políticas

Disponível em: https://www.internetjurisdiction.net/uploads/pdfs/Papers/IJ-Paper-Jurisdiction-on-the-Internet.pdf. Acesso em: 18 de nov de 2025.

[93] BRASIL. Ministério da Justiça e Segurança Pública. **Convenção de Budapeste é promulgada no Brasil.** Brasília, 3 mai. 2023. Disponível em: https://www.gov.br/mj/pt-br/assuntos/noticias/convencao-de-budapeste-e-promulgada-no-brasil. Acesso em: 20 jun. 2025.

> adotadas na temática de enfrentamento aos crimes cibernéticos, assim como na coleta e preservação das provas digitais.[94]

Além do aperfeiçoamento da cooperação internacional na instrução e elucidação dos delitos praticados no ambiente virtual, a Convenção também impulsiona o Brasil a dar continuidade ao desenvolvimento de seu ordenamento jurídico e de sua política diante do avanço da criminalidade no ambiente cibernético, assim o fazendo com o devido equilíbrio entre a intensificação da persecução penal e a proteção de dados pessoais.

Retrato da constante necessidade de atualização de normas e desenvolvimento de mecanismos de proteção é que, no decorrer de 2024, diversas operações conduzidas por autoridades internacionais resultaram na desarticulação de grupos relevantes atuantes no cenário global de ameaças cibernéticas, o que representa um avanço importante para a contenção de ataques de grande escala.[95]

Todavia, esse movimento produziu um efeito paralelo: enquanto estruturas maiores foram neutralizadas, observou-se um crescimento significativo de células menores, fragmentadas, bem como de agentes individuais – os chamados **"**lobos solitários"[96] – que passaram a ocupar o espaço deixado por organizações mais sofisticadas.

Essa pulverização ampliou o volume de ataques e tornou o ambiente digital ainda mais imprevisível. Além disso, alguns grupos remanescentes adaptaram suas estratégias para escapar do monitoramento estatal, passando a direcionar suas ações para pequenas e médias empresas, cujo nível de proteção costuma ser inferior ao das infraestruturas críticas tradicionalmente visadas, o que facilita a execução do ataque e reduz o risco de rápida identificação pelas forças de segurança.

Exemplos desses grupos desmantelados foram: *LockBit*, um grupo de *ransomware* RaaS[97], foi desestruturado graças aos esforços das forças de segurança, liderados pela Agência

---

[94] Idem.

[95] https://www.infosecurity-magazine.com/news-features/top-10-cyber-law-enforcement-2024/?utm_source=chatgpt.com

[96] O termo *lone wolf* tem origem nos estudos de extremismo violento, especialmente na estratégia de 'resistência sem liderança' descrita por Beam (1992) e posteriormente analisada por entidades como a ADL e o SPLC, que documentaram sua adoção por figuras como Tom Metzger e Alex Curtis..
LEVITT, Matthew; RICHTER, Ariel. ***Lone Wolf Terrorism: Policy Paper.*** Washington, DC: Washington Institute for Near East Policy, 2019.
BEAM, Louis. ***Leaderless Resistance***. *The Seditionist*, 1992.

[97] O modelo **Ransomware-as-a-Service (RaaS)** consiste em uma forma de comercialização criminosa na qual desenvolvedores de *ransomware* disponibilizam o *malware*, a infraestrutura de ataque e ferramentas de gerenciamento para outros agentes (os *afiliados*), que executam efetivamente as invasões e negociações com as vítimas. Trata-se de um modelo estruturado de afiliação, semelhante aos serviços legítimos oferecidos na economia digital, que profissionaliza e massifica o ecossistema do *ransomware* ao permitir que indivíduos com baixo conhecimento técnico realizem ataques sofisticados mediante divisão dos lucros obtidos.
LISKA, Allan; GALLO, Timothy. **Ransomware: Defending Against Digital Extortion.** Sebastopol: O'Reilly Media, 2016.

Nacional do Crime do Reino Unido, em colaboração com o FBI e a Europol[98]. *BlackCat*, um grupo RaaS que o FBI havia interrompido em 2023[99], encerrou suas operações em março de 2024, após realizar um ataque bem-sucedido contra a *Change Healthcare*, resultando em um pagamento de resgate estimado em mais de 22 milhões de dólares americanos[100]. *Black Basta* foi afetado pelo reforço do exame rigoroso e vigilância cuidadosa das autoridades após a divulgação de registros de conversas vazados.[101]

A consolidação de mecanismos regulatórios internacionais e a intensificação de ações coordenadas entre diferentes jurisdições são essenciais, no mínimo, para promover a redução dos pagamentos de resgate em casos de *ransomware*, ainda que não haja legislação específica suficiente a proteger e responsabilizar ataques dessa natureza.

Um marco recente e importante nesse processo foi a criação, em 2021, da própria Iniciativa Internacional de Combate ao *ransomware* (*Counter Ransomware Initiative* – CRI), já citada nos capítulos anteriores, liderada pelo governo dos Estados Unidos, que articula atualmente 68 países na formulação de estratégias conjuntas para desarticular o ecossistema global do *ransomware* e harmonizar políticas públicas de enfrentamento.

Em 2023, os países integrantes da CRI firmaram compromisso oficial desencorajando de maneira expressa qualquer pagamento de resgate por vítimas desse tipo de ataque, reforçando a diretriz de que a remessa de valores alimenta a cadeia criminosa e fragiliza a segurança cibernética internacional.

Paralelamente, alguns governos passaram a adotar medidas mais rígidas: o Reino Unido**,** por exemplo, apresentou proposta legislativa em janeiro de 2025 para vedar que órgãos públicos realizem pagamentos de resgate[102], enquanto estados norte-americanos como Flórida[103] e Carolina do Norte[104] já aprovaram leis com esse mesmo teor. No âmbito administrativo, o

---

[98] https://www.europol.europa.eu/media-press/newsroom/news/law-enforcement-disrupt-worlds-biggest-ransomware-operation

[99] https://www.justice.gov/archives/opa/pr/justice-department-disrupts-prolific-alphvblackcat-ransomware-variant

[100] https://www.healthcareinfosecurity.com/blackcat-ransomware-group-seizure-appears-to-be-exit-scam-a-24521

[101] https://www.databreachtoday.com/blogs/leaked-chat-logs-reveal-black-bastas-dark-night-soul-p-3828

[102] UNITED KINGDOM. Cabinet Office. ***Public Sector Ransomware Payments Ban: Consultation Document.*** London: Cabinet Office, Jan. 2025. Disponível em: https://www.gov.uk/government/consultations/public-sector-ransomware-payments-ban. Acesso em: 18 nov. 2025.

[103] FLORIDA. Legislature. ***House Bill 7055: Cybersecurity.*** Tallahassee: Florida Legislature, 2022. Disponível em: https://www.flsenate.gov/Session/Bill/2022/7055. Acesso em: 18 nov. 2025.

[104] NORTH CAROLINA. General Assembly. ***Session Law 2021-180 (House Bill 105): An Act to Enact the State Budget Act.*** Raleigh: NCGA, 2021. Disponível em: https://www.ncleg.gov/BillLookup/2021/H105. Acesso em: 18 nov. 2025.

FBI[105] mantém orientação clara no sentido de que organizações não realizem pagamentos, ao passo que o Departamento do Tesouro dos Estados Unidos alerta que transferências efetuadas para agentes sujeitos a sanções do *Office of Foreign Assets Control* (OFAC)[106] podem gerar responsabilização e violar regulamentos federais.

Assim, além dos impactos operacionais do ataque, empresas e entidades internacionais precisam avaliar cuidadosamente riscos regulatórios, de conformidade e de exposição a sanções ao considerar qualquer forma de pagamento de resgate.

No contexto da cooperação internacional, verificamos que diversas organizações multilaterais, como o Conselho da Europa, a INTERPOL, a Organização para a Cooperação e Desenvolvimento Econômico e o G8, têm desempenhado função decisiva na formulação de respostas coordenadas diante do avanço da criminalidade cibernética. Essas instituições reconhecem que a expansão global dos delitos informáticos impõe aos Estados a adoção de estratégias articuladas, capazes de superar as limitações inerentes às fronteiras territoriais e aos modelos tradicionais de persecução penal.

Medidas como o compartilhamento sistemático de informações, a produção de diretrizes técnicas, a realização de operações conjuntas e a promoção de normas de cooperação internacional figuram entre as principais iniciativas desenvolvidas com o objetivo de fortalecer a capacidade dos países membros na prevenção e repressão a tais condutas. Além disso, essas organizações têm atuado de maneira relevante na conscientização pública e institucional acerca dos riscos e impactos dos crimes cibernéticos, incentivando a adoção de políticas preventivas e contribuindo para o aprimoramento contínuo das legislações nacionais.

A reflexão construída neste capítulo evidencia que as convenções, tratados e instrumentos multilaterais constituem elementos estruturantes da resposta internacional aos crimes cibernéticos. A natureza transnacional dessas infrações, marcada pela fluidez das informações, pela descentralização das estruturas criminosas e pela fragmentação das evidências em múltiplas jurisdições, exige um modelo de enfrentamento pautado na integração e na coordenação global.

Nessa perspectiva, os instrumentos internacionais cumprem a função de estabelecer parâmetros comuns, harmonizar legislações, reduzir obstáculos procedimentais e facilitar a

---

[105] UNITED STATES. Federal Bureau of Investigation. ***Ransomware Prevention and Response for CISOs.*** Washington, D.C.: FBI, 2020. Disponível em: https://www.ic3.gov/Media/News/2020/200928.pdf. Acesso em: 18 nov. 2025.

[106] UNITED STATES. Department of the Treasury. Office of Foreign Assets Control. ***Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments.*** Washington, D.C.: Treasury Department, 1 Oct. 2020. Disponível em: https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020.pdf. Acesso em: 18 nov. 2025.

persecução penal efetiva. Ao reforçar os mecanismos de assistência jurídica mútua e ampliar a cooperação entre os Estados, esses diplomas multilaterais contribuem para uma resposta mais célere, eficiente e compatível com a velocidade das transformações tecnológicas que caracterizam o ciberespaço.

3. UMA ANÁLISE SOB A PERSPECTIVA PENAL

3.1. Leis vigentes no Brasil que regulamentam a internet

A Constituição Federal de 1988[107] consagra um conjunto de princípios estruturantes do sistema jurídico brasileiro, dentre os quais merecem destaque a legalidade e a reserva legal, ambos previstos no artigo 5º. Tais princípios foram instituídos com a finalidade de limitar o poder punitivo estatal, assegurando que apenas condutas expressamente definidas em lei, e resultantes de regular processo legislativo, possam ser consideradas criminosas. Trata-se de garantia essencial ao Estado Democrático de Direito, que impede a criminalização de comportamentos não tipificados e preserva a segurança jurídica.

Conforme assinala Marco Antônio Silva[108], o princípio da legalidade funciona simultaneamente como limite ao poder normativo e ao poder punitivo do Estado, constituindo desdobramento direto da dignidade da pessoa humana, na medida em que protege o indivíduo contra arbitrariedades e assegura previsibilidade quanto às consequências jurídico-penais de seus atos. Essa diretriz constitucional encontra respaldo no artigo 1º do Código Penal[109], que reforça a máxima *nullum crimen, nulla poena sine lege*, ao estabelecer que "não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal".

Dessa forma, a inexistência de previsão legal específica sobre determinada conduta – por mais socialmente reprovável que seja ou por maiores danos que cause a terceiros – impede sua configuração como crime no ordenamento brasileiro. O sistema penal adotado pelo constituinte é, portanto, o da estrita reserva legal, de modo que, na ausência de lei anterior definindo a conduta e cominando pena, é inviável qualquer pretensão punitiva estatal, em observância ao núcleo rígido do princípio da legalidade.

Até o ano de 2012, o Brasil ainda não possuía uma legislação abrangente e específica para tratar dos crimes cibernéticos, bem como não contava com nenhuma disposição legal no ordenamento jurídico que versasse, especificamente, sobre a punição dos crimes cibernéticos próprios, sendo as legislações existentes voltadas, principalmente, aos cibercrimes impróprios.

---

[107] BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil.** Brasília, DF: Senado Federal, 1988.
[108] SILVA, Marco Antônio Marques da Silva. **Acesso à Justiça Penal e Estado Democrático de Direito.** São Paulo: Ed. J. de Oliveira, 2001, p. 07
[109] BRASIL. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. **Código Penal**. Diário Oficial da União: Rio de Janeiro, RJ, 31 dez. 1940.

Antes da real promulgação de novas leis, ao Congresso Nacional já haviam sido apresentadas propostas legislativas voltadas à construção de um marco jurídico mais adequado para o enfrentamento dos crimes cibernéticos.

A primeira iniciativa de maior destaque foi o Projeto de Lei nº 84/1999[110], chamada "Lei dos Crimes Digitais", de autoria do deputado Luiz Piauhylino**,** cujo propósito era tipificar condutas como invasão e modificação indevida de conteúdo de sites, subtração de senhas, criação e disseminação de vírus, entre outras práticas ilícitas no ambiente virtual.

Na sequência, o senador Luiz Estevão apresentou o Projeto de Lei do Senado nº 151/2000[111], propondo a obrigatoriedade de guarda dos registros de conexão dos usuários — medida concebida com o intuito de ampliar a capacidade estatal de rastreamento de atividades online e, consequentemente, facilitar a apuração de delitos informáticos.[112]

Em 2002, sobreveio a promulgação do Código Civil Brasileiro[113], diploma legal que trouxe, em seus artigos 20 e 21 a tutela de garantias ligadas à proteção da personalidade e à responsabilidade civil, absolutamente adaptável e aplicável ao ambiente virtual, eis que são categorias que, mais a frente, se tornariam centrais nas disputas jurídicas envolvendo conteúdos divulgados no ambiente virtual. No entanto, ainda não foi suficiente em promover normativas capazes de responsabilizar e repreender a prática de condutas cibernéticas graves tal qual um ataque cibernético contra infraestruturas críticas.

Em 2008, a Lei nº 11.829/2008[114] representou o primeiro avanço expressivo no tratamento penal de condutas digitais, ao criminalizar a produção, o armazenamento e a divulgação de material pornográfico envolvendo crianças e adolescentes por meio da internet, inaugurando um diálogo mais direto entre o Direito Penal e os novos meios tecnológicos.

---

[110] BRASIL. Câmara dos Deputados. **Projeto de Lei nº 84, de 1999.** Dispõe sobre delitos informáticos. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=16485
. Acesso em: 18 nov. 2025.

[111] **BRASIL. Senado Federal. Projeto de Lei do Senado nº 151, de 2000.** Dispõe sobre a guarda de registros de conexão. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/37677. Acesso em: 21 nov. 2025.

[112] CARNEIRO, Lucas Vitor Vitório; SANTOS, Jackson Novaes; EDLER, Gabriel Octacilio Bohn. **O direito cibernético: o impacto gerado pela lei carolina dieckmann no combate aos crimes virtuais realizados contra as crianças e adolescentes**. Revista Ibero-Americana de Humanidades, Ciências e Educação, v. 8, n. 11, p. 2061-2080, 2022.

[113] BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. **Institui o Código Civil.** Diário Oficial da União: Brasília, DF, 11 jan. 2002.

[114] BRASIL. Lei nº 11.829, de 25 de novembro de 2008. **Altera o Estatuto da Criança e do Adolescente para tipificar crimes informáticos.** Diário Oficial da União: Brasília, DF, 26 nov. 2008.

O passo seguinte, e mais simbólico, foi dado em 2012, com a promulgação da Lei nº 12.737/2012[115], conhecida como "Lei Carolina Dieckmann**"**, que introduziu, pela primeira vez, um tipo penal específico para a invasão de dispositivo informático.

A Lei inseriu o artigo 154-A no Código Penal, criminalizando a conduta de: "invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança", com pena de detenção de 3 meses a 1 ano e multa, majorada se houver obtenção de informações, dados ou comunicações privadas, e agravada quando praticada contra autoridades ou órgãos públicos.

O dispositivo parece ser o que mais se aproxima de uma tipificação de ataque cibernético em sentido técnico, embora ele não alcance o uso de códigos maliciosos complexos, como *ransomware*, que envolvem criptografia e bloqueio de sistemas, e não apenas acesso indevido.

No mesmo ano, a Lei nº 12.735/2012[116] determinou a criação de delegacias especializadas em crimes cibernéticos e orientou a atuação das autoridades policiais, reforçando a repressão estatal.

O marco regulatório mais estruturante do ordenamento brasileiro somente surgiu em 2014, com a vigência do Marco Civil da Internet (Lei nº 12.965/2014)[117], o qual representa uma iniciativa normativa voltada, exclusivamente, à regulação do uso da internet no país. Foi concebido como uma "Constituição da Internet" no Brasil e estabeleceu princípios, garantias, direitos e deveres para usuários e provedores de serviço, disciplinando temas como neutralidade de rede, privacidade, guarda de registros e responsabilidade civil, sem se tratar propriamente de uma norma penal.

No entanto, à luz da criminalização dos ataques cibernéticos, sua relevância é incontestável, pois detalhou procedimentos de segurança e padrões de proteção de dados, aproximando o país de boas práticas internacionais.

Sob uma perspectiva dogmática, o Marco Civil não cria tipos penais, mas fornece os alicerces jurídico-normativos para a persecução penal de condutas praticadas no ambiente digital, ao garantir a guarda de registros, logs e dados essenciais à investigação de crimes informáticos.

---

[115] BRASIL. Lei nº 12.737, de 30 de novembro de 2012. **Dispõe sobre a tipificação criminal de delitos informáticos.** Diário Oficial da União: Brasília, DF, 3 dez. 2012.

[116] BRASIL. Lei nº 12.735, de 30 de novembro de 2012. **Dispõe sobre o combate a crimes cibernéticos e cria delegacias especializadas.** Diário Oficial da União: Brasília, DF, 3 dez. 2012.

[117] BRASIL. *Lei nº 12.965, de 23 de abril de 2014.* ***(Marco Civil da Internet)*****. Dispõe sobre princípios, garantias, direitos e deveres para o uso da Internet no Brasil.** Publicado no DOU de 24 abr. 2014, Seção 1, p. 1–13. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 20 jun. 2025.

Destacam-se, nesse sentido, os artigos 13 e 15 da lei, que impõem aos provedores de aplicação e de conexão a obrigação de manter registros de acesso sob sigilo, por prazos legalmente definidos, resguardando-se, porém, os direitos fundamentais à privacidade e à intimidade.

Essa dimensão instrumental do Marco Civil se mostra crucial para a viabilização da responsabilização penal em crimes como a invasão de dispositivos eletrônicos, interceptação de comunicações, disseminação de *malwares* e golpes eletrônicos, pois sem a coleta e a preservação dos dados eletrônicos, a persecução penal resta prejudicada.[118]

Outro ponto de destaque é a previsão do regime de responsabilização dos provedores de serviço, que, embora centrado na esfera cível, pode gerar reflexos indiretos na esfera penal, sobretudo quando tais agentes agem com dolo eventual ou omissão dolosa que favoreça a prática criminosa. A compreensão da função social da rede também passa a ser relevante, uma vez que a internet, como espaço de exercício de direitos fundamentais, deve ser protegida contra sua instrumentalização para fins ilícitos.

Assim, o Marco Civil configura-se como instrumento normativo de base, que, embora não seja lei penal em sentido estrito, oferece sustentáculo à repressão penal de ataques cibernéticos. Sua estrutura normativa permite a atuação articulada entre as esferas cível, penal e administrativa, tornando-se elemento indispensável à construção de uma política criminal eficaz no ambiente digital.

