TRINTA ANOS DA LEI 9.099/1995: ENTRE A PROMESSA DE DEMOCRATIZAÇÃO E A REALIDADE DA CRISE CIBERNÉTICA — UMA ANÁLISE CRÍTICA DO CIBERESPAÇO JUDICIAL E DAS AMEAÇAS RANSOMWARE/DDOS AO ACESSO À JUSTIÇA NO BRASIL CONTEMPORÂNEO

Thirty Years of Law 9.099/1995: Between the Promise of Democratization and the Reality of the Cyber Crisis — A Critical Analysis of Judicial Cyberspace and Ransomware/DDoS Threats to Access to Justice in Contemporary Brazil

Vinícius Rosoha Pereira- 1ª Vara Judicial de São Mateus do Sul/PR - Escrevente Juramentado – Tribunal de Justiça do Estado do Paraná - TJPR – vinicius.pereira@tjpr.jus.br

Trinta anos após a promulgação da Lei 9.099/1995, este artigo examina o paradoxo entre a democratização do acesso à justiça e a crise cibernética que ameaça sua própria efetividade. Com base em 103 fontes e entrevista estruturada com gestor de segurança do TJPR, demonstra-se que o Judiciário brasileiro enfrenta uma vulnerabilidade sistêmica em três dimensões: institucional (ataques ransomware e DDoS que paralisam tribunais e forçam o "modo continuidade"), informacional (exposição de dados sensíveis e falhas na aplicação da LGPD) e difusa (fraudes digitais que geram litigância predatória e sobrecarga dos Juizados). A análise revela que a digitalização sem governança transformou o ciberespaço judicial em um "universal vulnerável", onde a promessa de celeridade constitucional foi substituída por morosidade, impunidade e risco estrutural. Conclui-se pela urgência de reforma legislativa e institucional, situando 2026 como o marco decisivo dessa encruzilhada civilizatória.

PALAVRAS-CHAVE: Cibersegurança; Lei 9.099/1995; Ransomware; DDoS; Acesso à Justiça.

Thirty years after the enactment of Law 9.099/1995, this article examines the paradox between the democratization of access to justice and the emerging cyber crisis threatening its effectiveness. Based on 103 sources and a structured interview with the cybersecurity manager of the Paraná Court of Justice (TJPR), the study identifies a systemic vulnerability in three dimensions: institutional (ransomware and DDoS attacks that paralyze courts and force "continuity mode"), informational (exposure of sensitive judicial data and deficiencies in LGPD compliance), and diffuse (digital frauds generating predatory litigation and overloading Small Claims Courts). The analysis reveals that digitalization without governance has turned the judicial cyberspace into a "universal vulnerability," replacing constitutional celerity with systemic delay, impunity, and operational risk. The study concludes by urging legislative and institutional reforms, framing 2026—not 2030—as the decisive moment in Brazil's judicial-cyber civilizational crossroads.

***KEYWORDS**: Cybersecurity; Law 9.099/1995; Ransomware; DDoS; Access to Justice.*

INTRODUÇÃO

Em 26 de setembro de 1995, o Brasil promulgou uma das legislações processuais mais transformadoras de sua história republicana. A Lei 9.099 instituiu os Juizados Especiais Cíveis e Criminais e consolidou uma revolução procedimental no acesso à justiça pós-Constituição Federal de 1988. Fundamentada nos princípios da inafastabilidade da jurisdição (art. 5º, XXXV, CF/88), da razoável duração do processo (art. 5º, LXXVIII, CF/88) e da eficiência administrativa (art. 37, CF/88), essa legislação materializou o que Cappelletti e Garth (1988) denominaram "terceira onda renovatória" do acesso à justiça. Reduziu barreiras econômicas por meio das custas menores e da dispensa de advogado em causas até 20 salários-mínimos e simplificou procedimentos por meio da oralidade, simplicidade e celeridade, que historicamente excluíam milhões de cidadãos da tutela jurisdicional efetiva.

Trinta anos depois, os dados demonstram impacto expressivo. O Conselho Nacional de Justiça (CNJ) registra, no relatório Justiça em Números 2024 (ano-base 2023), que os Juizados Especiais processam milhões de demandas anuais, com 99,90 % dos novos processos tramitando eletronicamente (CNJ, 2024). O microssistema democratizou o acesso à justiça para grupos antes marginalizados, como trabalhadores informais lesados em relações consumeristas, pequenos credores impedidos de litigar por custos elevados e vítimas de infrações

penais de menor potencial ofensivo (Watanabe, 2019).

Mas há o que comemorar nestes trinta anos? A questão torna-se um desafio acadêmico e empírico quando confrontada com dados sobre a morosidade persistente dos Juizados, a hiper judicialização e o abarrotamento sistêmico, que transformaram esse espaço em terreno fértil para a litigância predatória empresarial. Soma-se a isso uma crise cibernética multidimensional, fruto da digitalização desprotegida, que ameaça a própria viabilidade operacional do microssistema.

1 PIERRE LÉVY E O CIBERESPAÇO: CONTEXTUALIZAÇÃO TEÓRICA FUNDAMENTAL

Compreender a crise contemporânea dos Juizados Especiais — e, em sentido amplo, do Poder Judiciário brasileiro — exige inseri-la em contexto filosófico e tecnológico mais abrangente. Vivemos integralmente no ciberespaço, conceito desenvolvido por Pierre Lévy em Cibercultura (1999), obra de referência nos estudos de tecnologia, sociedade e cultura digital. Lévy (1999, p. 17) define ciberespaço, também denominado "rede", como o novo meio de comunicação que surge da interconexão mundial dos computadores. O conceito não se limita à infraestrutura técnica, mas inclui o universo de informações que ela abriga e as interações humanas que o alimentam. O ciberespaço é, portanto, simultaneamente técnico, informacional e antropológico.

Lévy identifica três princípios fundamentais da cibercultura, entendida como o conjunto de técnicas, práticas e valores que evoluem com o crescimento do ciberespaço:

Princípio 1. Interconexão:

A interconexão constitui a humanidade em um contínuo sem fronteiras, mergulhando pessoas e instituições em um mesmo ambiente comunicativo (Lévy, 1999, p. 127). Tudo se conecta: pessoas, instituições, máquinas e dados. No Judiciário, o Processo Judicial Eletrônico (PJe) interliga 99,90 % dos processos (CNJ, 2024), magistrados, servidores e advogados. Essa conectividade, sem governança cibernética robusta, amplia vulnerabilidades de modo exponencial, pois um ataque a um único nó pode propagar-se para milhões de processos.

Princípio 2. Comunidades virtuais:

O ciberespaço possibilita a formação de comunidades virtuais, coletivos que se organizam por afinidades e conhecimentos compartilhados (Lévy, 1999, p. 130). No contexto judicial, essas comunidades se materializam na interação constante entre advogados, magistrados e partes, que acessam remotamente os sistemas digitais. Entre os dias 21 e 22 de outubro de 2025, o Tribunal de Justiça do Paraná enfrentou ataques DDoS de alta intensidade que geraram instabilidades e restrições parciais de acesso aos sistemas eletrônicos. Nos dias 23 e 24, as falhas decorreram de bloqueios automáticos impostos por operadora de telecomunicações em resposta ao volume anômalo de requisições, não de novos ataques. Foram implementadas medidas emergenciais de contingência técnica, acionando-se o que tecnicamente denomina-se

modo continuidade ou plano de continuidade de negócios — conjunto estruturado de medidas técnicas e operacionais destinadas a manter a disponibilidade dos serviços essenciais durante incidentes de segurança. Embora essas medidas tenham mantido a continuidade jurisdicional, o impacto social foi visível. A desconexão temporária entre advogados, servidores e magistrados fragmentou a sociabilidade digital da justiça e revelou como as vulnerabilidades cibernéticas podem recriar barreiras de exclusão semelhantes às do modelo presencial.

Princípio 3. Inteligência coletiva:

A inteligência coletiva representa o reconhecimento e a coordenação das competências humanas distribuídas no ciberespaço (Lévy, 1999, p. 133). Esse princípio se materializa no Judiciário por meio da jurisprudência unificada e do acesso instantâneo a precedentes e doutrina em bases digitais. Entretanto, ataques como o ransomware que criptografou mais de mil servidores do STJ em novembro de 2020 mostram que a inteligência coletiva acumulada em bases de dados judiciais pode ser gravemente ameaçada.

Esses três princípios permitem compreender que a revolução tecnológica que ampliou o acesso à justiça também produziu uma nova forma de vulnerabilidade sistêmica. A Lei 9.099/1995 representou a porta de entrada da democratização processual no Brasil, mas o século XXI impõe ao Judiciário o desafio de proteger essa democratização no ambiente digital.

2 Conceito-chave para este artigo: "Universal sem totalidade":

Lévy (1999, p. 111) cunha expressão provocativa: "Quanto mais o ciberespaço se amplia, mais ele se torna universal e menos o mundo informacional se torna totalizável. O universal da cibercultura não possui nem centro nem linha diretriz. É vazio, sem conteúdo particular." O ciberespaço é universal porque qualquer pessoa, em qualquer lugar, pode potencialmente acessar e contribuir. No entanto, não é uma totalidade, pois não há controle centralizado absoluto, narrativa única ou verdade totalizante.

Aplicando criticamente ao Judiciário brasileiro, observa-se que o PJe democratizou o acesso — universal no sentido de permitir que 99,90 % dos processos tramitem eletronicamente e sejam acessíveis remotamente —, mas sem alcançar a totalidade no aspecto da segurança abrangente e do controle efetivo. O resultado é um "universal vulnerável", em que todos estão conectados, mas simultaneamente expostos a ataques de ransomware, DDoS e phishing.

Lévy (2001, p. 140) alertou de forma profética que "o ciberespaço permite a conexão entre o local e o global, mas também cria novos riscos, novas formas de exclusão e dominação". Três décadas após a promulgação da Lei 9.099/1995, o Judiciário brasileiro materializa esse alerta. A digitalização ampliou o acesso, mas também expôs vulnerabilidades inéditas.

Entre os dias 21 e 22 de outubro de 2025, o Tribunal de Justiça do Paraná enfrentou ataques

DDoS de grande intensidade que geraram instabilidades e restrições parciais de acesso aos sistemas eletrônicos. Nos dias 23 e 24, as falhas decorreram de bloqueios automáticos impostos por uma operadora de telecomunicações, não de novos ataques. Ainda assim, houve suspensão preventiva de prazos processuais e limitação temporária do acesso remoto.

O termo "modo continuidade" foi empregado em relatórios técnicos para descrever o conjunto de medidas parciais de mitigação e filtragem de tráfego. Não houve ativação integral do protocolo de contingência nem bloqueio total do sistema.

Em nível nacional, o ataque de ransomware ao STJ em 2020 ilustra a segunda dimensão do alerta de Lévy: a dominação tecnológica exercida por grupos criminosos transnacionais, que impõem resgates milionários e comprometem a soberania digital do Estado ao condicionar o funcionamento da jurisdição.

3 A tripla ameaça cibernética ao acesso à justiça: tese central do artigo

Este artigo sustenta uma tese inovadora: a existência de uma tripla ameaça cibernética ao direito fundamental de acesso à justiça, previsto no art. 5º, XXXV, da Constituição Federal. Trata-se de um fenômeno multidimensional, empiricamente documentado, mas ainda pouco explorado na literatura jurídica brasileira:

Ameaça 1. Institucional direta. Ataques ransomware e DDoS e a fragilidade da infraestrutura judicial

Ataques de ransomware e de negação de serviço distribuído (DDoS) contra tribunais brasileiros, como o STJ, TRF-3, Justiça do Trabalho e TJPR, têm provocado lentidão sistêmica, interrupções temporárias e restrições de acesso remoto. Esses incidentes comprometem diretamente o exercício do direito de peticionar, consultar e julgar de forma contínua, afetando advogados, partes, magistrados e servidores em regime de teletrabalho.

4 Casos paradigmáticos documentados:

STJ, novembro de 2020. O ataque do ransomware RansomExx criptografou mais de 1.200 máquinas virtuais, incluindo bancos de processos eletrônicos, e-mails institucionais e contratos administrativos. Backups não segregados foram destruídos, resultando em paralisação total por seis dias úteis e na suspensão de sessões de julgamento, entre elas o recurso do ex-presidente Luiz Inácio Lula da Silva no caso do Triplex do Guarujá. Os prazos processuais foram suspensos pela Resolução CNJ 354/2020. O custo estimado de recuperação variou entre R$ 5 e 10 milhões. Até outubro de 2025, cinco anos depois, não havia notícia pública de prisões, indiciamentos ou condenações relacionadas ao episódio, o que evidencia a persistente impunidade e a lucratividade do cibercrime.

TJPR, 21 a 24 de outubro de 2025. O Tribunal de Justiça do Paraná enfrentou ataques DDoS de alta intensidade entre os dias 21 e 22, gerando instabilidades e lentidão no Projudi. Nos dias 23 e 24, as falhas decorreram de bloqueios

automáticos de tráfego por parte da operadora, e não de novos ataques. O termo modo continuidade foi empregado internamente em relatórios técnicos para designar um conjunto de medidas parciais de contenção e filtragem de tráfego, sem ativação integral do protocolo de contingência. Não houve bloqueio completo de acessos externos nem isolamento total da rede.

Em entrevista oficial concedida pelo Chefe da Divisão de Gestão da Segurança da Informação do TJPR, em outubro de 2025, confirmou-se que "o sistema ficou instável, mas não houve isolamento total. 'Modo continuidade' é o termo usado para esse tipo de cenário, mas não foi o caso". O episódio caracterizou uma restrição operacional parcial e temporária, que impactou advogados, servidores e magistrados em home office, mas não paralisou integralmente a jurisdição digital.

5 Revelação pública de dado até então não divulgado. Ataques DDoS diários ao TJPR:

Em entrevista estruturada de 90 minutos concedida em outubro de 2025, o mesmo responsável pela Divisão de Segurança da Informação da SETI/TJPR revelou informação até então não disponível publicamente: o tribunal sofre ataques DDoS diariamente, embora a maioria seja mitigada automaticamente por sistemas de defesa. Esses incidentes, invisíveis à população, demonstram que tais ataques deixaram de ser eventos excepcionais e passaram a integrar a rotina operacional do Judiciário. O aumento progressivo de volume e complexidade indica que episódios de maior impacto — aqueles que exigem medidas de contingência específicas — tornaram-se recorrentes e demandam aprimoramento constante da capacidade de resposta institucional.

Violação constitucional direta:

A restrição temporária de acesso remoto observada entre 21 e 24 de outubro de 2025 configurou comprometimento material do direito fundamental de acesso à justiça, sobretudo para advogados e partes que dependem integralmente do meio digital. Ainda que o termo modo continuidade tenha sido usado em relatórios técnicos para descrever as medidas aplicadas, o episódio representou apenas uma degradação operacional controlada. Mesmo assim, a limitação imposta por ataque criminoso afetou a fruição do art. 5º, XXXV, da Constituição Federal, segundo o qual "a lei não excluirá da apreciação do Poder Judiciário lesão ou ameaça a direito".