Portanto, sob uma análise sistemática, o Marco Civil da Internet inaugura um novo paradigma de proteção dos direitos digitais no Brasil, estabelecendo condições normativas que favorecem a efetiva responsabilização penal de condutas lesivas praticadas no ciberespaço, e contribuindo para a consolidação de um arcabouço jurídico coerente e alinhado aos desafios contemporâneos da criminalidade digital.[119]

Em 2015, o Código de Processo Civil (Lei nº 13.105/2015)[120] incorporou regras relevantes à esfera digital, ao disciplinar a responsabilidade civil por conteúdo ofensivo na internet e estabelecer mecanismos formais de retirada de material mediante ordem judicial.

---

[118] CGI.br — Comitê Gestor da Internet no Brasil. ***Marco Civil da Internet (Law of the Internet in Brazil).*** Brasília: CGI.br, 2014. Disponível em: https://www.cgi.br/pagina/marco-civil-law-of-the-internet-in-brazil/180. Acesso em: 20 jun. 2025.

[119] BRASIL. Decreto nº 8.771, de 11 de maio de 2016. **Regulamenta a Lei nº 12.965/2014**. Diário Oficial da União: Brasília, DF, 12 maio 2016.

[120] BRASIL. Lei nº 13.105, de 16 de março de 2015. **Código de Processo Civil.** Diário Oficial da União: Brasília, DF, 17 mar. 2015.

Em 2016, a Lei nº 13.344/2016[121], voltada ao tráfico de pessoas, incluiu expressamente o uso de tecnologias da informação e comunicação como meio de execução, evidenciando o papel da internet no fortalecimento de organizações criminosas transnacionais.

No ano seguinte, a Lei nº 13.441/2017[122] autorizou a infiltração policial virtual em investigações de crimes cometidos contra crianças e adolescentes, representando um avanço importante no campo da persecução penal digital e alinhando o Brasil a modelos já adotados por autoridades internacionais.

Foi em 2018 que a promulgação da Lei Geral de Proteção de Dados (Lei nº 13.709/2018)[123] marcou um divisor de águas. Inspirada em modelos europeus, a LGPD estruturou princípios, bases legais e deveres para o tratamento de dados pessoais por entes públicos e privados, inaugurando uma política nacional de privacidade e instituindo a Agência Nacional de Proteção de Dados como órgão regulador. Trata-se, sem dúvida, da norma mais sofisticada já produzida no país em matéria de proteção de dados e segurança da informação.

No contexto penal, a Lei nº 13.964/2019 (Pacote Anticrime)[124] introduziu a disciplina da cadeia de custódia da prova digital no art. 158-A do Código de Processo Penal, impondo rigor técnico na extração, preservação e tratamento de evidências eletrônicas – aspecto crucial para a responsabilização de autores de ataques cibernéticos.

Em 2020, o Projeto de Lei n. 4.554/2020[125], do Senador Izalci Lucas (PSDB-DF), foi aprovado pelo Senado e implementou alterações no Código Penal (Decreto-Lei 2.848, de 1940) para agravar penas como invasão de dispositivo, furto qualificado e estelionato ocorridos em meio digital, conectado ou não à internet, positivados na Lei nº 14.155/2021[126]**.**

Conforme a nova redação do Código, o crime de invasão de dispositivo informático passou a ser punido com reclusão, de um a quatro anos, e multa, aumentando-se a pena de um terço a dois terços se a invasão resultar em prejuízo econômico. Antes, a pena aplicável era de detenção de três meses a um ano e multa.

---

[121] BRASIL. Lei nº 13.344, de 6 de outubro de 2016. **Dispõe sobre prevenção e repressão ao tráfico de pessoas.** Diário Oficial da União: Brasília, DF, 7 out. 2016.
[122] BRASIL. Lei nº 13.441, de 8 de maio de 2017. **Altera o ECA para permitir infiltração virtual em investigação de crimes contra crianças e adolescentes.** Diário Oficial da União: Brasília, DF, 9 maio 2017.
[123] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Dispõe sobre a proteção de dados pessoais e cria a ANPD. D**iário Oficial da União: Brasília, DF, 15 ago. 2018.
[124] BRASIL. Lei nº 13.964, de 24 de dezembro de 2019. **Aperfeiçoa a legislação penal e processual penal**. Diário Oficial da União: Brasília, DF, 24 dez. 2019.
[125] BRASIL. Lei nº 14.132, de 31 de março de 2021. **Tipifica o crime de perseguição.** Diário Oficial da União: Brasília, DF, 1º abr. 2021.
[126] BRASIL. Lei nº 14.155, de 27 de maio de 2021. **Altera o Código Penal para agravar penas em crimes digitais.** Diário Oficial da União: Brasília, DF, 28 maio 2021.

A penalidade vale para aquele que invadir um dispositivo a fim de obter, adulterar ou destruir dados ou informações sem autorização do dono, ou ainda instalar vulnerabilidades para obter vantagens ilícitas.

A partir do projeto, foi aprovada a Lei nº 14.132/2021[127], tipificando o crime de *stalking*, com previsão expressa de cometimento por meios digitais.

Com a Convenção de Budapeste, a legislação penal brasileira passou a criminalizar condutas como o acesso indevido a sistemas informáticos, interceptação de dados e pornografia infantil, de modo que a lei penal precisou ser ajustada para contemplar integralmente as exigências do tratado. Isso incluiu a incorporação de novos tipos penais e a reformulação de definições ligadas aos crimes cibernéticos.

Somente em 2023, as inovações mais determinantes foram reunidas no Decreto nº 11.491/2023[128], o qual passou a regulamentar a Estratégia Nacional de Cibersegurança e colocou o Brasil, pela primeira vez, dentro de um modelo estruturado de governança cibernética alinhado aos padrões internacionais, estabelecendo diretrizes, objetivos e ações coordenadas para proteger a infraestrutura crítica brasileira, fortalecer capacidades defensivas e promover uma cultura nacional de cibersegurança.

Ao iniciar a análise comparativa, destaca-se o artigo 2º da Seção 1 do referido decreto, que trata do acesso não autorizado a sistemas de informação. A norma estipula que a invasão dolosa a sistemas protegidos, com o objetivo de obter dados ou por qualquer outro meio fraudulento, deve ser considerada crime. Tal previsão guarda correspondência com o artigo 154-A do Código Penal Brasileiro, inserido pela Lei nº 12.737/2012 (Lei Carolina Dieckmann), que tipifica a conduta de invadir dispositivo informático alheio para fins de obtenção, alteração ou destruição de dados.

A legislação nacional também prevê sanções para aqueles que acessam sistemas diversos sem autorização. Essa conduta converge com os objetivos da convenção internacional de coibir o uso ilícito de redes e sistemas de informação.

No tocante à interceptação ilícita, o artigo 3º do Decreto nº 11.491/2023 estabelece a criminalização da interceptação de transmissões de dados não públicas, realizadas com dolo e por meios técnicos, ainda que com propósito fraudulento. A Constituição Federal, em seu artigo 5º, inciso XII, garante a inviolabilidade do sigilo das comunicações, admitindo exceção apenas

[127] BRASIL. Lei nº 14.132, de 31 de março de 2021. **Tipifica o crime de perseguição.** Diário Oficial da União: Brasília, DF, 1º abr. 2021.
[128] BRASIL. Decreto nº 11.491, de 9 de agosto de 2023. **Aprova a Estratégia Nacional de Cibersegurança – E-Ciber.** Diário Oficial da União: Brasília, DF, 10 ago. 2023.

por ordem judicial, reforçada pela Lei nº 9.296/1996, que regula os procedimentos para interceptações telefônicas e telemáticas.

O artigo 7º, Título 2, do decreto, trata da falsificação informática, criminalizando a inserção, exclusão ou modificação de dados com a intenção de produzir efeitos jurídicos enganosos. A legislação brasileira já contemplava situações análogas na Lei nº 109/2009, ao prever punição à criação de documentos informáticos não genuínos com finalidades fraudulentas.

Quanto à fraude informática, o artigo 8º do mesmo decreto tipifica a conduta de causar prejuízo patrimonial por meio de alteração dolosa de dados ou interferência no funcionamento de sistemas. Essa previsão encontra paralelo no artigo 171, §§ 2º-A e 2º-B, do Código Penal, que trata da fraude eletrônica, aumentando a pena quando os atos são praticados com uso de servidores localizados no exterior.

No que se refere à pornografia infantil, o artigo 9º do Título 3 do decreto alinha-se ao disposto nos artigos 240 e 241 do Estatuto da Criança e do Adolescente (Lei nº 11.829/2008), que já previam a criminalização da produção e distribuição de material pornográfico envolvendo menores, inclusive por meios eletrônicos.

As movimentações legislativas mais recentes relativas a condutas virtuais se deram com a regulamentação do mercado de apostas desportivas e jogos *online*, bem como de criptomoedas.

A crescente utilização de criptoativos em esquemas fraudulentos e de lavagem de dinheiro, inclusive em invasões cibernéticas, levou à aprovação da Lei nº 14.478/2022[129], que instituiu o Marco Legal das Criptomoedas e ampliou mecanismos regulatórios sobre prestadores de serviços de ativos virtuais – tema diretamente conectado à sofisticação financeira dos grupos de *ransomware*.

Note-se que a legislação brasileira, apesar de já conter dispositivos alinhados à Convenção de Budapeste, passou a contar com um marco mais coeso e internacionalmente reconhecido apenas em 2023[130], fortalecendo a capacidade de cooperação jurídica internacional e a eficiência na repressão aos delitos cibernéticos.

As últimas décadas revelam uma trajetória legislativa marcada por avanços relevantes, embora ainda incompletos. Apesar de disposições dispersas, o país estruturou um ambiente

[129] BRASIL. Lei nº 14.478, de 21 de dezembro de 2022. **Dispõe sobre diretrizes para prestadores de serviços de ativos virtuais.** Diário Oficial da União: Brasília, DF, 22 dez. 2022.
[130] BRASIL. Decreto nº 11.741, de 2023. Promulga a Convenção sobre o Crime Cibernético (Convenção de Budapeste). Diário Oficial da União: Brasília, DF.

normativo mais robusto para a proteção de dados, a governança da internet e a repressão a crimes digitais.

Todavia, o que se percebe é que as normas até o momento desenvolvidas se atêm a contextos internos e de escala controlada, sendo ainda inexiste norma penal específica para criminalizar ataques de *ransomware* que representem riscos a estruturas nacionais, o que evidencia uma lacuna crítica, especialmente diante do crescimento da modalidade e da transnacionalidade inerente às invasões contemporâneas.

3.2. Ataque cibernético no Brasil

O Brasil consolidou-se, nas últimas décadas, como um dos países mais vulneráveis a ataques cibernéticos no cenário global. Relatórios oficiais do Senado Federal[131] revelam que, apenas em 2024, os prejuízos econômicos decorrentes de crimes cibernéticos no país alcançaram cifras estimadas em 2,3 trilhões de reais, representando o maior impacto financeiro registrado na América Latina.[132]

As pesquisas sugerem que o ambiente digital brasileiro se tornou um vetor privilegiado para a atuação de grupos criminosos altamente organizados.

Segundo a Associação Brasileira das Empresas de *Software*[133], a escalada desses ataques decorre de fatores estruturais: a intensa digitalização de serviços públicos e privados; a expansão da economia digital; a fragilidade de sistemas internos de segurança; e o uso massivo de engenharia social como porta de entrada para dinâmicas avançadas, como *ransomware*, *phishing* e *malware*s de acesso remoto.

Essa realidade evidencia uma assimetria preocupante entre o grau de sofisticação técnica dos ataques e o grau de resiliência das defesas implementadas por organizações brasileiras, especialmente em setores essenciais como saúde, finanças, varejo e infraestrutura crítica.

Relembrando o conceito brasileiro de infraestruturas críticas, essas são “instalações, serviços e bens, cuja interrupção ou destruição provocará sério impacto social, econômico, político, internacional ou à segurança nacional.”

---

[131] https://www12.senado.leg.br/noticias/infomaterias/2025/04/golpes-virtuais-aumentam-e-nao-fazem-distincao-de-idade

[132] FECOMERCIOSP. **Frente parlamentar de cibersegurança é instaurada pelo Senado Federal em alinhamento com o setor produtivo.** São Paulo, 26 mar. 2025. Disponível em: https://www.fecomercio.com.br/noticia/frente-parlamentar-de-ciberseguranca-e-instaurada-pelo-senado-federal-em-alinhamento-com-o-setor-produtivo?. Acesso em: 18 de nov de 2025.

[133] ALMEIDA, João Marcos. **Cibersegurança: desafios humanos na era digital.** Associação Brasileira das Empresas de Software – ABES, 13 nov. 2024. Disponível em: https://abes.org.br/ciberseguranca-desafios-humanos-na-era-digital/. Acesso em: 18 nov. 2025.

Atualmente, as infraestruturas críticas do Brasil incluem setores como energia (elétrica, nuclear, petróleo e gás), transportes (terrestres, aquaviários e aéreos), comunicações, finanças e água, que são vitais para a segurança, soberania e economia do país. A lista detalhada é gerenciada por diversos grupos de trabalho coordenados pelo Gabinete de Segurança Institucional da Presidência da República (GSI)[134].

Na área elétrica, existem, no Brasil, 162 (cento e sessenta e dois) Centros Operacionais, dos quais 36 (trinta e seis) são considerados críticos para o sistema. Estão inclusos no setor, reatores nucleares, redes elétricas, usinas hidrelétricas (Itaipu, Belo Monte e Tucuruí), instalações de petróleo e gás natural, dutos e armazenamento de combustível.

Na área de transportes aéreos, aquaviários e terrestres, estão presentes o Aeroporto de Guarulhos, portos como os de Outeiros, Miramar e o de Santos, bem como rodovias federais.

Nas áreas de comunicação, finanças e água, toda a infraestrutura de telecomunicação, sistemas bancários, saneamento e abastecimento de água são classificadas como críticas.

Por fim, no que tange à defesa, governo digital, biossegurança e bioproteção, o GSI categoriza as estruturas de Programa Nuclear Brasileiro, serviços públicos e aquelas que garantem a segurança biológica como setores basilares nacionais.

Vale relembrar, por oportuno, dois exemplos de casos reais ocorridos no Brasil, que ilustram, com maior clareza, a fragilidade dos sistemas brasileiros contra ataques de *ransonware*.

De acordo com comunicado oficial[135], no dia 03 de novembro de 2020, o Superior Tribunal de Justiça sofreu o que classificou como o mais grave ataque cibernético já perpetrado contra uma instituição pública brasileira. O ataque, posteriormente identificado como *ransomware*, paralisou de imediato o ambiente de rede e exigiu a completa reconstrução da infraestrutura tecnológica do Tribunal. Aproximadamente por 26 horas, nenhum sistema pôde ser manipulado, preservando-se o cenário para a perícia forense conduzida pela Polícia Federal, com apoio do Comando de Defesa Cibernética do Exército e do Serpro.

A retomada das atividades demandou intensa mobilização interna: a Secretaria de Tecnologia da Informação e Comunicação atuou na recuperação dos sistemas, auxiliada por

---

[134] https://www.gov.br/gsi/pt-br/assuntos/seguranca-de-infraestruturas-criticas#:~:text=As%20infraestruturas%20cr%C3%ADticas%20s%C3%A3o%20instala%C3%A7%C3%B5es%2C%20servi%C3%A7os%2C%20bens,comunica%C3%A7%C3%B5es%2C%20energia%2C%20transportes%2C%20finan%C3%A7as%2C%20%C3%A1gua%20e%20defesa.

[135] BRASIL. Superior Tribunal de Justiça. **Comunicado da Presidência – Ataque Cibernético ao STJ.** Brasília, 19 nov. 2020. Disponível em: https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/19112020-Comunicado-da-Presidencia-do-STJ.aspx. Acesso em: 18 de nov de 2025.

empresas de tecnologia e consultorias especializadas, como a própria *Microsoft*, Atos Brasil e *Redbelt Security*, as quais forneceram suporte técnico e reconstruíram sistemas e *backups*.

Em 09 de novembro do mesmo ano, o Sistema Justiça foi restaurado, permitindo a retomada dos julgamentos.

Como resposta preventiva, o Tribunal destacou o reforço das políticas de segurança, incluindo adoção de autenticação em duas etapas, revisão de práticas de acesso e fortalecimento geral da arquitetura de Tecnologia da Informação. Consoante o comunicado, o incidente, aparentemente, impulsionou mudanças estruturais na governança de segurança da informação do Superior Tribunal de Justiça e reforçou a necessidade de adequação contínua à Lei Geral de Proteção de Dados.

Além do episódio sofrido pela Corte Superior, um dos ocorridos mais recentes de ataques a infraestruturas críticas brasileiras se deu ainda no ano corrente, quando foi registrada uma invasão envolvendo a empresa C&M *Software* – provedora de estrutura tecnológica para a operação do sistema de pagamentos instantâneos (PIX) – oportunidade em que centenas de instituições foram afetadas.

O ecossistema do PIX, sistema de pagamentos instantâneos considerado infraestrutura essencial para o funcionamento econômico do país, esteve no centro de um incidente de segurança de grande repercussão após a invasão à empresa C&M *Software*, fornecedora de soluções tecnológicas utilizadas por centenas de instituições financeiras para integrações operacionais e de mensageria com o Banco Central.

A análise técnica divulgada pela Segura Security[136] evidenciou que o ataque teve como vetor inicial a exploração de vulnerabilidades presentes na infraestrutura externa da empresa, permitindo o acesso indevido a ambientes corporativos sensíveis utilizados para o tráfego de dados entre *fintechs*, bancos e o Sistema de Pagamentos Instantâneos.

Embora não tenha havido evidências de comprometimento direto dos sistemas do Banco Central, segundo informações da própria instituição, o episódio demonstrou a elevada interdependência da cadeia tecnológica do PIX, assim como é em diversos outros setores nacionais: a violação de um provedor terceirizado foi suficiente para expor riscos sistêmicos, afetar centenas de instituições simultaneamente e revelar fragilidades estruturais na segurança cibernética do setor financeiro brasileiro.

---

[136] SEGURA SECURITY. **Cyberattack on Brazil's Payment System: Technical Analysis, Timeline, Risks and Mitigation.** 2025. Disponível em: https://segura.security/post/cyberattack-on-brazils-payment-system-technical-analysis-timeline-risks-and-mitigation. Acesso em: 18 de nov de 2025.

O exemplo reacende justamente o debate travado nesta produção acadêmica sobre a necessária proteção das infraestruturas críticas, físicas ou digitais, e sobre a carência de políticas regulatórias mais rígidas para mitigar riscos decorrentes de terceiros, especialmente em sistemas de alta criticidade.

Ainda que os casos mencionados não pareçam representar danos complexos e de grande magnitude, o que se pretende é trazer ao campo da reflexão os impactos de um ataque ainda mais elaborado, nos moldes da *Colonial Pipeline*, a uma infraestrutura brasileira determinante, tal qual a rede de energia.

O que podemos extrair é que esses ataques ultrapassam a esfera privada e produzem efeitos sociais e econômicos de larga escala. A capacidade de desorganizar cadeias logísticas, paralisar serviços essenciais, comprometer dados sensíveis e gerar instabilidade institucional demonstra que o ataque cibernético já não pode ser compreendido como uma mera infração patrimonial, mas como uma ameaça sistêmica à segurança nacional, ante a violação a múltiplos, e incontroláveis, bens jurídicos.