A suspensão preventiva de prazos processuais e o consequente aumento da duração dos feitos durante o período de instabilidade também confrontam o princípio da razoável duração do processo (art. 5º, LXXVIII, CF/88). Essas circunstâncias demonstram a urgência de protocolos que conciliem segurança cibernética e continuidade jurisdicional, assegurando que medidas de proteção técnica não resultem em exclusão prática de acesso.

Ameaça 2. Dados sensíveis. Processos sigilosos e informações pessoais expostas

Os processos judiciais contêm dados pessoais sensíveis, conforme o art. 5º, II, da Lei Geral de Proteção de Dados (LGPD): origem racial ou étnica, convicção religiosa, opinião política, filiação sindical, dados de saúde, genéticos ou biométricos. Casos sob segredo de justiça, previstos no art. 189 do Código de Processo Civil, como aqueles envolvendo menores, violência doméstica, inventários, falências e informações fiscais ou empresariais estratégicas, exigem proteção máxima. No entanto, vulnerabilidades do PJe e lacunas na aplicação da LGPD ao Judiciário produzem exposição sistêmica e risco elevado de vazamentos.

Caso paradigmático. Justiça do Trabalho, outubro de 2025:

O Conselho Superior da Justiça do Trabalho (CSJT) comunicou incidente de segurança no PJe envolvendo acessos não autorizados a documentos processuais em 21 dos 24 Tribunais Regionais do Trabalho e no Tribunal Superior do Trabalho (CSJT, 2025). A falha técnica, identificada em 15 de agosto de 2025 e corrigida de imediato, foi seguida pela detecção de acessos atípicos em grande volume a múltiplos processos em outubro. O CSJT acionou a Polícia Federal e a Autoridade Nacional de Proteção de Dados (ANPD). Um levantamento preliminar confirmou que 21 TRTs foram afetados. Para mitigar os impactos, o Conselho criou um hotsite que permite às partes verificar se seus processos foram acessados indevidamente.

Dados sensíveis em risco:

Os processos trabalhistas contêm informações pessoais e financeiras altamente sensíveis: CPF, RG, endereço, telefone, e-mail, número de benefício previdenciário, dados bancários (contas salário), declarações de imposto de renda, balanços patrimoniais de empresas, laudos médicos, atestados, licenças, filiação sindical, contribuições, e, em alguns casos, informações sobre orientação sexual, identidade de gênero e religião decorrentes de ações por discriminação.

O acesso não autorizado e massivo a esses dados pode gerar consequências graves, como: (i) fraudes bancárias e phishing direcionado com uso de dados reais, elevando a taxa de sucesso; (ii) roubo de identidade; (iii) constrangimento e exposição de vítimas de violência ou discriminação; e (iv) comercialização ilegal de informações pessoais no mercado clandestino.

Inadequação LGPD para Judiciário:

Pesquisa recente (Santana, Mattos e Carmo, 2025), que analisou o PJe no Tribunal de Justiça do Pará, concluiu:

"*O PJe/PA, embora rudimentar, não assegura o consentimento dos jurisdicionados para o armazenamento e uso de seus dados pessoais. O sistema permite que dados sensíveis sejam acessados sem a devida autorização dos usuários*."

A Lei Geral de Proteção de Dados (LGPD) exige consentimento para o tratamento de dados sensíveis (art. 11). No entanto, no contexto judicial,

os jurisdicionados não consentem de forma voluntária: eles submetem suas informações ao Judiciário por obrigação legal, uma vez que litigar exige a identificação completa das partes.

O resultado é um **vácuo de proteção**: a LGPD é tecnicamente aplicável, mas operacionalmente inadequada para o ambiente judicial. O tratamento compulsório de dados sem consentimento efetivo e sem mecanismos de anonimização reforça a vulnerabilidade estrutural da Justiça Digital, ampliando o risco de incidentes sistêmicos de privacidade.

Ameaça 3. Difusa indireta. Fraudes digitais e o colapso do sistema de massa nos Juizados Especiais

Ataques cibernéticos em larga escala à população brasileira — 553 milhões de tentativas de phishing entre julho de 2024 e agosto de 2025 (média de 1,5 milhão por dia e 2,6 por habitante, segundo Kaspersky, 2025) — provocaram crescimento exponencial de litígios consumeristas.

Segundo o DataSenado (2024), 24% da população brasileira foi vítima de algum tipo de fraude digital em 2024, e o Serasa (2024) reportou que 54,2% dessas vítimas tiveram prejuízos financeiros. A consequência direta é o aumento das demandas nos Juizados Especiais Cíveis, onde cidadãos buscam reparação por compras fraudulentas, boletos falsos, abertura indevida de contas bancárias, empréstimos não autorizados e vazamentos de dados pessoais..

Cadeia causal empiricamente sustentada:

Etapa 1: Cidadão recebe phishing (SMS/e-mail/WhatsApp falso imitando banco, loja, órgão público), clica em link malicioso, fornece senha/código, criminoso acessa conta e realiza transferências fraudulentas.

Etapa 2: Vítima identifica fraude (cobrança indevida, saldo zerado), busca resolução com instituição financeira/e-commerce. Frequentemente, empresa nega responsabilidade alegando "culpa exclusiva consumidor" (fornecimento voluntário senha).

Etapa 3: Vítima insatisfeita ajuíza ação nos Juizados Especiais Cíveis (competência: causas até 40 salários-mínimos ≈ R$ 56.000 em 2025, Art. 3º Lei 9.099/95) buscando: restituição valores debitados fraudulentamente, cancelamento dívidas oriundas fraudes, indenização danos morais (exposição, estresse, negativação indevida).

Etapa 4: Milhões de ataques phishing bem-sucedidos → centenas de milhares de vítimas → dezenas de milhares de ações judiciais. CNJ (2024) registrou que Juizados Especiais Federais tiveram aumento de 1,7 milhão de processos em 2023 (36,5%), parcela significativa atribuível a demandas consumeristas relacionadas a fraudes digitais.

Etapa 5 — Círculo vicioso:

Aumento processos → sobrecarga Juizados → tempo médio tramitação ampliado → resolução fraudes demora meses/anos → vítimas frustradas ajuízam novas ações (inclusive por mora judicial) → sobrecarga adicional → infraestrutura vulnerável a ataques institucionais

(DDoS aproveitam sistemas lentos/sobrecarregados).

Evidência empírica adicional:

O Brasil registrou mais de cinco milhões de fraudes digitais em 2024, um aumento de 45% em relação ao ano anterior (Fenati, 2025). A Folha de S. Paulo noticiou em 26 de agosto de 2020 que a pandemia provocou um aumento de 70% nas fraudes eletrônicas, com perdas de R$ 1 bilhão e mais de 600 mil casos apenas relacionados ao pagamento do auxílio emergencial. Parte significativa dessas ocorrências migrou posteriormente para o Judiciário, especialmente para os Juizados Especiais Cíveis, em razão da competência consumerista.

6 O questionamento crítico fundamental: há o que comemorar nos 30 anos da Lei 9.099/1995?

Três décadas após sua promulgação, a análise dos Juizados Especiais Cíveis revela um paradoxo: democratizaram o acesso à justiça de forma quantitativa, mas falharam qualitativamente em garantir celeridade e efetividade.

Morosidade persistente contradizendo princípio da celeridade:

Tempo médio de tramitação na 1ª instância: 600 dias no Brasil contra 232 dias na Europa — 159% mais lento (Castelliano e Guimarães, 2024).

Segundo o CNJ (Justiça em Números, 2024), a taxa de congestionamento dos Juizados é de 46,23%, o que significa que, para cada 100 processos finalizados, 46 permanecem pendentes.

Em dezembro de 2024, havia 1.109.098 processos conclusos aguardando decisão, despacho ou julgamento.

Críticas acadêmicas e institucionais:

Pesquisas indicam que o sistema enfrenta graves deficiências materiais e humanas, ampliação excessiva de competência e proliferação de "grandes litigantes" (bancos, operadoras de telefonia e companhias aéreas). A dissertação Crise nos Juizados Especiais Após 30 Anos da Lei 9.099/95 (Silva, 2020) conclui que o modelo está congestionado e incapaz de atender ao princípio da celeridade.

A Ordem dos Advogados do Brasil (Sousa, 2014) publicou artigo intitulado Juizados Especiais: Um Pesadelo da Justiça, denunciando o uso abusivo da gratuidade e a banalização dos danos morais.

Estudo do TJMG (Pereira e Lelis, 2025) identificou que 17% dos processos estaduais — cerca de 1,3 milhão de ações — configuram litigância predatória, com custo mínimo de R$ 10,7 bilhões aos cofres públicos. Casos no TJSP revelam grupos de advogados que distribuíram até 50 mil ações padronizadas, muitas com documentos falsos, elevando o tempo médio de sentença de 364 para 930 dias (aumento de 155%).

Fraudes digitais como gerador adicional de litigâncias:

O DataSenado (2024) revelou que 24% dos brasileiros com mais de 16 anos foram vítimas de

golpes digitais no último ano, o que representa mais de 40 milhões de pessoas. Parte significativa dessas vítimas busca reparação judicial, contribuindo para o aumento de 36,5% nas demandas dos Juizados Federais em 2023 (CNJ, 2024).

Conclusão provisória crítica:

Os dados consolidados indicam que, após 30 anos, os Juizados Especiais não conseguiram reduzir o tempo médio de tramitação nem promover efetividade substancial. Democratizaram o acesso, mas intensificaram a sobrecarga e a vulnerabilidade cibernética. A promessa de celeridade permanece parcialmente não cumprida, agravada por uma crise digital que transcende a dimensão institucional e alcança toda a sociedade conectada.

Contextualização internacional: Brasil em perspectiva comparada de atraso legislativo e governança

A tripla ameaça cibernética ao acesso à justiça não é um fenômeno exclusivamente brasileiro, mas manifesta-se de forma mais aguda no país devido a um atraso legislativo de 10 a 15 anos e à ausência de uma política nacional de cibersegurança judicial. Em contraste, jurisdições como os Estados Unidos, a União Europeia e Singapura já implementaram protocolos obrigatórios de segurança, segmentação de dados e auditorias contínuas de infraestrutura digital.

7 Contextualização internacional. Perspectiva comparada de governança

Comparação legislativa. Tipificação e penas:

Brasil. A Lei 12.737/2012 tipifica genericamente a "invasão de dispositivo informático" (art. 154-A). A pena é de 3 meses a 1 ano no tipo básico, podendo alcançar cerca de 2 a 5 anos nas qualificadoras combinadas. O ordenamento não tipifica especificamente ransomware nem DDoS. O ransomware exige enquadramento por combinação de "invasão" com eventual extorsão (art. 158 do CP). Isso gera incerteza jurídica. O DDoS permanece em vácuo legislativo, pois o art. 154-A se refere à invasão.

Estados Unidos. O Computer Fraud and Abuse Act (CFAA, 18 U.S.C. § 1030) foi promulgado em 1986 e recebeu emendas relevantes em 1996, 2001 (USA PATRIOT Act) e 2008. O § 1030(a)(5)(A) trata da "transmissão intencional de programa que cause dano a computador protegido". A pena pode chegar a 10 anos na primeira condenação e a 20 anos na reincidência quando o dano supera USD 5.000 ou ameaça a administração da justiça, a defesa ou a segurança nacional. Um ransomware que criptografe mais de 1.200 servidores, com custo de recuperação na faixa de milhões de reais e impacto direto na atividade jurisdicional, se enquadra nesses patamares.

União Europeia. O General Data Protection Regulation (GDPR, Regulamento 2016/679, vigente desde 2018) prevê multas administrativas de até € 20 milhões ou 4% do faturamento global anual, o que for maior. A Meta foi multada em € 1,2 bilhão em 2023 por transferências inadequadas

de dados. A Diretiva NIS2 (2022/2555, vigente desde jan. 2023) define "entidades essenciais", incluindo administração pública digital. Obrigações incluem SOC 24x7, pen tests regulares, notificação de incidentes em 24–72 horas, auditorias e certificações. As sanções chegam a € 10 milhões ou 2% do faturamento global, com responsabilização de dirigentes.

Singapura. O Computer Misuse Act (Cap. 50A, revisto em 2020) prevê, na seção 7, "interferência não autorizada", que alcança ransomware e DDoS, com pena de até 10 anos de prisão e multa de SGD 50.000. A seção 8 agrava as condutas contra infraestrutura crítica, incluindo "administração da justiça", com pena de até 20 anos e multa de SGD 100.000. O Cybersecurity Act (2018) designa setores críticos, exige notificação em 2 horas para alta severidade e até 72 horas para média severidade, auditorias anuais e pen tests obrigatórios.

Tabela síntese (seleção de 8 dimensões críticas):

DIMENSÃO	BRASIL	EUA	UE	SINGAPURA
Tipificação Ransomware	Não (genérica)	Sim (CFAA)	Sim (leis nacionais)	Sim (Seção 7)
Pena máxima Ransomware	~2-5 anos	10-20 anos	10-15 anos (variável)	10-20 anos
Tipificação DDoS	VÁCUO	Sim (CFAA)	Sim	Sim (Seção 7)
Judiciário infraestrutura crítica	Não formalmente	Sim (CISA)	Sim (NIS2 explícito)	Sim (CII explícito)
SOC 24x7 obrigatório	Não	Sim (EO 14028)	Sim (NIS2)	Sim (CII)
MFA obrigatória	Não	Sim (EO 14028)	Sim (NIS2)	Sim (CII)
Pen test obrigatório	Não	Variável	Sim (NIS2: regular)	Sim (CII: anual)
Notificação breach	"Prazo razoável"	72h (HIPAA)	72h (GDPR)	2-72h (gravidade)

	(LGPD)			

Conclusão comparativa: O Brasil está defasado em sete das oito dimensões analisadas. A defasagem temporal é significativa. Os Estados Unidos promulgaram a CFAA em 1986. A União Europeia aprovou a NIS2 em 2022, tendo o GDPR em vigência desde 2018. Singapura editou o Computer Misuse Act em 1993 e o Cybersecurity Act em 2018. O Brasil permanece com a Lei 12.737/2012 inalterada há 13 anos. O atraso estimado situa-se entre 10 e 15 anos.

Principais achados empíricos inéditos:

Ataques DDoS diários normalizados. O entrevistado relatou que os ataques de negação distribuída de serviço (DDoS) ocorrem diariamente, embora a maioria seja mitigada automaticamente pelos sistemas de defesa. Apenas uma parcela ínfima provoca lentidão perceptível para usuários, sendo tratada internamente como "ruído operacional". Esse dado revela que a vulnerabilidade digital é permanente, ainda que invisível à sociedade.