Do ponto de vista legislativo, entretanto, o ordenamento brasileiro, como antecipado no capítulo anterior, ainda carece de um tipo penal específico destinado a enfrentar a complexidade do ataque cibernético de grande proporção em sua concepção contemporânea.

A legislação atual se mostra fragmentada e insuficiente. Por isso, vamos destrinchá-la.

A Lei nº 12.737/2012, já mencionada nesta dissertação como Lei Carolina Dieckmann, tipifica a invasão de dispositivo informático (normal que incluiu o artigo 154-A ao Código Penal). O nome se deu em referência à atriz de televisão que teve sua privacidade devassada, com a invasão de seu computador e divulgação de suas fotos íntimas na Internet, sendo vítima justamente da conduta que se pretende reprimir criminalmente por meio dessa nova lei.

O tipo penal consiste em “invadir dispositivo informático alheio, conectado, ou não, à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita”.

Também configura esse delito a conduta de quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta acima descrita.

Contudo, extrai-se da própria letra da lei que o objeto de proteção normativa está muito mais centralizado no direito constitucional à privacidade e intimidade do que na violação de dispositivo informático, compatibilizando a conduta ao crime cibernético impróprio, no qual a

rede mundial de computadores se torna apenas meio para o alcance da pretensão criminosa – neste caso, a vandalização de dados pessoais/íntimos.

Não à toa, o novo dispositivo foi criado em absoluta conexão com o artigo 154, que criminaliza a violação do segredo profissional e, somados aos artigos 153 e 154-B, integram o capítulo "Dos Crimes Contra a Inviolabilidade dos Segredos", estando destinado a assegurar direitos, e posteriormente dispositivos, pessoais, não sendo capaz de contemplar a complexidade de uma infraestrutura crítica, que está intimamente interligada a direitos e garantias coletivas e estatais.

Retrato disso é que quando se analisa a completude do artigo, há, em seus parágrafos, enfoque específico nas principais figuras/entidades nacionais, como o Presidente da República, governadores e prefeitos, Presidente do Supremo Tribunal Federal, Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal, ou dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal.

Isto é, um ataque praticado por grupos criminosos que não se utilizam da força bruta (entrada manual) mas sim de acessos obtidos fradulentamente (remotos), como as técnicas de *phishing*, que infectam integralmente sistemas de setores basilares, já não estariam abarcados pelo referido dispositivo, deixando a descoberto o principal método acionado em ataques de larga escala.

O Capítulo II do Código Penal, o qual versa sobre os crimes contra a segurança dos meios de comunicação e transporte e outros serviços públicos, poderia, pela sua natureza, sugerir uma proteção suficiente contra ataques cibernéticos nestes setores críticos.

Os artigos 260 a 266 do capítulo tangenciam, mas não capturam o núcleo de ilicitude de ataques que envolvem criptografia forçada, sequestro digital, roubo massivo de dados e, somente então, paralisação de sistemas críticos.

O artigo 266 em especial, referente à interrupção ou perturbação de serviço telegráfico, radiotelegráfico ou telefônico, revela-se um tanto quanto anacrônico diante das arquiteturas digitais modernas, cuja materialidade não se enquadra mais em sistemas de comunicação de natureza analógica.

Ainda que os dispositivos sejam capazes de abarcar os resultados criminosos eventualmente atingidos na prática dos ataques de *ransomware*, como a paralisação de transportes e serviços, a sequência de atos criminosos que envolve a arquitetura do ataque se queda pouco positivada, eis que nem sempre se trata de conduta praticada com o fim claro de atingir tão somente um sistema ferroviário ou de transporte marítimo causando desastres, mas

sim uma cadeia de atos que almeja a exposição e destruição temporária de todo um sistema informatizado, a violação da atividade fim em si, a manutenção de controle ostensivo, e ainda, a obtenção de vantagem econômica.

Outro diploma relevante é a Lei nº 9.983/2000, que incluiu no Código Penal o artigo 313-A, criminalizando a inserção de dados falsos em sistema informatizado, e o artigo 313-B, que trata da modificação ou alteração não autorizada de sistemas ou programas de informática da Administração Pública, com penas de reclusão de 2 a 12 anos. Esses dispositivos tutelam especificamente sistemas públicos, e são frequentemente aplicados em casos de ataques a órgãos estatais, como invasões a portais de tribunais ou sistemas de registros.

Os dispositivos foram inseridos no Título XI do Código Penal "Dos Crimes Contra a Administração Pública", Capítulo I "Dos Crimes Praticados por Funcionário Público Contra a Administração em Geral" que têm o condão de proteger infraestrutura basilar da sociedade, a administração pública. Porém, a partir da leitura da própria norma, extrai-se que a conduta criminalizada é de caráter próprio, eis que só é delituosa se praticada por funcionário público, o qual configura sujeito ativo pré-determinado

> Art. 313-A. Inserir ou facilitar, **o funcionário autorizado**, a inserção de dados falsos, alterar ou excluir indevidamente dados corretos nos sistemas informatizados ou bancos de dados da Administração Pública com o fim de obter vantagem indevida para si ou para outrem ou para causar dano:
> Pena – reclusão, de 2 (dois) a 12 (doze) anos, e multa.
> Modificação ou alteração não autorizada de sistema de informações
> Art. 313-B. Modificar ou alterar**, o funcionário**, sistema de informações ou programa de informática sem autorização ou solicitação de autoridade competente:
> Pena – detenção, de 3 (três) meses a 2 (dois) anos, e multa
> Parágrafo único. As penas são aumentadas de um terço até a metade se da modificação ou alteração resulta dano para a Administração Pública ou para o administrado.

Diante disso, é legislação limitada no que tange a ataques cibernéticos contra infraestruturas críticas, porque, como já trabalhado, são condutas normalmente praticadas por grupos criminosos que se valem, fraudulentamente, de acessos de funcionários e não necessariamente da própria pessoa física.

Em alguns contextos, o artigo 163 do Código Penal (dano qualificado) também poderia ser aplicado, em clara analogia, sobretudo quando há destruição de dados, programas ou equipamentos, especialmente em casos de "*defacement*" (pichação digital)[137] ou sabotagem.

[137] A expressão "pichação digital" não é um termo jurídico formal, mas pode se referir a ações como invasões de sites que danificam ou alteram páginas da web, sites governamentais ou sistema, com a inserção de mensagens não autorizadas, ou, ainda, a disseminação de conteúdo ofensivo como calúnia, injúria ou difamação.

Todavia, o dano qualificado melhor se amolda aos crimes cibernéticos impróprios, condutas na quais a rede mundial de computadores é apenas instrumento para o alcance do resultado criminoso. Claramente, qualquer ataque cibernético, a qualquer sistema informático, gera, ainda que indiretamente, um dano.

O crime do artigo 163 é, em algum grau, suficiente para concretizar uma das finalidades da pena (resposta estatal), mas ainda não satisfaz a necessidade de repressão e proteção dos bens jurídicos dissolvidos nas inúmeras infraestruturas críticas nacionais.

O dano causado em um ataque cibernético como o da companhia *Colonial Pipeline* ultrapassa a ideia de "prejuízo", atingindo esferas sociais, econômicas e políticas com repercussão nacional e internacional. Tudo isso em uma única dinâmica criminosa.

Mesmo a ampliação trazida pela Lei nº 14.155/2021 – que passou a prever a fraude eletrônica, figura específica para condutas realizadas mediante uso de informações fornecidas por redes de computadores, dispositivos eletrônicos ou sistemas semelhantes, para obtenção de vantagem ilícita, com pena de reclusão de 04 a 08 anos e multa – não abarca ataques que não envolvem fraude direta contra uma vítima individual, como aqueles que visam comprometer a disponibilidade, integridade e confiabilidade de redes inteiras.

Essa inovação representou um avanço na tentativa de adequar o sistema penal às condutas de *phishing* (golpes digitais), mas não abrange, por exemplo, a extorsão por bloqueio de sistemas por criptografia, característica central dos ataques de *ransomware*.

Há também o artigo 288 do Código Penal (associação criminosa) e a Lei nº 12.850/2013 (organização criminosa) que são aplicáveis quando o ataque é praticado de forma estruturada, com divisão de tarefas e finalidade de lucro, situação que de fato é comum em grupos cibercriminosos transnacionais.

Entretanto, os dispositivos penalizam a conduta de se unir com o fim único de cometer condutas ilícitas, deixando, a descoberto, a própria prática da invasão e os seus desdobramentos.

Por outro lado, o artigo 10 da Lei nº 9.296/1996 (interceptação de comunicações) e o artigo 10 da Lei nº 12.965/2014 (Marco Civil da Internet) protegem a privacidade e a inviolabilidade das comunicações digitais, sendo aplicáveis a casos de invasão e divulgação indevida de dados pessoais.

A Lei Geral de Proteção de Dados (Lei nº 13.709/2018), estabelece sanções administrativas e responsabilidade civil, funcionando como instrumento de *compliance* cibernético e de prevenção de incidentes de segurança. Em contrapartida, não cria tipos penais capazes de responsabilizar agentes criminosos que ameaçam a governança da internet.

No contexto de lavagem de capitais, o artigo 1º da Lei nº 9.613/1998 acaba por abarcar a ocultação ou dissimulação de valores obtidos também com crimes cibernéticos, especialmente aqueles envolvendo criptoativos provenientes de ataques de *ransomware*, eis que promulgada a lei que reconhece a legitimidade das moedas virtuais.

Contudo, mais uma vez, apenas é suficiente a criminalizar parte do contexto do ataque, quando a extorsão já foi concluída e os agentes criminosos se valem de atos de lavagem para dificultar o rastreio dos valores exigidos e obtidos.

A ratificação da Convenção de Budapeste sobre o Cibercrime pelo Decreto nº 11.491/2023 representou um marco na inserção do Brasil no sistema global de combate ao cibercrime. Porém, o país ainda não internalizou plenamente os mecanismos de preservação célere e cooperação direta previstos nos artigos 16 e 35 da Convenção.

Isabela Donza Corrêa e João Araújo Monteiro Neto[138] sustentam que a adesão formal à Convenção é apenas o "primeiro passo de uma convergência normativa inacabada", pois a criminalização brasileira não se comunica plenamente com os padrões da Organização para a Cooperação e Desenvolvimento Econômico e do Conselho da Europa, o que retarda respostas e inviabiliza o congelamento de ativos digitais, por exemplo.

Sendo assim, o panorama normativo atual permite responsabilizar parcialmente autores de ataques cibernéticos, mas não impede sua ocorrência, nem assegura a punição integral do ciclo delitivo.

Diante de tantos dispositivos que foram atualizados, ao longos dos anos, para que o sistema de normas se adaptasse às novas modalidades virtuais da prática de crimes, é visível que o modelo punitivo brasileiro ainda opera sob categorias clássicas (patrimônio, honra, liberdade individual) que não refletem a lógica dos ataques cibernéticos modernos, caracterizados por alta transnacionalidade, automatização, criptografia avançada, uso de infraestrutura global distribuída, lavagem de dinheiro por criptoativos e economia ilícita.

Dessa inadequação nasce a conclusão mais relevante: o ataque cibernético, em sua forma contemporânea, permanece juridicamente atípico no Brasil, salvo quando incidentalmente enquadrável em figuras penais analógicas, em um verdadeiro conjunto multifacetado de normas, o que viola frontalmente o princípio da legalidade estrita, preconizado no artigo 5º, inciso XXXIX, da Constituição Federal, e compromete a segurança jurídica.

A ausência de um tipo penal específico impede que o Estado brasileiro responda de maneira proporcional e eficiente à magnitude dos danos produzidos pelos ciberataques,

[138] Idem.

especialmente quando direcionados a infraestruturas críticas, redes governamentais ou sistemas essenciais.

Essa lacuna normativa revela um descompasso entre a complexidade dos ataques e a capacidade regulatória do Estado. Os tipos penais vigentes foram construídos para um paradigma anterior aos avanços tecnológicos atuais, que não contempla ataques distribuídos, cadeias globais de *ransomware*, criptografia coercitiva, invasões sistêmicas, destruição de *backups*, vazamento massivo de dados sensíveis e negociações conduzidas em criptomoedas por grupos transnacionais altamente estruturados.

Apesar do mosaico de dispositivos mencionados, o Brasil carece de um tipo penal unificado e sistemático para o ataque cibernético em larga escala, sobretudo no contexto de *ransomware*, *botnets* e invasões coordenadas.

Autores como Alessandro Barreto[139] e Vladimir Aras[140] observam que a "colcha de retalhos" legislativa força o intérprete a recorrer a analogias e à combinação de tipos, o que gera insegurança jurídica e inconsistência na resposta penal.

Para mais, a ausência de um tipo penal específico compromete até mesmo a efetividade da persecução penal e a capacidade de dissuasão do Estado, reforçando a necessidade de atualização legislativa, que deve buscar não apenas repressão, mas também coerência sistêmica com o ordenamento internacional e com a proteção dos bens jurídicos difusos afetados pelos crimes informáticos.

A doutrina de Alessandro Barreto, Karina Kufa e Marcelo Silva é clara ao apontar que o Brasil "atua de modo reativo, fragmentado e setorializado na segurança digital, o que favorece a impunidade".[141]

O resultado é um cenário paradoxal: o Brasil figura entre os países mais atacados do mundo, mas não possui um tipo penal capaz de abranger o núcleo de lesividade do ataque cibernético moderno. Transpondo a dimensão repressiva, a ausência de um tipo penal adequado compromete os mecanismos de cooperação jurídica internacional, vez que a maioria dos tratados e das operações conjuntas depende de harmonização típica entre os Estados envolvidos – o que o Brasil, atualmente, não possui.

---

[139] BARRETO, Alesandro Gonçalves; KUFA, Karina; SILVA, Marcelo Mesquita. ***Cibercrimes e seus reflexos no Direito brasileiro.*** São Paulo: JusPODIVM, 2021. ISBN 978-65-56806-327.

[140] ARAS, Vladimir. ***Investigação e prova nos crimes cibernéticos.*** In: SALGADO, Daniel de Resende; QUEIROZ, Ronaldo Pinheiro (Org.). ***A prova no enfrentamento à macrocriminalidade.*** Salvador: JusPodivm, 2015.

[141] Idem.

Diante desse diagnóstico, a necessidade de criação de um tipo penal específico de ataque cibernético emerge não apenas como questão dogmática, mas como medida indispensável para a proteção da soberania digital, da ordem econômica, da segurança nacional e dos cidadãos brasileiros.

O que se pode concluir a partir disso, ao menos neste primeiro ato, é que os tipos penais próprios para ataques de *ransomware*, *botnets* e sabotagens de infraestrutura devem buscar: estabelecer protocolos nacionais de resposta imediata e integração técnica entre órgãos e instituir a harmonização internacional de procedimentos de preservação e confisco de ativos digitais.

O capítulo final desta dissertação apresentará uma proposta normativo-penal que busca preencher essa lacuna, alinhando o ordenamento jurídico brasileiro às exigências tecnológicas e geopolíticas do século XXI.

Antes de adentrar ao desenvolvimento do tipo penal específico, é interessante ter conhecimento sobre o atual sistema de proteção brasileiro contra ataques/invasões cibernéticas.

O Brasil ainda não conta com normas capazes de criminalizar a magnitude de um ataque em larga escala, mas já há algum tempo tem desenvolvido mecanismos de proteção dos muros cibernéticos nacionais.

A análise da normativa nacional feita por autores como Vladimir Aras[142], Danilo Doneda[143], Carlos Eduardo Teixeira[144] e Carla Mattos[145] revela que, embora o Brasil disponha de um conjunto expressivo de instrumentos estratégicos voltados à segurança da informação e à proteção das infraestruturas críticas, esse arcabouço permanece fragmentado e em constante evolução.

O Brasil estruturou, ao longo da última década, um sistema normativo que busca harmonizar defesa nacional, governança cibernética e proteção de setores essenciais, sempre com ênfase na articulação entre instituições civis e militares.

A Política Nacional de Defesa (PND)[146] figura como ponto de partida desse alinhamento, ao reconhecer explicitamente a centralidade da segurança do espaço cibernético

---

[142] **ARAS, Vladimir.** ***Cooperação jurídica internacional em matéria penal: teoria e prática***. Salvador: JusPodivm, 2020.

[143] **DONEDA, Danilo; LEMOS, Ronaldo.** ***Ensaios sobre proteção de dados, privacidade e governança da informação***. São Paulo: Revista dos Tribunais, 2020.

[144] **TEIXEIRA, Carlos Eduardo da Silva.** ***Cibersegurança e defesa cibernética no Brasil.*** Brasília: Escola Superior de Guerra, 2018.

[145] **MATTOS, Carla; ALVES, Paola.** ***Governança de Segurança da Informação no Setor Público.*** Belo Horizonte: Fórum, 2019.

[146] BRASIL. Ministério da Defesa. *Política Nacional de Defesa*. Brasília: Ministério da Defesa, 2020. Disponível em: https://www.gov.br/defesa/pt-br/assuntos/copy_of_estado-e-defesa/pnd_end_2020.pdf. Acesso em: 27 nov. 2025.

para a soberania e o funcionamento dos sistemas de comando, controle e informação do Estado brasileiro.

Em consonância com a PND, a Estratégia Nacional de Defesa (END)[147] aprofunda essa diretriz ao afirmar que a proteção da população e do território depende da capacidade de vigilância integrada, incluindo o monitoramento do espaço cibernético como área estratégica de interesse nacional. A END ainda estabelece o setor cibernético como uma das três tecnologias essenciais para a defesa, atribuindo ao Exército Brasileiro a condução das capacidades relacionadas à área.

Esse movimento é complementado pela Política Nacional de Inteligência (PNI)[148] e pela Política Nacional de Segurança da Informação (PNSI)[149], que reforçam a necessidade de coordenação entre órgãos federais, compartilhamento seguro de informações e atuação preventiva diante de ameaças que possam comprometer ativos sensíveis.

Na sequência, a Estratégia Nacional de Segurança Cibernética (E-Ciber)[150] é apresentada como documento estruturante, detalhando objetivos, princípios e medidas para elevar a resiliência nacional e fomentar a cooperação com setores público e privado.

Foram instituídos também instrumentos operacionais, como o Plano de Gestão de Incidentes Cibernéticos da Administração Federal (PLANGIC)[151], que fornece diretrizes práticas para resposta, contenção e recuperação em caso de eventos adversos.

---

[147] BRASIL. Ministério da Defesa. ***Estratégia Nacional de Defesa.*** Brasília: Ministério da Defesa, 2020. Disponível em: https://www.gov.br/defesa/pt-br/assuntos/copy_of_estado-e-defesa/pnd_end_2020.pdf. Acesso em: 27 nov. 2025.

[148] BRASIL. Gabinete de Segurança Institucional; Agência Brasileira de Inteligência. ***Política Nacional de Inteligência.*** Brasília: GSI/PR, 2016. Disponível em: https://www.gov.br/abin/pt-br/assuntos/institucional/pni. Acesso em: 27 nov. 2025.

[149] BRASIL. Gabinete de Segurança Institucional. ***Política Nacional de Segurança da Informação.*** Portaria nº 93, de 20 de outubro de 2020. Brasília: GSI/PR, 2020. Disponível em: https://www.gov.br/gsi/pt-br/assuntos/seguranca-da-informacao/politica-nacional-de-seguranca-da-informacao. Acesso em: 27 nov. 2025.

[150] BRASIL. Gabinete de Segurança Institucional. ***Estratégia Nacional de Segurança Cibernética – E-Ciber.*** Brasília: GSI/PR, 2020. Disponível em: https://www.gov.br/gsi/pt-br/assuntos/seguranca-cibernetica/e-ciber. Acesso em: 27 nov. 2025.