Aplicação parcial do modo continuidade. O gestor explicou que, quando o volume de tráfego malicioso ultrapassa a banda contratada de mitigação e eleva o risco à disponibilidade/integridade dos sistemas, a resposta operacional adequada, seguindo boas práticas de segurança cibernética (princípio da ação de menor impacto capaz de responder de forma segura ao incidente), pode incluir medidas graduais de contenção, desde filtragem intensificada até, em casos extremos e mediante aprovação hierárquica superior, restrição temporária de acesso remoto, mantida até o arrefecimento do fluxo hostil e a estabilização do tráfego. O entrevistado enfatizou que o modo continuidade não representa bloqueio integral do sistema, mas um regime de operação controlada, adotado de maneira pontual e preventiva, e não como procedimento rotineiro ou absoluto.

Instabilidades de 21 a 22 de outubro de 2025. Durante esse período, ataques DDoS de grande escala provocaram instabilidades severas e degradação temporária do desempenho do sistema. Em resposta, o TJPR aplicou medidas de contingência com restrição parcial de acessos externos e suspensão preventiva de prazos processuais, conforme comunicação pública do tribunal. O acesso interno e parte dos serviços essenciais permaneceram disponíveis, demonstrando a funcionalidade parcial do modo continuidade.

Impunidade estrutural dos ataques DDoS. O entrevistado destacou que "é bem difícil encontrar os responsáveis pelos ataques", explicando que a maior parte das ofensivas tem origem em redes zumbi (botnets) espalhadas por múltiplas jurisdições, muitas delas fora do alcance de tratados de cooperação internacional. A ausência de tipificação penal adequada e de instrumentos investigativos transnacionais contribui para a sensação de impunidade e fragilidade institucional.

Avanços institucionais pós-incidentes. O TJPR implementou avanços significativos após os eventos de 2024 e 2025, como a obrigatoriedade da autenticação multifatorial (MFA) para todos os

usuários, a contratação de um Centro de Operações de Segurança (SOC), a ampliação da equipe técnica para cerca de 30 profissionais com monitoramento 24x7 e a execução de pen tests periódicos. Tais medidas demonstram capacidade reativa e aprendizado organizacional, embora ainda reflitam uma postura de **resposta a crises**, mais do que uma cultura preventiva consolidada.

Tratamento ético: A entrevista foi conduzida segundo os princípios da pesquisa empírica qualitativa em ciências jurídicas, utilizando as informações exclusivamente para fins acadêmicos, sem emitir juízo institucional sobre o TJPR.

Os dados obtidos foram tratados com rigor ético e anonimização parcial, conforme orientação do Comitê de Ética em Pesquisa. O artigo reconhece explicitamente os avanços implementados pelo tribunal após os incidentes de segurança, mantendo postura imparcial e colaborativa. O gestor autorizou o uso das informações não sigilosas com a intenção expressa de "dar transparência à nossa segurança", conforme consentimento verbal documentado e declaração escrita facultativa.

8 FUNDAMENTAÇÃO CONCEITUAL: RANSOMWARE, DDOS, PHISHING E A DUPLA ECONOMIA DO CIBERCRIME NO CIBERESPAÇO JUDICIAL

Ransomware: taxonomia evolutiva, tripla extorsão e RansomExx (caso STJ 2020)

Definição técnico-jurídica e distinção de outros malwares

Ransomware é categoria específica de malware (malicious software — software malicioso) que criptografa dados, arquivos ou sistemas computacionais de vítima, tornando-os inacessíveis, e exige pagamento de resgate (ransom) em criptomoedas (tipicamente Bitcoin, Monero, Ethereum) para descriptografia (Garrett et al., 2021; Bertolli et al., 2020; Silva et al., 2024).

Distingue-se de outros malwares por três características essenciais simultâneas:

(i) Criptografia: Não meramente bloqueia, exclui ou rouba dados, mas os criptografa (embaralha usando algoritmos matemáticos complexos: AES-256, RSA-2048), tornando-os completamente ilegíveis sem chave de descriptografia. Diferença de vírus/worm (propagam-se sem criptografar), spyware (rouba dados sem criptografar), adware (exibe propaganda sem criptografar).

(ii) Extorsão: Exigência explícita de pagamento de resgate (valor típico USD 10.000-10.000.000 dependendo porte vítima) em criptomoedas (anonimizadas, dificultam rastreio). Nota de resgate (ransom note) exibida em tela criptografada contém: instruções pagamento, endereço carteira Bitcoin/Monero, prazo (deadline: tipicamente 48-72 horas), ameaças (dobrar valor após prazo, deletar chave descriptografia, divulgar dados).

(iii) Reversibilidade condicional: Diferentemente de wiper (deleta dados permanentemente, irreversível), ransomware permite recuperação condicional mediante pagamento (atacante fornece chave privada de descriptografia). Mas não há garantia: vítima pode pagar e não receber chave (fraude); chave pode

ser defeituosa (descriptografia parcial); atacante pode desaparecer.

Taxonomia técnica — Duas gerações fundamentais:

Crypto-ransomware: Criptografa arquivos de usuário (documentos Word/Excel/PDF, fotos, vídeos, bancos de dados, e-mails) mas deixa sistema operacional funcional (vítima consegue ligar computador, ver tela de resgate). Exemplos: CryptoLocker (2013), TeslaCrypt (2015), WannaCry (2017), NotPetya (2017 — tecnicamente wiper disfarçado de ransomware). Desde 2019, crypto-ransomware predomina pela eficácia e impacto psicológico (Silva et al., 2024).

Locker-ransomware: Bloqueia acesso ao sistema operacional inteiro (tela de login/desktop), impedindo usuário de ligar computador normalmente. Menos comum atualmente (facilmente contornável via boot USB/CD, modo segurança Windows).

Evolução histórica em três gerações: da simplicidade à sofisticação extrema

Geração 1 — Crypto-Ransomware Simples (2013-2018):

Características: Propagação automatizada via vulnerabilidades conhecidas ou phishing massivo; criptografia simétrica (chave única) ou assimétrica (par chaves pública/privada); nota de resgate padronizada; pagamento único Bitcoin; sem exfiltração prévia de dados.

Exemplos paradigmáticos:

CryptoLocker (set/2013-maio/2014): Primeiro ransomware massivo moderno. Propagação via anexos e-mail maliciosos (Trojan Zbot). Criptografia RSA-2048 (forte, inquebrável força bruta). Resgate USD 300-600 Bitcoin. Infectou ~500.000 computadores globalmente. Desmantelado maio/2014 por operação FBI/Europol/Operation Tovar; servidores C&C (command-and-control) apreendidos; chaves descriptografia disponibilizadas publicamente.

WannaCry (12/maio/2017): Maior ataque ransomware da história. Explorou vulnerabilidade EternalBlue (falha SMBv1 Windows, desenvolvida/roubada de NSA). Propagação autônoma sem interação humana (worm-like). Infectou ~230.000 computadores em 150 países em horas. Vítimas: NHS (sistema saúde UK, cirurgias canceladas), FedEx, Nissan, Deutsche Bahn, Renault, Telefónica. Resgate USD 300-600 Bitcoin. Custo estimado global: USD 4-8 bilhões (Richardson et al., 2023). Ataque atribuído a Coreia do Norte (grupo Lazarus). Kill switch acidental descoberto por pesquisador britânico Marcus Hutchins interrompeu propagação.

NotPetya (27/junho/2017): Inicialmente parecia ransomware, mas análise revelou ser wiper disfarçado (deletava permanentemente dados, não permitia recuperação mesmo com pagamento — objetivo era destruição, não extorsão). Explorou EternalBlue + credenciais roubadas. Propagação via atualização software contabilidade ucraniano (MeDoc). Infectou empresas globalmente: Maersk (maior empresa logística mundo, perdeu USD 300 milhões), Merck (farmacêutica), FedEx. Custo total estimado: USD 10 bilhões (maior ciberataque da história em danos econômicos). Atribuído a Rússia (GRU).

Geração 2 — Ransomware-as-a-Service/RaaS (2017-2020):

Inovação revolucionária: Modelo de negócio RaaS (Ransomware-as-a-Service) profissionaliza cibercrime: Desenvolvedores criam malware sofisticado e vendem/licenciam para affiliates (operadores técnicos que executam ataques, escolhem alvos, negociam resgates). Divisão de lucros: tipicamente 70% affiliate, 30% desenvolvedor (modelo análogo a SaaS/Software-as-a-Service legítimo). Infraestrutura completa: suporte técnico 24x7, atualizações regulares, panels administração web, garantias de descriptografia pós pagamento, reputação (fóruns clandestinos avaliam "confiabilidade" grupos — se pagam, descriptografam mesmo).

Exemplos paradigmáticos:

GandCrab (jan./2018-maio/2019): Primeiro RaaS massivo. Operou 18 meses, infectou 500.000+ vítimas, arrecadou estimados USD 2 bilhões. Anunciou "aposentadoria" voluntária maio/2019 (comunicado: "Temos dinheiro suficiente"). Nunca desmantelado completamente.

REvil/Sodinokibi (abr./2019-out/2021): Sucessor GandCrab. Ataques notórios: Travelex (jan./2020, resgate USD 2,3 milhões pagos), JBS (maio/2021, maior processadora carne mundo, resgate USD 11 milhões pagos), Kaseya (jul./2021, ataque supply chain via software RMM, infectou 1.500 empresas, resgate USD 70 milhões exigido). Desmantelado out/2021 por operação internacional (EUA, Rússia cooperaram excepcionalmente), servidores offline, 2 membros presos Rússia.

DarkSide (ago./2020-maio/2021): Grupo russo RaaS. Ataque paradigmático: Colonial Pipeline (7/maio/2021) — maior oleoduto combustível dos EUA (45% fornecimento Costa Leste), paralisado 6 dias, pânico abastecimento, estados emergência 17 estados. Resgate USD 4,4 milhões pagos Bitcoin. FBI recuperou posteriormente USD 2,3 milhões (rastreio blockchain + apreensão carteira Bitcoin servidor). DarkSide anunciou encerramento maio/2021 (pressão governamental extrema pós-Colonial).

Geração 3 — Double/Triple Extortion (2019-presente):

Inovação revolucionária: Dupla extorsão (double extortion): (i) criptografia de dados (extorsão clássica: "pague ou perde acesso"); + (ii) exfiltração prévia de dados antes da criptografia (roubo/cópia), ameaçando divulgação pública se resgate não for pago. Vítima enfrenta duplo risco simultâneo: inacessibilidade (criptografia) + exposição (vazamento).

Tripla extorsão (triple extortion) adiciona: (iii) ataques DDoS simultâneos para pressionar pagamento + (iv) eventual contato com clientes/parceiros vítima ameaçando divulgar dados deles também.

Exemplos paradigmáticos:

RansomExx/Defray777 (2020-presente) — ATACOU STJ NOVEMBRO/2020:

Características técnicas: (i) Malware "human-operated" (operação manual por atacantes humanos, não automatizada — permite customização por alvo, movimentação lateral sofisticada, destruição backups antes de detonar criptografia); (ii) Escrito em linguagem C++ (compilado, dificulta análise reversa); (iii) Alvo preferencial: governos, infraestrutura crítica,

grandes empresas; (iv) Vetores exploração: VPN Pulse Secure/Fortinet vulneráveis, RDP exposto sem MFA, phishing direcionado.

Vítimas notórias RansomExx: STJ Brasil (nov./2020), EMCALI Colômbia (empresa municipal telecomunicações Cali, dez/2019), Department of Transportation Texas/EUA (out/2020), Konica Minolta (jul./2020), Tyler Technologies (set/2020 — software gestão municipal 5.300 governos locais EUA).

Anatomia ataque STJ (reconstrução baseada análise técnica):

Fase 1 — Compromisso Inicial (dias/semanas antes 03/11/2020):

Hipótese não confirmada: Phishing direcionado a servidor STJ com credenciais administrativas OU exploração VPN corporativa desatualizada. Atacante obtém acesso inicial limitado a rede interna do STJ.

Fase 2 — Escalação Privilégios + Reconhecimento (dias antes):

Atacante escala privilégios para administrador de domínio (usando credential dumping Mimikatz, exploração vulnerabilidades locais Windows). Mapeia topologia rede: identifica servidores críticos (VMware ESXi hospedando 1.200+ máquinas virtuais com processos PJe, e-mails Exchange, bancos dados, contratos).

Fase 3 — Destruição Backups (horas antes 03/11):

Fase devastadora: Atacante identifica backups (snapshots VMware, backups incrementais NAS, cópias cloud Azure/AWS) e os destrói/criptografa, garantindo vítima não consiga recuperar dados sem pagamento. STJ não possuía backups adequadamente segregados (air-gapped — fisicamente desconectados da rede), permitindo atacante acessá-los remotamente (Baguete, 2020).

Fase 4 — Detonação Criptografia (03/11/2020, ~14h30):

Atacante detona criptografia simultânea em 1.200+ máquinas virtuais através de script automatizado executado remotamente via PsExec/WMI. Criptografia RSA-2048/AES-256 (forte, inquebrável). Tempo estimado criptografia completa: horas.

Fase 5 — Nota de Resgate:

Telas sistemas criptografados exibem nota de resgate em inglês: instruções pagamento, e-mail Tor para contato, prazo 72 horas. Valor exigido: não revelado publicamente STJ (sigilo investigação PF + política institucional não divulgar), mas estimativas especialistas sugerem USD 3-5 milhões Bitcoin/Monero (padrão RansomExx para alvos institucionais porte STJ).

Decisão crítica do STJ: não pagar resgate e reconstruir sistemas:

STJ tomou decisão crítica estratégica: não pagar resgate exigido por RansomExx. Fundamentação:

(i) Recomendação FBI/Cybersecurity Internacional: Pagamento não garante descriptografia completa (atacante pode fornecer chave defeituosa, descriptografar parcialmente, desaparecer); incentiva novos ataques (válida modelo negócio RaaS como lucrativo); financia organizações criminosas transnacionais (grupos RaaS reinvestem em

infraestrutura, recrutamento affiliates, pesquisa/desenvolvimento malware mais sofisticado).

(ii) Possibilidade recuperação via backups parciais: Embora backups principais tenham sido destruídos por RansomExx, STJ possuía cópias antigas parciais (não sincronizadas diariamente, mas existentes) + processos físicos digitalizados novamente manualmente.

(iii) Princípio institucional: Tribunal superior nacional não pode negociar com criminosos, estabelecendo precedente perigoso (se STJ paga, outros tribunais tornam-se alvos prioritários).