[151] BRASIL. Gabinete de Segurança Institucional. ***Plano de Gestão de Incidentes Cibernéticos – PLANGIC.*** Brasília: GSI/PR, 2021. Disponível em: https://www.gov.br/gsi/pt-br/assuntos/seguranca-cibernetica/plangic. Acesso em: 27 nov. 2025.

No âmbito militar, destacam-se ainda a Política Cibernética de Defesa[152] e a Doutrina Militar de Defesa Cibernética[153], que organizam competências, definem níveis de decisão e disciplinam o emprego dual (civil e militar) das capacidades cibernéticas nacionais.[154]

Segundo Emerson Barros Castilho[155], o marco normativo voltado diretamente às infraestruturas críticas é inaugurado pela Política Nacional de Segurança de Infraestruturas Críticas (PNSIC)[156], que consolida o entendimento de que setores como comunicações, energia, transportes, finanças e águas constituem o núcleo sensível da segurança nacional.

A Estratégia Nacional de Segurança de Infraestruturas Críticas (ENSIC)[157], aprovada pelo Decreto nº 10.569/2020, é apresentada como documento orientador central da nova política, definindo objetivos estratégicos distribuídos em quatro eixos – articulação institucional, conscientização e capacitação, fomento a ações e gestão de dados e informações – que guiam a elaboração do Plano Nacional subsequente.

Por fim, o Plano Nacional de Segurança das Infraestruturas Críticas (PLANSIC)[158], promulgado pelo Decreto nº 11.200/2022, operacionaliza essa estrutura normativa ao distribuir competências entre o GSI/PR e os Ministérios setoriais. Entre suas atribuições, o GSI deve acompanhar riscos, implementar o Sistema Integrado de Dados de Segurança, articular-se com entidades nacionais e internacionais e coordenar grupos técnicos responsáveis pela segurança das infraestruturas críticas brasileiras.

No conjunto, o que se observa é a formação de um arcabouço coerente, ainda que disperso, que busca responder à crescente vulnerabilidade do país frente a ataques cibernéticos.

As diretrizes evidenciem avanços importantes – especialmente na consolidação de políticas integradas e no fortalecimento das capacidades de monitoramento e resposta –, porém

---

[152] BRASIL. Ministério da Defesa. ***Política Cibernética de Defesa.*** Portaria Normativa nº 1.266/MD, de 05 de outubro de 2021. Brasília: Ministério da Defesa, 2021. Disponível em: https://www.gov.br/defesa. Acesso em: 27 nov. 2025.

[153] BRASIL. Exército Brasileiro. Comando de Defesa Cibernética. ***Doutrina Militar de Defesa Cibernética.*** Brasília: ComDCiber/EB, 2020. Disponível em: https://www.eb.mil.br/defesa-cibernetica. Acesso em: 27 nov. 2025.

[154] Idem.

[155] CASTILHO, Emerson Barros. **Segurança Cibernética de Infraestruturas Críticas.** Rio de Janeiro: Escola Superior de Guerra, 2022.

[156] BRASIL. Gabinete de Segurança Institucional. ***Política Nacional de Segurança de Infraestruturas Críticas – PNSIC.*** Brasília: GSI/PR, 2018. Disponível em: https://www.gov.br/gsi/pt-br/assuntos/seguranca-de-infraestruturas-criticas/pnsic. Acesso em: 27 nov. 2025.

[157] BRASIL. Decreto nº 10.569, de 12 de dezembro de 2020. ***Aprova a Estratégia Nacional de Segurança de Infraestruturas Críticas.*** Diário Oficial da União, Brasília, 14 dez. 2020. Disponível em: https://www.in.gov.br/en/web/dou/-/decreto-n-10-569-de-11-de-dezembro-de-2020-292391264. Acesso em: 27 nov. 2025.

[158] BRASIL. Decreto nº 11.200, de 7 de setembro de 2022. ***Aprova o Plano Nacional de Segurança de Infraestruturas Críticas***. Diário Oficial da União, Brasília, 8 set. 2022. Disponível em: https://www.in.gov.br/en/web/dou/-/decreto-n-11.200-de-7-de-setembro-de-2022-424112674. Acesso em: 27 nov. 2025.

permanece perceptível a necessidade de evolução normativa, harmonização legislativa e aprofundamento da atuação cooperativa, sobretudo diante da crescente sofisticação das ameaças direcionadas às infraestruturas críticas nacionais.

4. O TIPO PENAL

4.1. Um olhar sobre o processamento penal do ataque de *ransomware*

A persecução penal do *ransomware* no Brasil ilustra a profunda assimetria, já mencionada no capítulo anterior, entre a complexidade técnico-operacional dessas atividades criminosas e o alcance limitado do arcabouço jurídico vigente.

De um lado, os ataques seguem uma verdadeira arquitetura estruturada, que inclui fases de implantação, instalação, comando, controle, destruição e extorsão. De outro, o ordenamento penal brasileiro oferece apenas respostas fragmentadas, tipificando isoladamente partes desse itinerário delitivo – como a invasão de dispositivo informático, a fraude eletrônica, a interrupção e perturbação de serviços essenciais ou, ainda, a destruição de dados.

O resultado é que enquanto o crime opera de forma integrada e sofisticada, a legislação tutela apenas episódios pontuais do *iter criminis*, deixando descobertos exatamente os aspectos mais estratégicos do fenômeno, como a criptografia coercitiva, a negociação extorsiva e a arquitetura transnacional da operação.

A consequência é a resposta reativa, casuística e insuficiente quando o ataque incide sobre infraestruturas críticas e serviços essenciais, com externalidades macroeconômicas e de segurança nacional – ponto já desenvolvido ao longo do trabalho, sobretudo a partir do caso *Colonial Pipeline*.

No contexto processual penal, a partir do momento em que não há norte legislativo no âmbito do direito penal material, reverbera a insegurança normativa identificada na tipificação do delito. A sequência processual natural a todos os crimes positivados na norma penal é a única alternativa que encontra respaldo legal.

Porém, quando se trata da conduta de ataque de *ransomware* contra infraestruturas críticas, o processamento encontra obstáculos que dificultam a própria investigação do ato. O recorte principal dos desafios processuais está no plano probatório, que é, sem sombra de dúvida, o gargalo da persecução criminal da conduta.

O processo penal é um sistema complexo composto por princípios constitucionais, estrutura procedimental, atos das partes e do juiz, regime de nulidades, medidas cautelares, garantias de liberdade, limites estatais, sistema probatório, entre outros institutos.

Diz Aury Lopes Junior[159] que o processo penal não se reduz ao sistema probatório, ainda que a atividade de produção e valoração da prova ocupe posição central na dinâmica processual. A persecução penal é estruturada por um conjunto de regras e princípios constitucionais que conformam e limitam a atuação estatal. Portanto, a finalidade do processo penal não é meramente reconstruir fatos passados, mas assegurar que o exercício do poder punitivo se dê dentro de parâmetros de racionalidade, controle e garantias.

Nesse sentido, o sistema probatório é apenas um dos pilares do processo[160], o qual envolve uma "arquitetura procedimental complexa", não sendo a prova capaz de esgotá-lo.

No entanto, também afirma Aury que a prova pode ser considerada o componente mais sensível do processo penal, sendo o espaço "onde se decide a vida e a liberdade das pessoas", motivo pelo qual recebe o maior grau de proteção e limites, sobretudo na era em que os crimes transpuseram as barreiras físicas, alcançando a realidade virtual.

O filósofo Larry Laudan[161] ensina que todos os sistemas democráticos de justiça penal estão estruturados, em certa ordem, na busca pela descoberta da verdade dos eventos imputados, sendo essa verdade correspondente ao valor teórico de referência externo ao processo, isto é, um ideal regulativo, como afirma Michele Taruffo[162].

Em sendo a prova o instrumento colocado à disposição dos envolvidos para a reconstrução do fato em todas as suas circunstâncias, mostra-se incontornável a necessidade de adequação epistemológica de sua regulamentação, o que demanda que a evidência levada ao processo seja exatamente aquela colhida durante a investigação.

Com esse propósito, foi promovido pelo legislador a disciplina do instituto da cadeia de custódia da prova, por intermédio da Lei n. 13.964/2019, que incluiu os artigos 158-A a 158-F no Código de Processo Penal.

Os dispositivos expõem os amparos conceituais da estrutura de preservação da prova e todo o procedimento que deve ser adotado na manipulação do elemento probatório, concentrado no registro cronológico, atestado, testemunhado e inviolado do caminho percorrido pelo vestígio, desde sua coleta até o momento de sua apresentação processual, garantindo, através da rastreabilidade da prova, a sua autenticidade e idoneidade.

---

[159] LOPES JR., Aury. **Direito Processual Penal**. 21. ed. São Paulo: Saraiva, 2024.
[160] PACELLI, Eugênio; FISCHER, Douglas. **Comentários ao Código de Processo Penal.** 18. ed. São Paulo: Atlas, 2023.
[161] LAUDAN, Larry. ***Verdad, error y proceso penal: un ensayo de epistemología jurídica.*** Madrid: Marcial Pons, 2013.
[162] TARUFFO, Michele. **Uma simples verdade: o juiz e a construção dos fatos.** Trad. Vitor de Paula Ramos. Madrid: Marcial Pons, 2012.

No entanto, os artigos não especificam regras próprias para evidências cibernéticas, o que dificulta a validação judicial de logs, chaves ou registros voláteis. A mutabilidade da evidência digital exige preservação imediata, encadeamento técnico de cadeia de custódia e cooperação internacional tempestiva. Sem esse tripé, a imputação tende a ruir.

A persecução penal de crimes cibernéticos complexos – especialmente ataques de *ransomware* direcionados a infraestruturas críticas – depende de modo decisivo da preservação rigorosa da cadeia de custódia da prova digital. A eminência constante de alta replicabilidade e fácil adulteração das evidências digitais torna essencial que o Estado observe protocolos técnicos capazes de assegurar sua integridade, autenticidade e auditabilidade.

Autores como Furlaneto Neto e Santos[163] demonstram que a prova digital exige procedimentos altamente especializados, sob pena de perda de confiabilidade e consequente inviabilidade probatória no processo penal. Segundo os autores, a cadeia de custódia "tutela a identidade, integridade e autenticidade dos elementos da prova", sendo sua inobservância apta a comprometer o contraditório e gerar nulidades substanciais, sobretudo em crimes que dependem exclusivamente de rastros informacionais para comprovação de autoria e materialidade.

A ruptura, ainda que mínima, da cadeia de custódia da prova digital produz prejuízos praticamente irreparáveis. Denise Provazi Vaz[164] destaca que as características essenciais da prova eletrônica – imaterialidade, volatilidade, suscetibilidade de clonagem e possibilidade de dispersão – tornam-na extremamente frágil a qualquer manipulação não documentada.

Dalla Vecchia[165], por sua vez, observa que, justamente por essa fragilidade intrínseca, a validade forense da prova digital depende da capacidade de demonstrar que os dados analisados refletem fielmente seu estado original, de modo que qualquer interferência indevida destrói a credibilidade do material probatório. Se a cadeia de custódia não for documentada desde o reconhecimento inicial do vestígio, perde-se a possibilidade de rastrear a cronologia das intervenções, impossibilitando auditorias independentes e abrindo espaço para alegações de manipulação, contaminação ou adulteração dos dados.

Esse problema é particularmente agudo nos ataques de *ransomware*, nos quais as evidências se apresentam, com frequência, cifradas, suprimidas ou deliberadamente mascaradas

---

[163] FURLANETO NETO, Mário; SANTOS, José Eduardo Lourenço dos. **Apontamentos sobre a cadeia de custódia da prova digital no Brasil.** Revista Em Tempo, Marília, v. 13, p. 1–16, 2020.

[164] VAZ, Denise Provazi. **Provas digitais no processo penal: formulação do conceito, definição das características e sistematização do procedimento probatório.** 2012. 198 f. Tese (Doutorado em Direito) – Faculdade de Direito, Universidade de São Paulo, São Paulo, 2012.

[165] VECCHIA, Evandro Dalla. **Perícia digital: da investigação à análise forense.** 2. ed. Campinas: Millennium, 2019.

por mecanismos de anti-identificação. Sem documentação contínua e precisa, todo o processo investigativo fica desprovido de fundamento técnico e jurídico.

A quebra da cadeia de custódia repercute diretamente sobre as garantias constitucionais do processo penal. Giacomolli[166] sustenta que a confiabilidade da prova é elemento estruturante do devido processo legal, de modo que a deficiência na preservação dos vestígios compromete o exercício da ampla defesa e torna o processo vulnerável à nulidade. Embora Nucci[167] qualifique a inobservância da cadeia de custódia como causa de nulidade relativa, na prática sua violação pode inviabilizar investigações de criminalidade organizada e transnacional, nas quais a prova digital constitui o único caminho para reconstruir o *modus operandi* dos agentes.

Em razão dessas dificuldades, autores como Machado[168] defendem a necessidade de adoção, no Brasil, da ABNT NBR ISO/IEC 27037:2012[169] como parâmetro técnico de referência para a identificação, coleta, aquisição e preservação da prova digital.

Trata-se do mais importante padrão internacional no campo da forense digital, amplamente utilizado em países com maturidade avançada na investigação de crimes cibernéticos. A norma estabelece requisitos fundamentais, como auditabilidade, justificabilidade, repetibilidade e reprodutibilidade, sem os quais a prova digital não é considerada tecnicamente confiável.

Além disso, diferencia dados voláteis e não voláteis, orienta a ordem adequada de coleta, exige o emprego de ferramentas apropriadas, determina a documentação detalhada de todos os procedimentos adotados e recomenda o uso de funções *hash* para assegurar a integridade dos arquivos.

No contexto de ataques de *ransomware* direcionados a infraestruturas críticas, a importância da cadeia de custódia torna-se ainda mais evidente. Ambientes como sistemas de energia, telecomunicações, transporte, saúde e abastecimento operam com arquiteturas híbridas de Tecnologia da Informação (TI) e Tecnologia Operacional (OT), utilizando redes distribuídas que dependem de sistemas altamente sensíveis, nos quais os dados voláteis podem desaparecer em segundos.

---

[166] GIACOMOLLI, Nereu José. **O devido processo penal: abordagem conforme a Constituição Federal e o Pacto de São José da Costa Rica.** 3. ed. São Paulo: Atlas, 2016.
[167] NUCCI, Guilherme de Souza. **Pacote anticrime comentado: Lei 13.964/2019.** Rio de Janeiro: Forense, 2020.
[168] MACHADO, Leonardo Marcondes. **Aplicação da cadeia de custódia da prova digital.** Revista Consultor Jurídico, 31 mar. 2020. Disponível em: https://www.conjur.com.br/2020-mar-31/academia-policia-aplicacao-cadeia-custodia-prova-digital. Acesso em: 28 nov. 2025.
[169] ABNT – Associação Brasileira de Normas Técnicas. NBR ISO/IEC 27037:2012 – Tecnologia da informação – Técnicas de segurança – Diretrizes para identificação, coleta, aquisição e preservação de evidência digital. Rio de Janeiro: ABNT, 2013.

Langill e Knapp[170] explicam que TI e OT são dois domínios tecnológicos distintos, porém profundamente interligados, especialmente no contexto de infraestruturas críticas. A Tecnologia da Informação (TI) abrange sistemas voltados ao processamento, armazenamento e circulação de dados: servidores, computadores, bancos de dados, redes corporativas, sistemas administrativos, aplicações empresariais e infraestruturas em nuvem. Sua finalidade é sustentar as atividades gerenciais e operacionais da organização, garantindo a integridade, confidencialidade e disponibilidade das informações.

Já a Tecnologia Operacional (OT) compreende sistemas que controlam processos físicos no mundo real, como equipamentos industriais, sensores, atuadores, sistemas de automação, controladores lógicos programáveis, redes industriais e plataformas de supervisão. Esses sistemas são responsáveis por operar e monitorar atividades essenciais, como fluxo de energia, pressão em tubulações, funcionamento de turbinas, automação de linhas industriais e distribuição de insumos críticos, motivo pelo qual sua principal preocupação é a segurança funcional e a continuidade operacional.

Embora historicamente tenham funcionado como ambientes separados, TI e OT tornaram-se crescentemente integrados com a digitalização das infraestruturas críticas. Segundo Andrew Ginter[171], especialista em tecnologia da informação, os sistemas industriais antes isolados passaram a depender de redes corporativas para monitoramento remoto, análise de dados, atualização de software e coordenação logística.

Essa convergência elevou a superfície de ataque, tornando viáveis incidentes cibernéticos capazes de transitar entre os dois domínios. Em ataques de *ransomware*, por exemplo, um comprometimento inicial de TI – via *phishing*, exploração de vulnerabilidade ou credenciais roubadas – pode se estender à OT, levando operadores a desligarem manualmente sistemas físicos por risco de perda de controle, como ocorreu no caso *Colonial Pipeline*.

A interdependência entre esses ambientes implica que um ataque baseado em dados (TI) pode gerar efeitos diretos sobre processos físicos (OT), com potenciais consequências para a segurança, a economia e a continuidade de serviços essenciais.

Essa conexão entre TI e OT impacta profundamente a produção e preservação de vestígios digitais.

---

[170] KNAPP, Eric D.; LANGILL, Joel Thomas. **Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems.** 2. ed. Waltham: Syngress/Elsevier, 2014.

[171] GINTER, Andrew. **Secure Operations Technology: The New Discipline for Protecting Industrial Control Systems.** New York: Waterfall Security Solutions, 2019.

Eoghan Casey[172], um dos mais renomados cientistas da forense digital, em seu estudo "*Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*", trabalha que na TI, os registros relevantes costumam envolver logs de sistema, metadados de arquivos, trilhas de execução, pacotes de rede e rastros de autenticação, os quais tendem a ter maior persistência e são armazenados em estruturas relativamente padronizadas. Na OT, por outro lado, muitos vestígios são altamente voláteis: dados temporários de sensores, estados de controladores industriais, registros de telemetria e parâmetros de operação podem desaparecer com o desligamento dos equipamentos, *reset* automático, falhas de comunicação ou simplesmente pelo ciclo de funcionamento dos dispositivos.

Nessas circunstâncias, a resposta forense precisa ocorrer de modo imediato e tecnicamente preciso, sob pena de perda definitiva de logs, chaves criptográficas, registros temporários de execução, conexões de comando e controle e indicadores de comprometimento.

Cada intervenção deve ser documentada, pois a reconstrução do *iter criminis* digital depende do encadeamento lógico e temporal desses vestígios. Sem isso, torna-se impossível identificar a porta de entrada do ataque, a exploração de vulnerabilidades, a movimentação realizada pelos agentes, a escalada de privilégios no sistema e os vetores de exfiltração ou destruição de dados.

Nesse cenário, a preservação rigorosa da cadeia de custódia não se limita a assegurar a confiabilidade interna da prova digital, mas constitui condição necessária para que a investigação avance para estágios mais complexos de atribuição e desarticulação das estruturas criminosas envolvidas.

Uma vez identificados os vetores técnicos do ataque, a análise forense precisa conectar esses elementos a indicadores de comprometimento amplamente reconhecidos na comunidade internacional de cibersegurança, correlacionando *hashes,* endereços IP, padrões de movimentação e artefatos de *malware* com *modus operandi* previamente registradas em bases globais de inteligência.

Essa correlação depende de vestígios íntegros e auditáveis, pois qualquer inconsistência na documentação dos dados inviabiliza a comparação técnica com registros internacionais e compromete a capacidade do Estado de demonstrar, de forma juridicamente válida, que determinado ataque está associado a um grupo específico ou a uma infraestrutura criminosa transnacional.

---

[172] CASEY, Eoghan. **Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet**. 3. ed. Amsterdam: Elsevier, 2011.

Consequentemente, a responsabilização penal por ataques de *ransomware* exige cooperação internacional, já que a validade da prova compartilhada internacionalmente depende de sua integridade e de sua rastreabilidade, ambas garantidas apenas por uma cadeia de custódia sólida e conforme padrões reconhecidos.

Assim, a preservação adequada dos vestígios digitais não apenas viabiliza a persecução penal interna, mas também possibilita pedidos de assistência jurídica mútua, cumprimento de ordens de bloqueio, identificação de endereços de carteira de criptomoeda utilizados no pagamento de resgate e até correlação de indicadores técnicos com grupos cibercriminosos conhecidos.

No Brasil, o único marco normativo obrigatório aplicável a todas as espécies de vestígios – inclusive digitais no que couber – seguem sendo os já mencionados artigos 158-A a 158-F do Código de Processo Penal.

Como vimos, esses dispositivos possuem natureza essencialmente procedimental e não detalham aspectos metodológicos específicos para a manipulação de evidências tecnológicas, deixando lacunas que precisam ser supridas por padrões técnicos externos à legislação processual penal.

Diante dessa insuficiência normativa, de fato tem se consolidado no país a adoção da ABNT NBR ISO/IEC 27037:2012[173] como principal referência técnica para a identificação, coleta, aquisição e preservação de vestígios digitais. Embora não seja juridicamente obrigatória, a ISO/IEC 27037 tornou-se o padrão de fato utilizado por peritos criminais e especialistas em forense digital, em razão de estabelecer diretrizes internacionalmente reconhecidas sobre integridade, auditabilidade, repetibilidade e reprodutibilidade da prova digital.

A própria Secretaria Nacional de Segurança Pública (SENASP)[174] incorporou essa norma como base metodológica para seus Procedimentos Operacionais Padrões (POPs)[175], que são documentos institucionais que orientam a atuação de equipes policiais e periciais em casos envolvendo dispositivos informáticos. Entretanto, esses procedimentos carecem de padronização nacional e não possuem força normativa vinculante, o que reforça o caráter não unificado da política brasileira de manipulação de vestígios digitais.

---

[173] ABNT. NBR ISO/IEC 27037:2012 – Tecnologia da informação – Técnicas de segurança – **Diretrizes para identificação, coleta, aquisição e preservação de evidência digital**. Rio de Janeiro: Associação Brasileira de Normas Técnicas, 2013.

[174] BRASIL. Ministério da Justiça e Segurança Pública. Secretaria Nacional de Segurança Pública. **Procedimento Operacional Padrão: Perícia Criminal.** Brasília: SENASP, 2013b.
(Documento institucional citado no artigo de Furlaneto Neto e Santos; inclui diretrizes para perícia digital e manuseio de vestígios.)

[175] BRASIL. Ministério da Justiça e Segurança Pública. Secretaria Nacional de Segurança Pública. **Manual de Procedimentos Operacionais Padrão – POP.** Brasília: SENASP, 2013.

Os órgãos persecutórios, por sua vez, têm buscado adaptar-se progressivamente ao fenômeno dos crimes cibernéticos.

A Polícia Federal[176] estruturou centros especializados, como o Centro de Combate a Crimes Cibernéticos, e diversas Polícias Civis estaduais criaram delegacias e núcleos dedicados à investigação digital, como amplamente divulgado no sítio eletrônico do governo brasileiro. Paralelamente, institutos de criminalística investiram na formação de peritos com capacitação específica para atuar em ambientes complexos como redes corporativas, dispositivos móveis, sistemas em nuvem e infraestruturas industriais.

A disseminação de cursos, certificações e treinamentos em análise de *malware*, aquisição forense, resposta a incidentes e rastreamento de criptomoedas demonstra a crescente profissionalização das equipes responsáveis pela persecução penal.

A modernização também alcança o parque tecnológico das instituições, que passaram a empregar ferramentas forenses avançadas – como FTK, EnCase, Magnet AXIOM e Cellebrite – além de bloqueadores de escrita e equipamentos destinados à clonagem forense de dispositivos. Esses recursos permitem maior precisão na aquisição de dados, minimizam a manipulação indevida do vestígio e facilitam a verificação independente por parte da defesa. A adoção sistemática de funções *hash* robustas evidencia a consolidação de boas práticas técnicas compatíveis com padrões internacionais.

A adaptação brasileira aos crimes cibernéticos também se dá no âmbito internacional, dada a natureza transnacional das organizações criminosas envolvidas em ataques de *ransomware*. Embora o Brasil ainda não tenha ratificado a Convenção de Budapeste, a cooperação com órgãos como Interpol, Europol, CISA e FBI tornou-se mais frequente, especialmente por meio de tratados bilaterais de assistência jurídica mútua.

Apesar dos avanços, o Brasil permanece distante de um modelo normativo integralmente estruturado para a prova digital. Furlaneto Neto e Santos destacam que a ausência de regulamentação específica dificulta a padronização operacional e compromete a efetividade da persecução penal.

Machado observa que a dependência exclusiva do Código de Processo Penal é insuficiente para enfrentar a volatilidade, a complexidade e a dinamicidade dos dados digitais, razão pela qual a adoção de normas internacionais deve ser compreendida como etapa transitória rumo à criação de protocolos nacionais unificados.

---

[176] https://www.gov.br/mj/pt-br/assuntos/noticias/policia-federal-cria-unidade-especial-para-intensificar-a-repressao-a-crimes-ciberneticos

Em síntese, o método brasileiro atual depende da conjugação entre legislação processual genérica, padrões técnicos internacionais, diretrizes internas de órgãos públicos e uma crescente especialização de profissionais, compondo um sistema que evolui, mas que ainda carece de consolidação normativa mais robusta e coerente com a complexidade do cenário cibernético contemporâneo.

A conclusão é inequívoca: nos crimes de *ransomware* contra infraestruturas críticas, não existe persecução penal eficaz sem a preservação rigorosa da cadeia de custódia da prova digital. A volatilidade dos vestígios, a sofisticação das táticas empregadas, a rápida dinâmica de destruição de dados e a necessidade de validação técnico-jurídica tornam imprescindível a adoção de protocolos compatíveis com padrões globais e a formação de equipes multidisciplinares altamente especializadas.

Trata-se, portanto, de requisito estrutural para a proteção da soberania digital, da segurança nacional e da continuidade de serviços essenciais à sociedade contemporânea.

Se fosse possível resumir as provocações de Aury Lopes Junior, Michele Taruffo e Ferrajoli e trazê-las à realidade brasileira, eu diria: a lei brasileira tem mais interesse em punir o crime do que em assegurar a prova dele.

Destaque-se que o recorte da presente produção acadêmica não vislumbra a análise de decisões judiciais em crimes cibernéticos, justamente diante da dificuldade que os órgãos persecutórios enfrentam na instauração da própria investigação, ante a infinidade de obstáculos operacionais atrelados à preservação da prova.

Portanto, não foram encontrados nesta pesquisa casos práticos que alcancem julgamentos no âmbito dos tribunais estaduais ou, ainda, superiores, que possam ser utilizados como parâmetro para uma melhor compreensão da persecução penal brasileira dos crimes cibernéticos.

4.2. O tipo penal específico

A compreensão da necessidade de criminalizar de forma específica o ataque de *ransomware* a infraestruturas críticas exige um retorno às bases do conceito de crime em sociedades complexas, eis que vivemos uma realidade em que a materialidade do delito não se manifesta mais por vestígios físicos, mas por sinais voláteis, distribuídos e, frequentemente, intangíveis.

A dogmática clássica identifica o crime como comportamento socialmente intolerável, contrário às tradições e valores de determinada comunidade. Contudo, no ambiente tecnológico

contemporâneo, marcado pela interconexão global e pela dependência de sistemas informacionais essenciais, esse critério tradicional se revela insuficiente. O desvalor da conduta não decorre apenas da violação pontual de um bem jurídico individual, mas de sua capacidade de produzir riscos sistêmicos que ultrapassam fronteiras, setores econômicos e esferas estatais.

No ambiente digital, a conduta ilícita se perfaz no ciberespaço por meio da manipulação de sistemas informáticos, da exploração de vulnerabilidades ou da apropriação indevida de dados, gerando ofensas que repercutem tanto sobre bens individuais – como privacidade e patrimônio – quanto sobre bens coletivos, como segurança da informação e estabilidade operacional de redes essenciais.

Assim, diferentemente do crime clássico, cuja constatação empírica é, em regra, imediata, o fato gerador do crime cibernético se apresenta de maneira difusa e, muitas vezes, apenas não identificável pela análise técnica de metadados, logs e fragmentos digitais que podem desaparecer em segundos.

O *ransomware*, enquanto modalidade de macrocriminalidade digital, exemplifica essa mutação: não se trata apenas de um ataque patrimonial, mas de um fenômeno que compromete a segurança funcional de redes que sustentam atividades vitais à sociedade, interferindo na ordem pública digital e no funcionamento de infraestruturas críticas.

Nesse sentido, a tipificação dessas condutas demanda abordagem própria, pois a dinâmica do cibercrime é estruturalmente distinta da criminalidade analógica. O uso de ferramentas digitais permite a execução de fraudes, invasões, interceptações ilícitas e disseminação de códigos maliciosos sem que o agente precise sequer se aproximar de suas vítimas, o que desloca os parâmetros tradicionais de imputação, materialidade e autoria.

Como observa André Gonçalves[177], o ciberespaço constitui ambiente em permanente mutação, no qual as fronteiras tecnológicas evoluem mais rapidamente do que as estruturas normativas destinadas a regulá-lo, exigindo revisão constante dos instrumentos penais e processuais.

Ademais, o fato gerador não se reduz ao mero acesso não autorizado a sistemas. Ele abrange um espectro amplo de condutas que comprometem privacidade, disponibilidade e integridade de dados, alcançando inclusive a ordem pública digital.

Fábio Ulhoa Coelho[178] destaca que a criminalização no ambiente informacional deve se orientar pela proteção de bens jurídicos fundamentais transpostos ao domínio digital, impondo

[177] GONÇALVES, André. ***Direito Penal Cibernético*.** São Paulo: Thomson Reuters Brasil, 2019.
[178] COELHO, Fábio Ulhoa. **Direito Penal: Parte Geral.** São Paulo: Saraiva, 2020.

ao legislador o dever de precisão normativa para garantir segurança jurídica e proporcionalidade sancionatória.

No Brasil, a legislação penal atual oferece apenas uma proteção fragmentada e incapaz de apreender o desvalor global desse comportamento. Os tipos penais existentes – como os arts. 154-A, 266, 313-A/B, 163 e 171, §2º-A do Código Penal, entre outros vistos nesta produção acadêmica – cobrem apenas parcelas do ataque, alcançando, isoladamente, a invasão, o dano informático, a fraude eletrônica ou a interrupção de serviço.

Entretanto, o *ransomware* combina quatro elementos estruturantes: (i) intrusão; (ii) criptografia ou indisponibilização maliciosa; (iii) sequestro funcional do sistema ou dos dados; e (iv) exigência condicionante, usualmente, econômica.

Nenhum tipo penal vigente incorpora simultaneamente esses elementos. A prática forense reflete essa insuficiência: o Ministério Público e o Judiciário têm recorrido a composições típicas – invasão de dispositivo (154-A) somada a extorsão ou fraude – mas essa solução é apenas contingencial e produz insegurança jurídica.

A sugestão desta dissertação é que a análise da insuficiência legislativa seja conduzida inspirada nas perspectivas propostas por Claus Roxin[179], que concebe o Direito Penal a partir de uma política criminal racional. Seria como estabelecer um tripé, com acento em prevenção, a fim de evitar mera reação a fatos consumados, clareza típica repressiva, com proporcionalidade e segurança jurídica, contemplando também a imprescindibilidade da cooperação internacional frente à criminalidade organizada.

Não obstante Claus Roxin não formule em suas obras um modelo rígido tripartido, sua reflexão sobre política criminal e função do Direito Penal permite extrair esses vetores como exigências funcionais de um sistema penal: de um lado, a necessidade de prevenção racional de riscos, de outro, a repressão proporcional e juridicamente segura, e, por fim, a indispensável articulação com mecanismos de cooperação.

Para Roxin, o Direito Penal moderno não se limita a reagir ao delito consumado, mas deve estruturar-se para prevenir riscos previsíveis em sociedades altamente tecnológicas. A ausência de um tipo penal próprio enfraquece a capacidade de prevenção geral positiva: sem definição normativa clara, o Estado não comunica ao cidadão a expectativa jurídica de punibilidade, e a mensagem preventiva perde eficácia.

---

[179] ROXIN, Claus. **Politica Criminal y Sistema Jurídico-Penal**. Madrid: Civitas, 2000.
ROXIN, Claus. **Problemas Fundamentales de Derecho Penal.** Madrid: Reus, 1981.
ROXIN, Claus. **Derecho Penal. Parte General.** 2. ed. Madrid: Civitas, 1997.

Além disso, o Brasil carece de políticas estruturantes mínimas no campo da segurança cibernética nacional, como padrões de *backup* imutável, requisitos de resiliência e mecanismos unificados de resposta rápida – elementos que conversam intimamente com os ensinamentos de Roxin, quando trata de riscos sistêmicos que demandam "estratégias antecipatórias" do Estado.

A repressão, também é fragilizada. Para Roxin, a repressão criminal legítima depende de clareza tipológica, proporcionalidade e segurança epistêmica. Nesse cenário, o atual mosaico típico brasileiro para condutas cibernéticas acaba por produzir atipicidade parcial: nenhuma figura penal captura a totalidade da conduta, e a investigação enfrenta obstáculos severos devido à volatilidade dos vestígios digitais, à deficiência da cadeia de custódia e à limitada capacidade pericial.

A repressão ainda sofre com a desproporcionalidade entre dano e pena: ataques que paralisam hospitais, tribunais, sistemas de energia ou meios de pagamento acabam tipificados como mero estelionato eletrônico, o que contraria o entendimento de Roxin de que o Estado não pode desconsiderar "lesões massivas a bens jurídicos coletivos".

O terceiro eixo, a cooperação, revela igualmente a insuficiência do modelo brasileiro.

O *ransomware* é estruturalmente transnacional: operações distribuídas, comprometimentos em múltiplas jurisdições, uso de criptomoedas e infraestrutura terceirizada (Ransomware-as-a-Service).

Roxin observa que o Estado contemporâneo é estruturalmente incapaz de enfrentar sozinho a criminalidade organizada internacional, razão pela qual a cooperação passa a ser pressuposto funcional do Direito Penal.

Como apontam Corrêa e Monteiro Neto, a adesão brasileira à Convenção de Budapeste inaugura um processo ainda em consolidação, marcado por uma harmonização normativa incompleta e pela necessidade de ajustes internos para que o país possa atender plenamente às exigências de cooperação e preservação célere de dados previstas no tratado.[180]

Sem alinhamento típico, o Brasil enfrenta entraves operacionais para ordens de preservação, congelamento de criptoativos e assistência jurídica mútua – instrumentos centrais na resposta global ao *ransomware*.

Esse panorama revela que o déficit legislativo brasileiro não é apenas técnico, mas político-criminal. Winfried Hassemer[181] adverte que a intervenção penal só se legitima quando

[180] CORRÊA, Isabela Donza; MONTEIRO NETO, João Araújo. **A adesão do Brasil à Convenção de Budapeste e o enfrentamento do cibercrime.** Revista Direito & TI, 2023.
[181] HASSEMER, Winfried; MUÑOZ CONDE, Francisco. **Introdução à Criminologia e ao Direito Penal.** 2. ed. São Paulo: RT, 2005.

submetida a um controle rigoroso de necessidade, adequação e proporcionalidade — critérios especialmente relevantes quando se trata de bens supraindividuais e de riscos tecnológicos que desafiam a racionalidade da política criminal.

A criminalização de uma conduta socialmente danosa só se justifica quando é indispensável para proteger bens fundamentais.

No caso do *ransomware*, o bem jurídico vulnerado transcende a esfera patrimonial ou a privacidade individual. O que se atinge é a segurança e a integridade de sistemas informáticos essenciais, capazes de sustentar funções vitais do Estado e da sociedade – energia, transporte, saúde, comunicações, finanças.

Sua interrupção gera efeitos em cascata, afetando a continuidade de serviços essenciais, a estabilidade econômica, a segurança pública e a própria soberania digital. Assim, o bem jurídico tutelado pelo tipo penal proposto deve ser compreendido como a segurança informacional sistêmica das infraestruturas críticas, categoria compatível com a dogmática penal que admite a proteção de bens supraindividuais indispensáveis à vida contemporânea.

A literatura técnica corrobora essa necessidade. Allan Liska e Timothy Gallo[182] demonstram como ataques de *ransomware* multifásicos desmontam tipificações penais tradicionais baseadas em delitos isolados.

Bruce Schneier[183] evidencia a assimetria estrutural entre atacantes e defensores e o papel da criptografia aplicada na indisponibilização sistêmica.

Eugene Kaspersky[184] detalha a industrialização do crime por meio de modelos RaaS, revelando que o *ransomware* deixou de ser um ataque artesanal para se tornar uma economia criminosa global. Sem um tipo que una criptografia/indisponibilização e exigência condicionante, o sistema penal permanece incapaz de enfrentar a macrocriminalidade digital.

A volubilidade dos vestígios digitais agrava esse cenário. Ferramentas de anonimização, como criptografia, dificultam a identificação dos autores e a reconstrução do percurso da ação delitiva. A prova digital, por sua própria natureza, é frágil, perecível e altamente dependente de procedimentos técnicos adequados de coleta e preservação.

---

[182] LISKA, Allan; GALLO, Timothy. **Ransomware: defending against digital extortion.** Sebastopol: O'Reilly Media, 2016.

[183] SCHNEIER, Bruce. **Applied Cryptography: protocols, algorithms, and source code in C**. 2. ed. New York: John Wiley & Sons, 1996.

SCHNEIER, Bruce. **Secrets and Lies: digital security in a networked world.** New York: John Wiley & Sons, 2000.

[184] KASPERSKY, Eugene. **Threats, challenges and solutions: the new world of cybercrime.** Moscow: Kaspersky Lab, 2011.

Marcelo Semer[185] destaca que a ausência de evidências físicas e a facilidade de encobrimento das ações ilícitas tornam a persecução penal dos crimes cibernéticos especialmente desafiadora, impondo ao sistema de justiça a necessidade de desenvolver expertise técnica e metodológica compatível com essa nova realidade.

A dimensão coletiva dos danos também não pode ser negligenciada. Como observa Cleber Masson[186], os efeitos dos crimes cibernéticos podem ultrapassar a vítima imediata e gerar impactos econômicos e sociais amplificados, especialmente quando direcionados a setores sensíveis, como o sistema financeiro, serviços essenciais ou infraestruturas críticas. Isso reforça que a resposta penal deve ser pensada de maneira sistêmica, e não restrita a categorias tradicionais de tutela fragmentada.

Essas premissas permitem delinear as bases dogmáticas para um novo tipo penal. A técnica legislativa deve positivar de forma clara o liame funcional que distingue o *ransomware*: o ataque informático com finalidade de criptografar ou tornar indisponíveis dados/serviços, seguido de exigência de vantagem ou condição para restituição.