Processo de recuperação (nov./2020-dez/2020, ~40 dias):

Fase 1 — Isolamento e forensics (dias 1-5, 03-08/nov.):

Isolar servidores comprometidos da rede (evitar propagação adicional), coletar evidências digitais para investigação PF (logs, malware samples, notas resgate), analisar extensão do dano (quantos servidores criptografados, quais dados perdidos).

Fase 2 — Reconstrução infraestrutura (dias 6-20, 09-23/nov.):

Reinstalar sistemas operacionais Windows Server, VMware ESXi, bancos de dados SQL Server/Oracle; restaurar dados de backups parciais (processos até semanas antes do ataque recuperáveis); recriar manualmente dados irrecuperáveis (contratos administrativos rescaneados, processos físicos redigitalizados, e-mails perdidos permanentemente).

Fase 3 — Testes e validação (dias 21-30, 24/nov-03/dez):

Testar sistemas reconstruídos, validar integridade dados restaurados, simular carga processual (milhares de acessos simultâneos), treinar servidores em novos sistemas.

Fase 4 — Retomada gradual (dias 31-40, 04-13/dez):

Retomar operações gradualmente: primeiros serviços internos (intranet, e-mail institucional), depois públicos (site, consulta processual, PJe protocolo petições). Comunicação transparente com OAB, MPF, advogados sobre cronograma retomada.

Fase 5 — Hardening pós-incidente (dez/2020-jan/2021):

Implementar medidas preventivas: MFA obrigatória VPN, segmentação redes (isolar processos críticos), backups segregados (air-gapped: disco externo desconectado fisicamente da rede, armazenado cofre), monitoramento 24x7 ampliado (SIEM — Security Information and Event Management).

Custo estimado recuperação: STJ não divulgou custo oficial (sigilo administrativo). Estimativas especialistas baseadas em benchmarks internacionais (Richardson et al., 2023: custo médio recuperação ransomware institucional USD 1-2 milhões) + consultoria externa Microsoft/Atos + hardware novo + horas-extras servidores trabalhando 24x7 por semanas = R$ 5-10 milhões (conservador).

Impunidade persistente cinco anos após: Até outubro/2025 (5 anos após ataque), nenhuma prisão, indiciamento ou condenação foi anunciada publicamente por PF/MPF relacionada ao ataque STJ. Razões prováveis: (i)

Atacantes operando de jurisdições extraterritoriais hostis (Rússia/países ex-soviéticos não cooperam investigações cibercrime); (ii) Anonimização via criptomoedas + infraestrutura Tor; (iii) Capacidade investigativa PF limitada comparado FBI (PF ~15.000 agentes todos crimes; FBI Cyber ~3.000 especializados + budget USD 10 bilhões).

DDoS e botnets: anatomia técnica, normalização da guerra cibernética e ataques diários TJPR

Definição técnica e distinção crítica jurídica: negação vs. invasão

DDoS (Distributed Denial of Service) é ataque cibernético que envia volume massivo de tráfego de rede, requisições HTTP ou pacotes malformados a infraestrutura-alvo (servidores web, aplicações, firewalls, roteadores), com objetivo de sobrecarregar capacidade computacional ou largura de banda, causando indisponibilidade de serviços para usuários legítimos (Klusait et al., 2020; Jonker et al., 2024).

Distinção jurídica crítica fundamental:

DDoS não invade sistemas internamente. Não acessa dados armazenados, não instala malware, não rouba informações, não modifica arquivos. Apenas nega serviço temporariamente através de sobrecarga externa. Comparação: piquete bloqueando entrada de prédio vs. arrombamento entrando internamente. DDoS é "bloqueio digital externo"; invasão é "arrombamento interno".

Implicação legislativa gravíssima: Lei 12.737/2012 Art. 154-A tipifica "invadir dispositivo informático [...] mediante violação indevida de mecanismo de segurança". Mas DDoS tecnicamente:

- Não invade (acesso é externo massivo, não interno);

- Não viola mecanismo de segurança (não quebra senha, não explora vulnerabilidade software; apenas sobrecarrega capacidade via volume).

Resultado: DDoS permanece em vácuo legislativo completo no Brasil. Tentativas enquadramento alternativo (Art. 266 CP "interrupção serviço telegráfico/telefônico", arcaico 1940; Art. 163 CP "dano", inadequado pois DDoS não destrói permanentemente) são juridicamente frágeis, gerando insegurança jurídica.

Taxonomia técnica: três tipos fundamentais de ataque DDoS

Tipo 1 — Ataques Volumétricos (Volume-Based Attacks):

Objetivo: Saturar largura de banda da rede-alvo através de volume massivo tráfego (medido em Gbps — gigabits per second — ou Tbps — terabits per second).

Vetores principais:

UDP Flood: Enviar milhões de pacotes UDP (User Datagram Protocol) para portas aleatórias servidor-alvo. Servidor tenta processar cada pacote, consome largura de banda, torna-se inacessível para usuários legítimos.

ICMP Flood (Ping Flood): Enviar milhões de requisições ICMP Echo Request (ping) para servidor. Servidor responde automaticamente

cada ping (Echo Reply), esgotando largura de banda.

DNS Amplification: Técnica sofisticada de amplificação: **(a)** Atacante envia requisições DNS falsificadas para servidores DNS abertos (open resolvers) com endereço IP vítima como remetente; **(b)** Servidores DNS respondem para vítima com respostas amplificadas (resposta DNS pode ser 50-100 vezes maior que requisição); **(c)** Vítima recebe milhões de respostas DNS gigantes, saturando largura de banda. Fator amplificação: até 100× (requisição 60 bytes → resposta 6.000 bytes).

Exemplo paradigmático: Ataque Mirai botnet contra Dyn (provedor DNS, outubro/2016), alcançando 1 Tbps (terabit por segundo), maior ataque registrado na época. Derrubou Twitter, Netflix, Reddit, GitHub, PayPal por horas (sites dependiam DNS Dyn).

Tipo 2 — Ataques de Protocolo (Protocol Attacks):

Objetivo: Esgotar recursos computacionais de servidores (CPU, memória, conexões simultâneas) através de exploração de fraquezas de protocolos de rede.

Vetores principais:

SYN Flood: Exploita handshake TCP (processo estabelecimento conexão: SYN → SYN-ACK → ACK). Atacante envia milhões de pacotes SYN (solicitação conexão) com endereços IP falsificados, nunca completando handshake (não envia ACK final). Servidor mantém milhares de conexões "meio-abertas" (half-open) aguardando ACK que nunca chega, esgotando slots de conexão disponíveis. Usuários legítimos não conseguem conectar.

Ping of Death: Enviar pacotes ICMP maiores que tamanho máximo permitido (65.535 bytes). Servidores antigos com proteções inadequadas podem crashar ao processar pacotes oversized.

Smurf Attack: Enviar requisições ICMP Echo para endereço broadcast de rede (todos dispositivos recebem), falsificando IP vítima como remetente. Todos os dispositivos respondem simultaneamente para vítima, amplificando ataque.

Impacto: Mesmo com largura de banda suficiente (link gigabit, terabit), servidor fica inacessível por esgotamento recursos computacionais (CPU 100%, memória RAM esgotada, tabela conexões cheia).

Tipo 3 — Ataques de Camada de Aplicação (Application Layer Attacks / Layer 7):

Objetivo: Exaurir recursos de aplicações web específicas através de requisições HTTP/HTTPS aparentemente legítimas, mas computacionalmente custosas.

Vetores principais:

HTTP Flood: Enviar milhões de requisições GET/POST para páginas web dinâmicas que exigem processamento banco de dados intensivo (exemplo: página busca processos judiciais executando query SQL complexa a cada requisição). Servidor web processa cada requisição como legítima, esgotando CPU/memória/conexões banco dados.