Essa união não existe no atual Código Penal e é o elemento que explica a ofensividade particular dessa modalidade criminosa. A norma deve prever majorantes coerentes com a gravidade da conduta quando direcionada a infraestruturas críticas, quando provocar risco sistêmico, quando envolver organização criminosa ou dados sensíveis de grande escala. Além disso, a norma deve integrar o ciclo econômico do crime, prevendo punição para a ocultação, conversão ou dissimulação da vantagem obtida – inclusive por meio de ativos virtuais – de forma a facilitar o confisco e o rastreio do dinheiro em linha com as melhores práticas internacionais.[187]

Diante desse panorama, o fato gerador dos crimes cibernéticos deve ser compreendido não apenas como a realização de uma ação típica no ambiente digital, mas como fenômeno que impõe ao Direito Penal a necessidade de adaptação contínua. A tipificação, a coleta e a validação das provas, a cooperação internacional e a proteção de bens jurídicos fundamentais exigem uma arquitetura normativa dinâmica, capaz de responder aos desafios impostos pela cibercriminalidade contemporânea. Em síntese, enfrentar adequadamente esses delitos requer um Direito Penal tecnicamente informado, epistemologicamente consistente e institucionalmente preparado para lidar com um campo em constante transformação.

---

[185] SEMER, Marcelo. **Crimes Cibernéticos e a Efetividade do Direito Penal**. São Paulo: Revista dos Tribunais, 2021.
[186] MASSON, Cleber. **Crimes Cibernéticos: o impacto do uso de tecnologia no Direito Penal.** São Paulo: Método, 2020.
[187] GOMES, Luiz Flávio. **Direito Penal e Criminologia.** São Paulo: Revista dos Tribunais, 2017.

Integrando os três pilares – prevenção, repressão e cooperação – evidencia-se que a criação de um tipo penal específico para *ransomware* não amplia o poder punitivo de forma simbólica, mas corrige um déficit funcional do sistema penal brasileiro e alinha o país aos padrões globais exigidos pela Convenção de Budapeste e pela Estratégia Nacional de Segurança Cibernética (E-Ciber).

A proteção das infraestruturas críticas demanda resposta proporcional à complexidade dos riscos contemporâneos, preservando a racionalidade da política criminal e garantindo segurança jurídica na persecução penal de ataques cibernéticos de alta complexidade.

A partir de todas as premissas discutidas, o texto proposto ao novo tipo penal seria (ANEXO A)

Art. 154-B – (Ataque Cibernético de *Ransomware*)

Atacar, remota ou manualmente, mediante emprego de código malicioso, fraude ou qualquer técnica informática, sistema informatizado público ou privado, com o fim de criptografar, inutilizar, interromper, destruir, subtrair ou tornar inacessíveis dados, programas ou serviços, exigindo, direta ou indiretamente, vantagem econômica ou outra condição para a restituição, desbloqueio, abstenção de divulgação ou restauração do funcionamento:
Pena – reclusão, de 4 (quatro) a 10 (dez) anos, e multa.
§ 1º A pena é aumentada de 1/3 até metade se o crime:
I – Recair sobre infraestrutura crítica;
II – Causar risco ou prejuízo relevante à segurança nacional, econômica, energética, sanitária ou tecnológica;
III – For cometido por organização, associação criminosa ou célula terrorista;
IV – Envolver dados pessoais sensíveis em grande escala.
§ 2º Incorre nas mesmas penas quem oculta, converte ou dissimula, total ou parcialmente, a vantagem obtida, inclusive por meio de ativos virtuais, sem prejuízo da legislação de lavagem de capitais.
§ 3º Aplicam-se, no que couber, os regimes de perda ampliada e de cooperação internacional para identificação, rastreio e confisco de criptoativos.

CONSIDERAÇÕES FINAIS

A análise empreendida ao longo desta dissertação evidenciou que o Brasil se encontra diante de um ponto de inflexão na compreensão e no enfrentamento dos ataques de *ransomware* dirigidos a infraestruturas críticas. Se, de um lado, a globalização tecnológica ampliou exponencialmente a capacidade do Estado e da iniciativa privada de gerir serviços essenciais por meio de estruturas informatizadas, de outro, expôs fragilidades profundas que não podem mais ser negligenciadas.

O primeiro capítulo delimitou o fenômeno do *ransomware* como um problema jurídico-criminal de relevância crescente no cenário global, estabelecendo o pano de fundo tecnológico, econômico e geopolítico que molda a criminalidade cibernética contemporânea.

A reconstrução detalhada do caso *Colonial Pipeline* cumpre dupla função metodológica: (i) ilustra empiricamente o potencial destrutivo de um ataque dirigido a infraestrutura crítica e (ii) demonstra que os efeitos ultrapassam a esfera patrimonial, alcançando setores vitais do Estado.

Assim, este capítulo introduz o caráter sistêmico do *ransomware* e fundamenta, desde o início, a necessidade de um olhar jurídico não fragmentado.

O segundo capítulo aprofundou a compreensão técnica das etapas do ataque cibernético, descrevendo o ciclo completo — desde a intrusão inicial até a extração, criptografia, interrupção de serviços e demanda de resgate. Essa decomposição técnico-operacional é essencial porque evidencia como a conduta é plurissubsistente e multifásica, o que desvela imediatamente a inadequação da tipificação penal atual.

Ao mostrar que o *ransomware* não é um ato isolado, mas um processo estruturado, esse capítulo prepara o terreno para demonstrar que nenhum tipo penal vigente abarca a totalidade da ação delitiva.

O terceiro capítulo deslocou o foco para o sistema jurídico brasileiro, com análise minuciosa da legislação penal e dos instrumentos normativos ligados à segurança da informação, governança cibernética e cooperação internacional. Restou demonstrado que, embora o país disponha de mecanismos administrativos relevantes (Marco Civil, LGPD, E-Ciber, diretrizes de preservação), o arcabouço penal permanece fragmentado e incapaz de responder ao ataque de *ransomware* como fenômeno unitário.

A identificação dessa lacuna é essencial, pois revela a ruptura entre a materialidade técnica do crime e a sua representação jurídico-normativa. A partir daqui a necessidade de criminalização específica deixa de ser hipótese e passa a ser constatação.

O quarto capítulo adentrou o problema da prova digital e da cadeia de custódia, destacando que a volatilidade dos vestígios, a dependência de metadados e a natureza distribuída da infraestrutura tecnológica tornam a investigação de ataques de *ransomware* extremamente delicada.

A articulação com normas internacionais, como a ISO/IEC 27037, e com a estrutura de cooperação da Convenção de Budapeste, revela que, sem integridade probatória, o Estado sequer consegue atingir o patamar mínimo de eficiência repressiva. Assim, este capítulo reforça que o déficit normativo penal não é apenas dogmático: ele compromete a investigação, a cooperação internacional e o rastreamento financeiro — componentes indispensáveis para a persecução do *ransomware*.

O quinto capítulo, que contém a análise dogmática e político-criminal, consolida toda a argumentação anterior. A partir dos ensinamentos de Roxin e Hassemer buscou-se demonstrar que a criminalização moderna exige racionalidade, proporcionalidade e adequação frente aos riscos tecnológicos.

Mostra-se que o bem jurídico vulnerado transcende patrimônio ou privacidade, alcançando a segurança informacional sistêmica do Estado. A partir das bases teóricas, técnicas e empíricas construídas nos capítulos anteriores, este capítulo evidencia de modo definitivo que o ordenamento brasileiro não possui resposta penal coerente ao fenômeno. É neste ponto que a necessidade de tipificação autônoma deixa de ser sugestão e se torna imperativo político-criminal.

O caso *Colonial Pipeline* serviu como paradigma justamente por demonstrar que a vulnerabilidade de um único sistema é capaz de gerar efeitos sistêmicos, transnacionais e imediatos, alcançando economia, segurança energética, estabilidade política e, em última instância, a própria soberania estatal.

O percurso desenvolvido nesta pesquisa revelou que, embora o Brasil tenha avançado em iniciativas de governança cibernética — com normas voltadas à proteção de dados, diretrizes estratégicas de segurança cibernética, estruturas nacionais de resposta e adesão à Convenção de Budapeste — tais medidas ainda não se comunicam com a precisão e a densidade necessárias para permitir uma persecução penal minimamente eficaz.

A legislação penal em vigor, construída para um contexto analógico, demonstra clara insuficiência para abarcar a complexidade das condutas praticadas em ambiente digital, sobretudo aquelas que combinam a indisponibilização de dados, a paralisação de serviços essenciais e a exigência condicionante de pagamento em criptomoedas.

Nesse cenário, tornou-se evidente que o grande obstáculo não reside apenas na criminalização deficiente, mas na própria definição do bem jurídico tutelado. Os ataques de *ransomware* contra infraestruturas críticas desafiam a lógica tradicional do Direito Penal, fundada na proteção de bens individuais ou, quando muito, coletivos delimitáveis.

A invasão massiva a sistemas essenciais compromete simultaneamente o funcionamento do Estado, a continuidade de serviços indispensáveis, a estabilidade econômica e a integridade de dados cuja quebra repercute para além das fronteiras nacionais. Trata-se, portanto, de bens jurídicos de caráter estrutural: a resiliência cibernética estatal e a estabilidade operacional das infraestruturas críticas.

A constatação de que o ordenamento jurídico brasileiro não dispõe de tipo penal específico apto a refletir essa complexidade reforça a necessidade de construção normativa que supere o reducionismo analógico e incorpore elementos objetivos que representem a materialidade do ataque contemporâneo.

Como demonstrado, a tentativa de enquadramento pelos tipos penais existentes – sequestro, extorsão mediante sequestro, estelionato, dano informático, entre outros – conduz a soluções parciais, fragmentadas e incapazes de refletir a realidade técnica da conduta ou as consequências de sua execução. Além disso, não oferecem resposta proporcional ao risco sistêmico envolvido, tampouco mecanismos eficientes de prevenção e repressão.

A ausência de um tipo penal específico também fragiliza a cooperação internacional, elemento imprescindível à persecução de ataques cuja origem frequentemente ultrapassa fronteiras. Sem criminalização clara, o Brasil permanece em desvantagem ao acionar instrumentos de assistência mútua, solicitar preservação de dados, rastrear valores de resgate ou correlacionar indicadores de ataque com grupos criminosos internacionais.

Diante disso, a formulação de um tipo penal dirigido ao ataque de *ransomware* contra infraestruturas críticas não constitui expansão punitiva arbitrária, mas resposta necessária à reconstrução do paradigma normativo de proteção do Estado na era digital. Trata-se de uma criminalização orientada por proporcionalidade e necessidade, fundamentada na defesa de bens jurídicos cuja violação pode comprometer toda a estrutura social, econômica e institucional do país.

O tipo penal proposto nesta dissertação – construído a partir de parâmetros técnicos, da experiência internacional, do estudo das etapas do ataque e da identificação dos bens jurídicos envolvidos – busca tentar preencher esse vazio normativo ao conferir objetividade à conduta, distinguir o ataque comum daquele dirigido a sistemas essenciais e estabelecer gradações de responsabilização compatíveis com o impacto real do delito.

Ademais, a proposta incorpora elementos que dialogam com o processamento penal contemporâneo, como a necessidade de preservação da cadeia de custódia da prova digital, a rastreabilidade dos vestígios e a estruturação de mecanismos que favoreçam a cooperação internacional.

Em síntese, os resultados alcançados demonstram que o Brasil ainda carece de um arcabouço jurídico penal sólido, coerente e tecnicamente orientado para enfrentar ataques de *ransomware* que visam à infraestrutura crítica. O futuro, inevitavelmente digital, exige que o Estado adote postura preventiva e responsiva compatível com o nível de risco que tais condutas representam.

A criminalização adequada não se encerra em si mesma: ela integra um ecossistema maior de governança cibernética, que precisa ser fortalecido por políticas públicas, investimento em tecnologia, capacitação institucional e cooperação internacional contínua.

Conclui-se, portanto, que o país deve avançar no desenvolvimento de mecanismos legais e técnicos que garantam a proteção de suas estruturas basilares, assegurando que a modernização tecnológica seja acompanhada por um Direito Penal capaz de preservar a segurança, a funcionalidade e a autonomia das instituições em uma sociedade cada vez mais dependente do ambiente digital.

O tipo penal proposto constitui apenas um dos passos necessários – mas um passo indispensável – para que o Brasil esteja, de fato, preparado para enfrentar a criminalidade cibernética dos próximos séculos.

REFERÊNCIAS BIBLIOGRÁFICAS

ABNT. NBR ISO/IEC 27037:2012 – Tecnologia da informação – Técnicas de segurança – Diretrizes para identificação, coleta, aquisição e preservação de evidência digital. Rio de Janeiro: Associação Brasileira de Normas Técnicas, 2013.

AFFONSO, Annibal. Você está preparado para a quarta revolução industrial?. Disponível em: https://professorannibal.com.br/2017/05/09/voce-esta-preparado-para-a-quarta-revolucao-industrial/. Acesso em: maio 2024.

ALEMANHA. Strafgesetzbuch (StGB) – Código Penal Alemão, §§ 202a–b, 303a–b (arts. sobre espionagem de dados e sabotagem de computador). Disponível em: https://www.gesetze-im-internet.de/englisch_stgb/. Acesso em: 20 jun. 2025.

ALMEIDA, João Marcos. Cibersegurança: desafios humanos na era digital. Associação Brasileira das Empresas de Software – ABES, 13 nov. 2024. Disponível em: https://abes.org.br/ciberseguranca-desafios-humanos-na-era-digital/. Acesso em: 18 nov. 2025.

ANTAKI, G. A. Piping and Pipeline Engineering: Design, Construction, Maintenance, Integrity, and Repair. 1. ed. Boca Raton: CRC Press (Taylor & Francis Group), 2003. 564 p. ISBN 978-0824709648

ARAS, Vladimir. Cooperação jurídica internacional em matéria penal: teoria e prática. Salvador: JusPodivm, 2020.

ARAS, Vladimir. Investigação e prova nos crimes cibernéticos. In: SALGADO, Daniel de Resende; QUEIROZ, Ronaldo Pinheiro (Org.). A prova no enfrentamento à macrocriminalidade. Salvador: JusPodivm, 2015.

ARAS, Vladimir. O crime de stalking do art. 147-A do Código Penal. Blog do Vlad. Disponível em: https://is.gd/Jur0074. Acesso em: out. 2021.

ARAÚJO, Luís Guilherme N. de. Resenha Vigiar e punir: poder, punição, disciplina e indústria. São Paulo: Editora Primeiros Escritos, 2018.

ARTIFICIAL Intelligence and Gender Equality: key findings of UNESCO's Global Dialogue. UNESCO, set. 2020. Disponível em: https://unesdoc.unesco.org/ark:/48223/pf0000374174. Acesso em: 02 maio 2024.

BACH, Sirlei Lourdes. Contribuição do Hacker para o desenvolvimento da informática. 2001. 135 f. Tese (Doutorado) - Curso de Ciência da Computação, Universidade Federal de Santa Catarina, Florianopolis, 2001.

BARBOSA, André. Constitucionalismo digital e a Lei Geral de Proteção de Dados Pessoais. Revista Jus Navigandi, Teresina, ano 23, n. 5515, 19 atrás. 2018.

BARRETO, Alesandro Gonçalves; KUFA, Karina; SILVA, Marcelo Mesquita. Cibercrimes e seus reflexos no Direito brasileiro. São Paulo: JusPODIVM, 2021.

BASSO, Maristela. Direito da Internet e dos Sistemas de Informação. São Paulo: Saraiva, 2009.

BATES, Jim. Trojan Horse: AIDS Information Introductory Diskette Version 2.0. Virus Bulletin, Oxfordshire, v. 2, n. 1, p. 3-5, jan. 1990. Disponível em: https://www.virusbulletin.com/uploads/pdf/magazine/1990/199001.pdf. Acesso em: 15 jan. 2025.

BEAM, Louis. Leaderless Resistance. The Seditionist, 1992.

BECHARA, Fábio Ramazzini; FLORES, Dímitri Molina. Crimes cibernéticos: qual é o lugar do crime para fins de aplicação da pena e determinação da competência jurisdicional. Revista Direito Mackenzie, v. 13, n. 2, p. 1-21, 2019.

BEERMAN, Jack; BERENT, David; FALTER, Zach; BHUNIA, Suman. A Review of Colonial Pipeline Ransomware Attack. In: IEEE/ACM 23rd International Symposium on Cluster, Cloud and Internet Computing Workshops (CCGridW), 2023, Bangalore, Índia.

BELLAMKONDA, Srikanth. Ransomware Attacks on Critical Infrastructure: A Study of the Colonial Pipeline Incident. International Journal of Research in Computer Applications and Information Technology, v. 7, n. 2, p. 1423-1433, 2024. Disponível em: https://iaeme.com/MasterAdmin/Journal_uploads/IJRCAIT/VOLUME_7_ISSUE_2/IJRCAIT_07_02_110.pdf. Acessado em: 12 nov. 2025.

BIONI, Bruno Ricardo. Proteção de Dados Pessoais: A Função e os Limites do Consentimento. Rio de Janeiro: Forense, 2019.

BOGAGE, Jacob. Colonial Pipeline CEO says paying $4.4 million ransom was ‘the right thing to do for the country’. The Washington Post, Washington, 19 maio 2021.

BRASIL. Câmara dos Deputados. Projeto de Lei nº 84, de 1999. Dispõe sobre delitos informáticos. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=16485. Acesso em: 18 nov. 2025.

BRASIL. Constituição (1988). Constituição da República Federativa do Brasil. Brasília, DF: Senado Federal, 1988.

BRASIL. Decreto N° 3.810, de 2 de maio de 2001, Acordo de Assistência Judiciária em Matéria Penal entre Brasil e Estados Unidos. Disponível em http://www.planalto.gov.br/ccivil_03/decreto/2001/D3810.htm Acesso em: 18 de nov de 2025.

BRASIL. Decreto nº 10.569, de 12 de dezembro de 2020. Aprova a Estratégia Nacional de Segurança de Infraestruturas Críticas. Diário Oficial da União, Brasília, 14 dez. 2020. Disponível em: https://www.in.gov.br/en/web/dou/-/decreto-n-10-569-de-11-de-dezembro-de-2020-292391264. Acesso em: 27 nov. 2025.

BRASIL. Decreto nº 11.200, de 7 de setembro de 2022. Aprova o Plano Nacional de Segurança de Infraestruturas Críticas. Diário Oficial da União, Brasília, 8 set. 2022. Disponível em: https://www.in.gov.br/en/web/dou/-/decreto-n-11.200-de-7-de-setembro-de-2022-424112674. Acesso em: 27 nov. 2025.

BRASIL. Decreto nº 11.491, de 12 de abril de 2023. Promulga a Convenção sobre o Crime Cibernético. Diário Oficial da União, 13 abr. 2023. Disponível em:

https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/d11491.htm e https://legis.senado.leg.br/norma/36966539. Acesso em: 20 jun. 2025.

BRASIL. Decreto nº 11.741, de 2023. Promulga a Convenção sobre o Crime Cibernético (Convenção de Budapeste). Diário Oficial da União: Brasília, DF.

BRASIL. Decreto nº 8.771, de 11 de maio de 2016. Regulamenta a Lei nº 12.965/2014. Diário Oficial da União: Brasília, DF, 12 maio 2016.

BRASIL. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. Código Penal. Diário Oficial da União: Rio de Janeiro, RJ, 31 dez. 1940.

BRASIL. Exército Brasileiro. Comando de Defesa Cibernética. Doutrina Militar de Defesa Cibernética. Brasília: ComDCiber/EB, 2020. Disponível em: https://www.eb.mil.br/defesa-cibernetica. Acesso em: 27 nov. 2025.

BRASIL. Gabinete de Segurança Institucional; Agência Brasileira de Inteligência. Política Nacional de Inteligência. Brasília: GSI/PR, 2016. Disponível em: https://www.gov.br/abin/pt-br/assuntos/institucional/pni. Acesso em: 27 nov. 2025.

BRASIL. Gabinete de Segurança Institucional. Estratégia Nacional de Segurança Cibernética – E-Ciber. Brasília: GSI/PR, 2020. Disponível em: https://www.gov.br/gsi/pt-br/assuntos/seguranca-cibernetica/e-ciber. Acesso em: 27 nov. 2025.

BRASIL. Gabinete de Segurança Institucional. Plano de Gestão de Incidentes Cibernéticos – PLANGIC. Brasília: GSI/PR, 2021. Disponível em: https://www.gov.br/gsi/pt-br/assuntos/seguranca-cibernetica/plangic. Acesso em: 27 nov. 2025.

BRASIL. Gabinete de Segurança Institucional. Política Nacional de Segurança da Informação. Portaria nº 93, de 20 de outubro de 2020. Brasília: GSI/PR, 2020. Disponível em: https://www.gov.br/gsi/pt-br/assuntos/seguranca-da-informacao/politica-nacional-de-seguranca-da-informacao. Acesso em: 27 nov. 2025.

BRASIL. Gabinete de Segurança Institucional. Política Nacional de Segurança de Infraestruturas Críticas – PNSIC. Brasília: GSI/PR, 2018. Disponível em: https://www.gov.br/gsi/pt-br/assuntos/seguranca-de-infraestruturas-criticas/pnsic. Acesso em: 27 nov. 2025.

BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. Institui o Código Civil. Diário Oficial da União: Brasília, DF, 11 jan. 2002.

BRASIL. Lei nº 11.829, de 25 de novembro de 2008. Altera o Estatuto da Criança e do Adolescente para tipificar crimes informáticos. Diário Oficial da União: Brasília, DF, 26 nov. 2008.

BRASIL. Lei nº 12.735, de 30 de novembro de 2012. Dispõe sobre o combate a crimes cibernéticos e cria delegacias especializadas. Diário Oficial da União: Brasília, DF, 3 dez. 2012.

BRASIL. Lei nº 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos. Diário Oficial da União: Brasília, DF, 3 dez. 2012.

BRASIL. Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Dispõe sobre princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Publicado no DOU de

24 abr. 2014, Seção 1, p. 1–13. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 20 jun. 2025.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. (Marco Civil da Internet). Dispõe sobre princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Publicado no DOU de 24 abr. 2014, Seção 1, p. 1–13. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 20 jun. 2025.

BRASIL. Lei nº 13.105, de 16 de março de 2015. Código de Processo Civil. Diário Oficial da União: Brasília, DF, 17 mar. 2015.

BRASIL. Lei nº 13.344, de 6 de outubro de 2016. Dispõe sobre prevenção e repressão ao tráfico de pessoas. Diário Oficial da União: Brasília, DF, 7 out. 2016.

BRASIL. Lei nº 13.441, de 8 de maio de 2017. Altera o ECA para permitir infiltração virtual em investigação de crimes contra crianças e adolescentes. Diário Oficial da União: Brasília, DF, 9 maio 2017.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e cria a ANPD. Diário Oficial da União: Brasília, DF, 15 ago. 2018.

BRASIL. Lei nº 13.964, de 24 de dezembro de 2019. Aperfeiçoa a legislação penal e processual penal. Diário Oficial da União: Brasília, DF, 24 dez. 2019.

BRASIL. Lei nº 14.132, de 31 de março de 2021. Tipifica o crime de perseguição. Diário Oficial da União: Brasília, DF, 1º abr. 2021.

BRASIL. Lei nº 14.155, de 27 de maio de 2021. Altera o Código Penal para agravar penas em crimes digitais. Diário Oficial da União: Brasília, DF, 28 maio 2021.

BRASIL. Lei nº 14.478, de 21 de dezembro de 2022. Dispõe sobre diretrizes para prestadores de serviços de ativos virtuais. Diário Oficial da União: Brasília, DF, 22 dez. 2022.

BRASIL. Ministério da Defesa. Estratégia Nacional de Defesa. Política Nacional de Defesa. Brasília, DF: MD, 2020. Disponível em: https://www.gov.br/defesa/ptbr/assuntos/copy_of_estado-e-defesa/pnd_end_congresso_.pdf. Acesso em: 10 out. 2023.

BRASIL. Ministério da Defesa. Política Cibernética de Defesa. Portaria Normativa nº 1.266/MD, de 05 de outubro de 2021. Brasília: Ministério da Defesa, 2021. Disponível em: https://www.gov.br/defesa. Acesso em: 27 nov. 2025.

BRASIL. Ministério da Justiça e Segurança Pública. Convenção de Budapeste é promulgada no Brasil. Publicado em 17 abr. 2023. Disponível em: https://www.gov.br/mj/pt-br/assuntos/noticias/convencao-de-budapeste-e-promulgada-no-brasil. Acesso em: 20 jun. 2025.

BRASIL. Ministério da Justiça e Segurança Pública. Secretaria Nacional de Segurança Pública. Procedimento Operacional Padrão: Perícia Criminal. Brasília: SENASP, 2013b.

BRASIL. Presidência da República. Glossário de Segurança da Informação. Portaria GSI/PR nº 93, de 18 de outubro de 2021. Dispõe sobre a classificação das infraestruturas críticas nacionais e estabelece diretrizes para sua proteção. Diário Oficial da União: seção 1, Brasília, DF, 20 out. 2021. Disponível em: https://www.gov.br/gsi/pt-br/seguranca-da-informacao-e-cibernetica/glossario-de-seguranca-da-informacao-1 Acesso em: 28 mar 2025.

BRASIL. Senado Federal. Ataques cibernéticos causaram prejuízos de até R$ 2,3 trilhões ao Brasil em 2023, diz especialista. Agência Senado, Brasília, 19 mar. 2024. Disponível em: https://www12.senado.leg.br/noticias/materias/2024/03/19/ataques-ciberneticos-causaram-prejuizos-de-ate-r-2-3-trilhoes-ao-brasil. Acesso em: 20 jun. 2025.

BRASIL. Senado Federal. Projeto de Lei do Senado nº 151, de 2000. Dispõe sobre a guarda de registros de conexão. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/37677. Acesso em: 21 nov. 2025.

Brewer, R. Colonial Pipeline CEO defends $4.4 million ransom payment to hackers. CBS News.

CARNEIRO, Lucas Vitor Vitório; SANTOS, Jackson Novaes; EDLER, Gabriel Octacilio Bohn. O direito cibernético: o impacto gerado pela lei carolina dieckmann no combate aos crimes virtuais realizados contra as crianças e adolescentes. Revista Ibero-Americana de Humanidades, Ciências e Educação, v. 8, n. 11, p. 2061- 2080, 2022.

CASEY, Eoghan. Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. 3. ed. Amsterdam: Elsevier, 2011.

CASTILHO, Emerson Barros. Segurança Cibernética de Infraestruturas Críticas. Rio de Janeiro: Escola Superior de Guerra, 2022.

CETIC.br. Segurança e privacidade na internet: pesquisa TIC Domicílios 2023. São Paulo: CGI.br, 2024. Disponível em: https://cetic.br. Acesso em: 20 jun. 2025.

CGI.br — Comitê Gestor da Internet no Brasil. Marco Civil da Internet (Law of the Internet in Brazil). Brasília: CGI.br, 2014. Disponível em: https://www.cgi.br/pagina/marco-civil-law-of-the-internet-in-brazil/180. Acesso em: 20 jun. 2025.

CHEN, Thomas M.; JAJODIA, Sushil. Cybersecurity: Principles and Practice. 3ª ed. Springer, 2021.

CLARKE, Richard; KNAKE, Robert. Cyber War: The Next Threat to National Security and What to Do About It. Nova York: HarperCollins, 2010.

COELHO, Fábio Ulhoa. Direito Penal: Parte Geral. São Paulo: Saraiva, 2020.

COLONIAL PIPELINE COMPANY. About Us. [S.l.]: Colonial Pipeline, s.d. Disponível em: https://www.colpipe.com/about-us/. Acesso em: 20 jun. 2025.

CONSELHO DA EUROPA. Convenção sobre o crime cibernético (Convenção de Budapeste). Budapeste, 23 nov. 2001. Disponível em: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561. Acesso em: 20 jun. 2025.

CORRÊA, Isadora Donza; MONTEIRO NETO, João Araújo. A adesão do Brasil à Convenção de Budapeste e o enfrentamento do Cibercrime: entre a Cooperação Internacional e a expansão

do Direito Penal. Revista Brasileira de Direito e Tecnologia da Informação, v. 1, n. 16, 2023. Disponível em: https://revista.direitoeti.com.br/RBTI/article/view/160. Acesso em: 20 jun. 2025.

DA SILVA, Patrícia Santos. Direito e crime cibernético: análise da competência em razão do lugar no julgamento de ações penais. Brasília: Vestnik, 2015.

DANTAS, Marcos. Cibersegurança e Políticas Públicas no Brasil: Avanços e Retrocessos. Brasília: Editora UnB, 2020.

DANTAS, Marcos. Cibersegurança no Brasil: O Desafio de Proteger o Ciberespaço Nacional. Revista Brasileira de Cibersegurança, v. 5, n. 2, p. 71-94, 2018.

DE LA CHAPELLE, Bertrand; FEHLINGER, Paul. Internet & Jurisdiction: Jurisdiction on the Internet: From Legal Arms Race to Transnational Cooperation. Internet & Jurisdiction Global Policy Network, abril 2016. Disponível em: https://www.internetjurisdiction.net/uploads/pdfs/Papers/IJ-Paper-Jurisdiction-on-the-Internet.pdf. Acesso em: 18 de nov de 2025.

DIAS, Vinicius Loures Silva. Direito Penal Cibernético: Teoria e Prática no Combate aos Crimes Digitais. São Paulo: JH Mizuno, 2021.

DONEDA, Danilo; LEMOS, Ronaldo. Ensaios sobre proteção de dados, privacidade e governança da informação. São Paulo: Revista dos Tribunais, 2020.

DONEDA, Danilo; MENDONÇA, Marcela Mattiuzzo. Lei Geral de Proteção de Dados Pessoais: Comentada. São Paulo: Thomson Reuters Brasil, 2020.

DUDLEY, Renee; GOLDEN, Daniel. The Ransomware Hunting Team: A Band of Misfits' Improbable Crusade to Save the World from Cybercrime. New York: Macmillan, 2022.

EATON, Collin; VOLZ, Dustin. Colonial Pipeline CEO Tells Why He Paid Hackers a $4.4 Million Ransom. The Wall Street Journal, New York, 19 maio 2021.

ESTADOS UNIDOS. Computer Fraud and Abuse Act (CFAA). Public Law 99 474, 100 Stat. 1213, 16 out. 1986 (18 U.S.C. § 1030). Disponível em: https://www.govinfo.gov/app/details/STATUTE-100/STATUTE-100-Pg1213. Acesso em: 20 jun. 2025.

ESTADOS UNIDOS. Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA). Public Law 117-103, 15 dez. 2022.

ESTADOS UNIDOS. Federal Information Security Modernization Act of 2014 (FISMA). Public Law 113 283, 18 dez. 2014 (atualização da Federal Information Security Management Act de 2002). Disponível em: https://csrc.nist.gov/topics/laws-and-regulations/laws/fisma. Acesso em: 20 jun. 2025.

ESTADOS UNIDOS. Office of Foreign Assets Control — Department of the Treasury. Orientações sobre pagamento de resgates relacionados a entidades sancionadas. Disponível no site do Departamento do Tesouro. Acesso em: 20 jun. 2025.

ESTADOS UNIDOS. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act). Public Law 107 56, 02 out. 2001.

FADIVA, 2014. E-book. Disponível em: http://www.fadiva.com.br/documentos/jusfadiva/2014/18.pdf. Acesso em: 06 abr. 2022.

FECO¬MERCIOSP. Frente parlamentar de cibersegurança é instaurada pelo Senado Federal em alinhamento com o setor produtivo. São Paulo, 26 mar. 2025. Disponível em: https://www.fecomercio.com.br/noticia/frente-parlamentar-de-ciberseguranca-e-instaurada-pelo-senado-federal-em-alinhamento-com-o-setor-produtivo?. Acesso em: 18 de nov de 2025.

FERREIRA, Poliana Agostinho Calheiros; COELHO, Vânia Maria Bemfica Guimarães Pinto. Crimes Virtuais. Varginha:

FLORIDA. Legislature. House Bill 7055: Cybersecurity. Tallahassee: Florida Legislature, 2022. Disponível em: https://www.flsenate.gov/Session/Bill/2022/7055. Acesso em: 18 nov. 2025.

FORNASIER, Mateus de Oliveira; SPINATO, Tiago Protti; RIBEIRO, Fernanda Lencina. Ransomware e cibersegurança: a informação ameaçada por ataques a dados. Revista Thesis Juris–RTJ, São Paulo, v. 9, n. 1, p. 208-236, jan./jun. 2020. http://doi.org/10.5585/rtj.v9i1.16739

FURLANETO NETO, Mário; SANTOS, José Eduardo Lourenço dos. Apontamentos sobre a cadeia de custódia da prova digital no Brasil. Revista Em Tempo, Marília, v. 13, p. 1–16, 2020.

GANDEL, S. The Colonial pipeline ransomware hackers had a secret weapon: Cyber insurance firms. CBS News.

GAWAZAH, Lazarus; RONDLA, Arjun; BALHARETH, Mohammad Saleh A. To Pay or Not to Pay: The US Colonial Pipeline Ransomware Attack. Disponível em: https://www.researchgate.net/publication/383206534_To_Pay_or_Not_to_Pay-_The_US_Colonial_Pipeline_Ransomware_Attack. Acesso em: 28 mar 2025

GIACOMOLLI, Nereu José. O devido processo penal: abordagem conforme a Constituição Federal e o Pacto de São José da Costa Rica. 3. ed. São Paulo: Atlas, 2016.

GINTER, Andrew. Secure Operations Technology: The New Discipline for Protecting Industrial Control Systems. New York: Waterfall Security Solutions, 2019.

GOMES, Luiz Flávio. Direito Penal e Criminologia. São Paulo: Revista dos Tribunais, 2017.

GONÇALVES, André. Direito Penal Cibernético. São Paulo: Thomson Reuters Brasil, 2019.

GONÇALVES, Victor Eduardo Rios. Direito penal: parte especial. Coord. Pedro Lenza. 11. ed. São Paulo: Saraiva Educação, 2021.

GONÇALVES, Victor Eduardo Rios. Direito Penal: Parte Geral e Parte Especial. 2. ed. São Paulo: Saraiva, 2018.

GRECCO, Rogério. Novo crime: Perseguição - art. 147-A do Código Penal. Instituto de Ensino Pesquisa e Atividades de Extensão em Direito, 2021.

GUEIROS, Artur; JAPIASSÚ, Carlos Eduardo. Direito penal: volume único. São Paulo: Atlas, 2018.

GUIDI, Guilherme Berti de Campos; REZEK, Op. Cit. p.276-288, p. 279.

HASSEMER, Winfried; MUÑOZ CONDE, Francisco. Introdução à Criminologia e ao Direito Penal. 2. ed. São Paulo: RT, 2005.

HOBBS, A. (2021). The Colonial Pipeline Hack: Exposing Vulnerabilities in U.S. Cybersecurity. Sage Publications. ISBN 978-1529789768

JAKOBS, Gunther. Ciência do Direito e Ciência do Direito Penal. São Paulo: Manole, 2003. (Coleção Estudos de Direito Penal, v. 1). Tradução: Maurício Antônio Ribeiro Loppes.

KASPERSKI, Alexandre; CAMPOS, Edilson Vitorelli. Direito e Inteligência Artificial: Aspectos Éticos e Jurídicos. Curitiba: Juruá Editora, 2020.

KNAPP, Eric D.; LANGILL, Joel Thomas. Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems. 2. ed. Waltham: Syngress/Elsevier, 2014.

KONRAD, A. U.S. recovers millions in cryptocurrency paid to Colonial Pipeline ransomware hackers. CNBC. Disponível em: https://www.cnbc.com/2021/06/07/us-recovers-millions-incryptocurrency-paid-to-colonial-pipeline-ransomware-hackers.html. Acessado em: 28 out 2025.

LAI, Sauvei; MOURÃO, Pedro Borges. Lei 14.155/2021 dos crimes cibernéticos. CONAMP: Associação Nacional dos Membros do Ministério Público, 2021. Disponível em: https://www.conamp.org.br/publicacoes/artigos-juridicos/8468-lei-14-155-2021-dos-crimes-ciberneticos.html.

LAUDAN, Larry. Verdad, error y proceso penal: un ensayo de epistemología jurídica. Madrid: Marcial Pons, 2013.

LEVITT, Matthew; RICHTER, Ariel. Lone Wolf Terrorism: Policy Paper. Washington, DC: Washington Institute for Near East Policy, 2019.

LIMA, Renato Brasileiro de. Manual de processo penal: volume único. 8. ed. rev., ampl. e atual. Salvador: JusPodivm, 2020.

LISKA, Allan; GALLO, Timothy. Ransomware: Defendendo-se da Extorsão Digital. Tradução de Lúcia A. Kinoshita. 1. ed. São Paulo: Novatec, 2017. ISBN 978-85-7522-551-6. Disponível em: https://books.google.com.br/books?hl=pt-BR&lr=&id=gf6ZDwAAQBAJ&oi=fnd&pg=PT4&dq=tudo+sobre+ransomware&ots=SG-jELbn2D&sig=psdr924270DhngNSeEOQwoWbuRc&redir_esc=y#v=onepage&q=tudo%20sobre%20ransomware&f=false

LOPES JR., Aury. Direito Processual Penal e sua Conformidade Constitucional. São Paulo: Saraiva, 2019.

LUBIN, Asaf. Cyber Plungers: Colonial Pipeline and the Case for an Omnibus Cybersecurity Legislation. Georgia Law Review, v. 57, p. 1605-1674, 2023. Disponível em: https://www.repository.law.indiana.edu/facpub/3082/. Acessado em: 12 nov. 2025.

MACHADO, Leonardo Marcondes. Aplicação da cadeia de custódia da prova digital. Revista Consultor Jurídico, 31 mar. 2020. Disponível em: https://www.conjur.com.br/2020-mar-31/academia-policia-aplicacao-cadeia-custodia-prova-digital. Acesso em: 28 nov. 2025.

MARTINS, João Pedro; SILVA, Ana Carolina; PEREIRA, Lucas. Ransomware attacks and the protection layer on government systems. Núcleo do Conhecimento, [S.l.], 30 mar. 2022. Disponível em: https://www.nucleodoconhecimento.com.br/technology-en/ransomware-attacks. Acesso em: 28 mar. 2025.

MASSON, Cleber. Crimes Cibernéticos: o impacto do uso de tecnologia no Direito Penal. São Paulo: Método, 2020.

MATTOS, Carla; ALVES, Paola. Governança de Segurança da Informação no Setor Público. Belo Horizonte: Fórum, 2019.

MENDES, Gilmar Ferreira; FERNANDES, Victor Oliveira. Constitucionalismo digital e jurisdição constitucional: uma agenda de pesquisa para o caso brasileiro. Revista Brasileira de Direito, Passo Fundo, v. 16, n. 1, p. 1-33, jan./abr. 2020.

MENDES, Gilmar Ferreira; FREITAS, Matheus Pimenta de. Constituição, Direito Penal e Novas Tecnologias. 1. ed. Brasília: Almedina, 2024.

MINISTÉRIO DA JUSTIÇA. Manual de Cooperação Jurídica Internacional. Matéria Penal e Recuperação de Ativos. 4. ed. Brasília, 2019. Disponível em: https://www.gov.br/mj/pt-br/assuntos/sua-protecao/lavagemdedinheiro/institucional-2/publicacoes/manuais/cooperacao-juridica-internacional-em-materia-penal/manualpenalonline-final-2.pdf. Acesso em: 18 de nov de 2025.

NORTH CAROLINA. General Assembly. Session Law 2021-180 (House Bill 105): An Act to Enact the State Budget Act. Raleigh: NCGA, 2021. Disponível em: https://www.ncleg.gov/BillLookup/2021/H105. Acesso em: 18 nov. 2025.

NUCCI, Guilherme de Souza. Pacote anticrime comentado: Lei 13.964/2019. Rio de Janeiro: Forense, 2020.

O'NEIL, Cathy. Algoritmos de Destruição em Massa: Como o Big Data Aumenta a Desigualdade e Ameaça a Democracia. Tradução: Rafael Abraham. 1. ed. São Paulo: Rua do Sabão, 2020.

OLIVEIRA, Anderson Soares Furtado. Crime por Meios Eletrônicos. Brasília: Universidade Gama Filho, 2009.

OLORUNLANA, Taiwo Justice; MOHAMMED, Hamdiya. Analysis of the Colonial Pipeline Cybersecurity Incident. International Journal of Science, Architecture, Technology, and Environment, v. 2, n. 4, abr. 2025.

PACELLI, Eugênio; FISCHER, Douglas. Comentários ao Código de Processo Penal. 18. ed. São Paulo: Atlas, 2023.

PINHEIRO, Vinicius Marques de Carvalho. Marco Civil da Internet Comentado. São Paulo: Saraiva, 2015.

PIOTTO, Danilo. Crimes Eletrônicos: O Direito Penal na Era Digital. Rio de Janeiro: Lumen Juris, 2016.

PIRES JÚNIOR, Paulo Abrão. O papel da cooperação jurídica internacional. In: Manual de cooperação jurídica internacional e recuperação de ativos. Secretaria Nacional da Justiça. 2. ed. Brasília, 2012, p. 17.

REINO UNIDO. Computer Misuse Act 1990. Cap. 18. Londres: Secretaria de Estado do Reino Unido, 1990. Disponível em: https://www.legislation.gov.uk/ukpga/1990/18. Acesso em: 20 jun. 2025.

REUTERS. Colonial Pipeline CEO acknowledges paying hackers to restore pipeline. 19 maio 2021.

ROXIN, Claus. Derecho Penal. Parte General. 2. ed. Madrid: Civitas, 1997.

ROXIN, Claus. Política Criminal e Sistema Jurídico-Penal. São Paulo: RT, 2000.

ROXIN, Claus. Problemas Fundamentales de Derecho Penal. Madrid: Reus, 1981.

RUSSELL, Stuart; NORVIG, Peter. Artificial Intelligence: A Modern Approach. 4ª ed.

Pearson, 2021. Disponível em: https://dl.ebooksworld.ir/books/Artificial.Intelligence.A.Modern.Approach.4th.Edition.Peter.Norvig.%20Stuart.Russell.Pearson.9780134610993.EBooksWorld.ir.pdf. Acessado em: 14 set 2025.

SANGER, David E.; PERLROTH, Nicole. Pipeline attack yields urgent lessons about U.S. cybersecurity: the hack underscored how vulnerable government and industry are to even basic assaults on computer networks. New York Times, New York, 14 May 2021. Disponível em: https://www.nytimes.com/2021/05/14/us/politics/pipelinehack.html. Acesso em: 13 jan 2025.

SCHNEIER, Bruce. Applied Cryptography: Protocols, Algorithms, and Source Code in C. 2. ed. New York: John Wiley & Sons, 1996. ISBN 978-1119096726.

SCHNEIER, Bruce. Secrets and Lies: Digital Security in a Networked World. New York: John Wiley & Sons, 2000. ISBN 978-1119092438.

SCHWAB, Klaus; DAVIS, Nicholas. Aplicando a Quarta Revolução Industrial. Tradução de Daniel Moreira Miranda. São Paulo: Edipro, 2018.

SCHWAB, Klaus. A quarta revolução industrial. Tradução de Daniel Moreira Miranda. São Paulo: Edipro, 2016.

SEGURA SECURITY. Cyberattack on Brazil’s Payment System: Technical Analysis, Timeline, Risks and Mitigation. 2025. Disponível em: https://segura.security/post/cyberattack-on-brazils-payment-system-technical-analysis-timeline-risks-and-mitigation. Acesso em: 18 de nov de 2025.

SEMER, Marcelo. Crimes Cibernéticos e a Efetividade do Direito Penal. São Paulo: Revista dos Tribunais, 2021.

SHEA, Chris. White House: Arrested Russian hacker was behind Colonial Pipeline attack. The Record, 14 jan. 2022. Disponível em: https://therecord.media/biden-official-one-of-arrested-russian-hackers-carried-out-the-colonial-pipeline-attack. Acesso em: 28 mar. 2025.

SILVA, Marco Antônio Marques da Silva. Acesso à Justiça Penal e Estado Democrático de Direito. São Paulo: Ed. J. de Oliveira, 2001, p. 07

SILVA, Marco Aurélio Barbosa da. Cibercrimes: Aspectos Jurídicos e Técnicos. 2. ed. São Paulo: Revista dos Tribunais, 2017.

SOUZA, C. A. Cibersegurança no Brasil: Análise das Políticas Públicas e da Infraestrutura. Revista de Direito e Tecnologia, v. 20, n. 3, p. 33-55, 2019.

SOUZA, C. A. Privacidade e Segurança Cibernética: Desafios para o Brasil. Rio de Janeiro: Editora FGV, 2017.

SOUZA, C. A.; RIBEIRO SILVA, G.; DANTAS, M. Reflexões sobre a Cibersegurança Brasileira: Política, Desafios e Perspectivas. Revista Brasileira de Estudos em Tecnologia e Direito, v. 6, n. 1, p. 102-118, 2022.

SOUZA, Carlos Eduardo de Oliveira. A defesa das infraestruturas críticas brasileiras à luz dos normativos e dos objetivos do Exercício Guardião Cibernético: uma análise construtiva. 2021. 85 f. Trabalho de Conclusão de Curso (Bacharelado em Ciências Militares) — Escola de Guerra Naval, Rio de Janeiro, 2021. Disponível em: https://www.marinha.mil.br/egn/sites/www.marinha.mil.br.egn/files/TCM%20-%20Carlos%20Eduardo%20de%20Oliveira%20Souza.pdf. Acesso em: 28 mar. 2025.

STALLINGS, William. Cryptography and Network Security: Principles and Practice. 8. ed. Boston: Pearson, 2023.

TARUFFO, Michele. Uma simples verdade: o juiz e a construção dos fatos. Trad. Vitor de Paula Ramos. Madrid: Marcial Pons, 2012.

TEIXEIRA, Carlos Eduardo da Silva. Cibersegurança e defesa cibernética no Brasil. Brasília: Escola Superior de Guerra, 2018.

TROTTA, Sandro Brescovit; FERREIRA, Luciano Vaz. Cooperação jurídica internacional em matéria penal: contornos históricos. Sistema Penal & Violência, v. 5, n. 1, 2013.

UNITED KINGDOM. Cabinet Office. Public Sector Ransomware Payments Ban: Consultation Document. London: Cabinet Office, Jan. 2025. Disponível em: https://www.gov.uk/government/consultations/public-sector-ransomware-payments-ban. Acesso em: 18 nov. 2025.

UNITED STATES. Congress. Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA). Washington, D.C., 2022. Disponível em: https://www.congress.gov/bill/117th-congress/senate-bill/3600. Acesso em: 12 nov. 2025.

UNITED STATES. Department of Homeland Security; Cybersecurity and Infrastructure Security Agency. Cyber Safety Review Board FAQs. January 24 2024. Disponível em: https://www.cisa.gov/sites/default/files/2024-01/CSRB%20FAQs%202024.01.24_508c.pdf. Acessado em: 18 nov. 2025.

UNITED STATES. Department of the Treasury. Office of Foreign Assets Control. Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments. Washington, D.C.: Treasury Department, 1 Oct. 2020. Disponível em: https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020.pdf. Acesso em: 18 nov. 2025.

UNITED STATES. Federal Bureau of Investigation. Ransomware Prevention and Response for CISOs. Washington, D.C.: FBI, 2020. Disponível em: https://www.ic3.gov/Media/News/2020/200928.pdf. Acesso em: 18 nov. 2025.

UNITED STATES. The White House. Executive Order 14028: Improving the Nation's Cybersecurity. Washington, D.C., 12 may 2021. Disponível em: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/. Acesso em: 12 nov. 2025.

UNITED STATES. The White House. Fact Sheet: Biden-Harris Administration Convenes Fourth Global Gathering to Counter Ransomware. Washington, D.C.: The White House, 02 out. 2024. Disponível em: https://www.presidency.ucsb.edu/documents/fact-sheet-biden-harris-administration-convenes-fourth-global-gathering-counter-ransomware. Acessoado em: 18 nov. 2025.

UNITED STATES. Transportation Security Administration. Security Directive Pipeline-2021-01 (SD-01) and Pipeline-2021-02 (SD-02): Enhancing Pipeline Cybersecurity Requirements. Washington, D.C., 2021. Disponível em: https://www.tsa.gov. Acesso em: 12 nov. 2025.

VAZ, Denise Provazi. Provas digitais no processo penal: formulação do conceito, definição das características e sistematização do procedimento probatório. 2012. 198 f. Tese (Doutorado em Direito) – Faculdade de Direito, Universidade de São Paulo, São Paulo, 2012.

VECCHIA, Evandro Dalla. Perícia digital: da investigação à análise forense. 2. ed. Campinas: Millennium, 2019.

WENDT, Emerson; GUEIROS, Guilherme. Ransomware 360°: Abordagens Multidisciplinares da Extorsão Criptoviral. 1. ed. São Paulo: Opice Blum Academy, 2021.

WHELAN, Chad; BRIGHT, David; MARTIN, James. Reconceptualising organised (cyber)crime: The case of ransomware. Journal of Criminology, v. 57, n. 1, p. 45-61, 2024. Disponível em: https://journals.sagepub.com/doi/10.1177/26338076231199793. Acesso em: 18 de nov de 2025.

GLOSSÁRIO

Android: Sistema operacional móvel de código aberto desenvolvido pelo Google, amplamente utilizado em dispositivos móveis.[188]

Backdoors: Mecanismos ocultos em sistemas que permitem acesso remoto não autorizado, normalmente utilizados para manter persistência após a invasão inicial.[189]

Backup: Procedimento de cópia de segurança de dados, destinado à recuperação de informações em caso de falhas, ataques ou perdas acidentais.[190]

Bitcoin: Criptomoeda descentralizada baseada em tecnologia *blockchain*, utilizada como meio de pagamento digital sem intermediação de autoridades centrais, amplamente empregada em crimes de *ransomware.*[191]

Bots: Programas automatizados capazes de executar tarefas repetitivas de forma autônoma, frequentemente utilizados em ataques coordenados, como envio massivo de *spam*.[192]

Cellebrite: Tecnologia forense especializada na extração de dados de dispositivos móveis, empregada por órgãos de persecução penal em todo o mundo.[193]

Colonial Pipeline Company: Empresa norte-americana do setor de energia, responsável por um dos maiores oleodutos dos Estados Unidos, alvo em 2021 de um ataque de ransomware que impactou severamente o abastecimento de combustíveis no país.[194]

Criptografia: Conjunto de técnicas matemáticas destinadas a proteger informações por meio da transformação de dados legíveis em dados cifrados, garantindo confidencialidade, integridade e autenticidade.[195]

DarkSide (DarkSid): Organização criminosa especializada em *Ransomware-as-a-Service* (RaaS), responsável pelo ataque à *Colonial Pipeline*, operando mediante modelo de afiliação entre desenvolvedores e executores dos ataques.[196]

---

[188] GOOGLE. **Android developer documentation.** Mountain View: Google LLC, s.d. Disponível na documentação oficial do sistema operacional Android.
[189] NIST – NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **Guide to Malware Incident Prevention and Handling** *(SP 800-83)*. Gaithersburg: NIST, 2013.
[190] NIST – NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **Contingency Planning Guide for Federal Information Systems** (SP 800-34). Gaithersburg: NIST, 2010.
[191] ANTONOPOULOS, Andreas M. Mastering **Bitcoin: unlocking digital cryptocurrencies.** Sebastopol: O'Reilly Media, 2015.
[192] CERT.BR. **Cartilha de segurança para internet.** São Paulo: NIC.br, 2023.
[193] Cellebrite. **Digital intelligence platform overview.** Petah Tikva: Cellebrite, s.d.
[194] UNITED STATES. **Department of Justice. Investigation on the Colonial Pipeline ransomware attack**. Washington, 2021.
[195] STALLINGS, William. **Cryptography and network security: principles and practice.** 7. ed. Boston: Pearson, 2017.
[196] EUROPOL. **Internet organised crime threat assessment (IOCTA)**. Haia, 2021.

Dark Web: Porção da Deep Web acessível apenas por meio de *softwares* específicos, caracterizada pelo anonimato das comunicações e frequentemente associada a mercados ilícitos, crimes cibernéticos e trocas de dados anonimizadas.[197]

Deep Web: Conjunto de conteúdos existentes na internet que não são indexados por mecanismos de busca convencionais, como Google ou Bing, abrangendo bancos de dados privados, intranets, conteúdos protegidos por login e sistemas restritos.[198]

Descriptografia: Processo inverso da criptografia, consistente na conversão do dado cifrado novamente em sua forma original, mediante uso de chave apropriada.[199]

EnCase: Ferramenta forense amplamente utilizada para coleta, preservação e análise de evidências digitais em investigações criminais.[200]

Fake News: Conteúdos deliberadamente falsos, divulgados com aparência de notícia jornalística, com o objetivo de desinformar, manipular a opinião pública ou obter vantagem política ou econômica.[201]

Firewalls: Dispositivos ou sistemas de segurança responsáveis por monitorar, filtrar e controlar o tráfego de dados entre redes, conforme regras predefinidas, geralmente com o intuito de impedir invasões indesejadas.[202]

Hackers: Indivíduos que utilizam conhecimentos técnicos avançados em computação para explorar, testar, modificar ou violar sistemas computacionais, podendo atuar tanto de forma lícita (segurança) quanto ilícita.[203]

Hash: Função matemática que gera um valor único e fixo para um determinado arquivo, utilizada para garantir a integridade da prova digital. O aquivo que é manipulado gera alterações em seu código, o que permite a fácil identificação de eventual inautenticidade.[204]

iOS: Sistema operacional desenvolvido pela Apple Inc. para iPhones e iPads.[205]

Link: Elemento de hipertexto que permite a conexão entre páginas, documentos ou recursos digitais na internet.[206]

Magnet AXIOM: Plataforma avançada de perícia digital utilizada para extração e correlação de dados provenientes de dispositivos móveis, computadores e nuvem.[207]

---

[197] EUROPOL. **Dark Web investigations and cybercrime.** Haia, relatórios institucionais.
[198] NIST – NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **Glossary of key information security terms** (IR 7298). Gaithersburg: NIST, 2019.
[199] STALLINGS, William. **Cryptography and network security.** Boston: Pearson, 2017.
[200] OPENTEXT. **EnCase forensic user guide.** Waterloo: OpenText Corporation, s.d.
[201] UNESCO. **Journalism, fake news and disinformation.** Paris: UNESCO Publishing, 2018.
[202] NIST – NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. **Guidelines on firewalls and firewall policy** (SP 800-41). Gaithersburg: NIST, 2009.
[203] CERT.BR. **Segurança da informação para usuários**. São Paulo: NIC.br, 2023.
[204] ISO/IEC 27037:2012. **Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence.** Genebra: ISO, 2012.
[205] Apple Inc.. **iOS security guide.** Cupertino: Apple, s.d.
[206] W3C – WORLD WIDE WEB CONSORTIUM. **Hypertext specification.** Cambridge: MIT/W3C, s.d.
[207] MAGNET FORENSICS. **Magnet AXIOM technical overview.** Waterloo: Magnet Forensics, s.d.

Malware: Termo genérico que designa programas desenvolvidos com finalidade maliciosa, destinados a causar danos, obter dados, sequestrar sistemas ou violar informações.[208]

Phishing: Técnica de engenharia social destinada a induzir a vítima a fornecer dados sensíveis, mediante simulação de comunicações aparentemente legítimas.[209]

Ransomware: Espécie de *malware* que criptografa dados da vítima e exige pagamento de resgate para a liberação das informações, constituindo uma das principais modalidades de ataque cibernético contemporâneo.[210]

RaaS (Ransomware-as-a-Service): Modelo de negócio criminoso no qual desenvolvedores de ransomware licenciam suas ferramentas a afiliados, repassando parte dos valores obtidos nos resgates.[211]

Software: Conjunto de programas, instruções e dados computacionais que permitem o funcionamento de dispositivos eletrônicos.[212]

Windows: Sistema operacional desenvolvido pela Microsoft Corporation para computadores pessoais, amplamente utilizado em ambientes corporativos e domésticos.[213]

---

[208] ISO/IEC 27002:2022. **Information security, cybersecurity and privacy protection — Information security controls.** Genebra: ISO, 2022.
[209] CERT.BR. **Cartilha de segurança para internet**. São Paulo: NIC.br, 2023.
[210] CISA – CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY. **Ransomware guide.** Washington, 2020.
[211] EUROPOL. **Internet organised crime threat assessment (**IOCTA). Haia, 2021.
[212] IEEE. **Standard glossary of software engineering terminology** (IEEE 610.12). New York: IEEE, 1990.
[213] Microsoft. **Windows security architecture overview.** Redmond: Microsoft Corporation, s.d.

ANEXO A – PROJETO DE TIPO PENAL ESPECÍFICO

Art. 154-B – (Ataque Cibernético de Ransomware)

Atacar, remota ou manualmente, mediante emprego de código malicioso, fraude ou qualquer técnica informática, sistema informatizado público ou privado, com o fim de criptografar, inutilizar, interromper, destruir, subtrair ou tornar inacessíveis dados, programas ou serviços, exigindo, direta ou indiretamente, vantagem econômica ou outra condição para a restituição, desbloqueio, abstenção de divulgação ou restauração do funcionamento:

Pena – reclusão, de 4 (quatro) a 10 (dez) anos, e multa.

§ 1º A pena é aumentada de 1/3 até metade se o crime:

I – recair sobre infraestrutura crítica;

II – causar risco ou prejuízo relevante à segurança nacional, econômica, energética ou sanitária;

III – for cometido por organização, associação criminosa, célula terrorista ou mediante contratação de Ransomware-as-a-Service;

IV – envolver dados pessoais sensíveis em grande escala.

§ 2º Incorre nas mesmas penas quem oculta, converte ou dissimula, total ou parcialmente, a vantagem obtida, inclusive por meio de ativos virtuais, sem prejuízo da legislação de lavagem de capitais.

§ 3º Aplicam-se, no que couber, os regimes de perda ampliada e de cooperação internacional para identificação, rastreio e confisco de criptoativos