Slowloris: Técnica "lenta e silenciosa": abrir múltiplas conexões HTTP com servidor e mantê-

las abertas indefinidamente enviando headers HTTP incompletos lentamente. Servidor aguarda headers completos, mantém conexão aberta, eventualmente esgota slots de conexão. Poucos computadores atacantes (até dezenas) conseguem derrubar servidores grandes.

RUDY (R-U-Dead-Yet?): Variante Slowloris focada em requisições POST: atacante envia formulário web gigante (POST) byte-a-byte extremamente devagar. Servidor aguarda corpo completo POST, mantém conexão aberta, esgota recursos.

Sofisticação: Ataques Layer 7 imitam comportamento usuários legítimos (requisições HTTP normais, user-agents navegadores reais, cookies válidos), dificultando distinção por firewalls tradicionais (não identificam como "tráfego malicioso" pois tecnicamente é HTTP válido).

Botnets: redes zumbis distribuídas e recordes alarmantes

Botnet (bot + network) é rede de dispositivos comprometidos (computadores, smartphones, servidores, dispositivos IoT: câmeras IP, roteadores domésticos, DVRs, TVs smart, geladeiras conectadas) infectados por malware e controlados remotamente por botmaster (operador da rede, criminoso/Estado-nação). Dispositivos comprometidos são "bots" ou "zumbis"; proprietários geralmente desconhecem que seus dispositivos fazem parte de botnet.

Arquitetura típica botnet:

Componente 1 — Malware infectante:

Vírus/worm que infecta dispositivos via: phishing, exploração vulnerabilidades (roteadores com firmware desatualizado, senhas padrão não alteradas "admin/admin"), drive-by download (sites maliciosos).

Componente 2 — Bots (zumbis):

Dispositivos infectados executando malware, aguardando comandos botmaster. Podem ser: PCs Windows/Mac, servidores Linux, smartphones Android, câmeras IP (Mirai explorou massivamente), roteadores domésticos.

Componente 3 — C&C (Command-and-Control server):

Servidor(es) controlando botnet. Botmaster envia comandos via C&C: "atacar IP X.X.X.X com SYN Flood por 24 horas". Bots recebem comandos, executam sincronizadamente. C&C frequentemente usa: servidores bulletproof hosting (Rússia, países ex-soviéticos, China — provedores que ignoram reclamações legais), infraestrutura Tor (anonimização), domínios fast-flux (IPs mudam constantemente dificultando bloqueio).

Evolução temporal botnets paradigmáticas:

Mirai (agosto/2016-presente):

Primeiro botnet IoT massivo. Malware escrito em C, código-fonte vazado publicamente outubro/2016 (github), permitindo variantes proliferarem. Infectou ~600.000 dispositivos IoT (câmeras IP, DVRs) explorando senhas padrão fracas (lista 60+ combinações comuns: admin/admin, root/root, admin/password). Ataques notórios: Dyn outubro/2016 (1 Tbps), OVH setembro/2016 (1,1 Tbps — provedor hosting francês). Criadores (3 jovens EUA) presos

dezembro/2017, condenados, mas botnet persiste (variantes Mirai continuam ativas 2025).

3ve (2014-2018):

Botnet fraude publicitária (ad fraud). Rede de 1,7 milhão de IPs infectados simulando cliques anúncios, gerando USD 29 milhões/dias receitas fraudulentas para criminosos. Desmantelado novembro/2018 por operação FBI + Google + parceiros internacionais. 8 indivíduos indiciados (Rússia, Cazaquistão).

TrickBot (2016-2020):

Botnet foco instituições financeiras, roubo credenciais bancárias, ransomware (entregava Ryuk/Conti ransomware para vítimas de alto valor). ~1 milhão de dispositivos pico. Desmantelado parcialmente outubro/2020 por operação Microsoft + FinCEN + parceiros, mas infraestrutura ressurgiu.

Maior botnet descoberta em 2024:

Pesquisadores cibersegurança identificaram botnet com 1,33 milhão de dispositivos comprometidos globalmente (Cybernews, 2025; Asper, 2025), superando todos os recordes anteriores. Composição: IoT (câmeras, roteadores) + servidores cloud comprometidos. Capacidade destrutiva: potencial ataques múltiplos Tbps.

Capacidade destrutiva atual:

Botnets de 1+ milhão dispositivos podem gerar ataques DDoS de 3-5 Tbps. Cloudflare (provedor proteção DDoS) reportou ataque recorde 3,8 Tbps em setembro/2024, maior já mitigado (Cloudflare, 2025).

Aluguel de botnets (DDoS-for-hire / booter services):

Mercado clandestino (fóruns Tor, Telegram) oferece aluguel botnets por USD 50-500/hora. Qualquer indivíduo com conhecimento técnico mínimo (saber usar Tor, pagar Bitcoin) pode lançar ataque DDoS massivo contra alvos arbitrários. Democratização do cibercrime: não exige mais ser "hacker expert"; booter service fornece interface web amigável (escolher IP-alvo, duração ataque, tipo vetor, clicar "atacar").

Brasil: país mais atacado América Latina e ataques diários TJPR revelados

Dados estatísticos consolidados contextos Brasil:

Netscout DDoS Threat Intelligence Report 2025.1:

O Brasil registrou aproximadamente **550 mil ataques DDoS no primeiro semestre de 2025**, consolidando-se como o país mais visado da América Latina (Netscout, 2025). A média nacional supera **3 mil incidentes diários**, demonstrando a crescente vulnerabilidade das infraestruturas críticas brasileiras.

Cloudflare DDoS Threat Report 2025 Q1:

Dados recentes da Cloudflare corroboram essa tendência global. Conforme demonstrado na Figura 1, a empresa mitigou 20,5 milhões de ataques DDoS apenas no primeiro trimestre de 2025, representando aumento de 358% em comparação ao mesmo período de 2024 e de 198% em relação ao último trimestre do ano anterior (CLOUDFLARE, 2025).

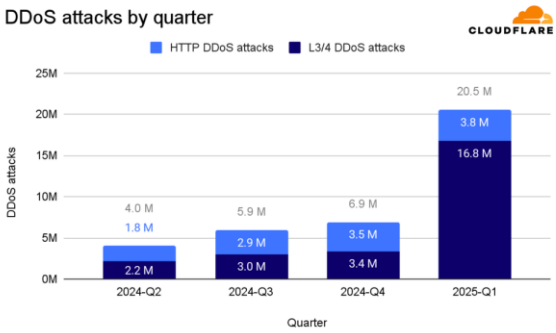

Figura 1 – Crescimento exponencial de ataques DDoS mitigados pela Cloudflare (Q1/2024 - Q1/2025) Fonte: Cloudflare (2025) apud Canaltech (2025)

Qrator Labs:

Segundo o levantamento da Qrator Labs (2025), o Brasil está entre os países com maior volume proporcional de ataques por habitante. Comparativamente, os Estados Unidos (330 milhões de habitantes) registraram cerca de 2 milhões de ataques semestrais, enquanto o Brasil (215 milhões de habitantes) sofreu 550 mil. Assim, embora o volume absoluto seja inferior, o impacto relativo considerando o nível de infraestrutura digital é desproporcional.

Revelação inédita — ataques DDoS diários no TJPR

A entrevista estruturada com o Chefe da Divisão de Gestão da Segurança da Informação da SETI/TJPR (outubro/2025) revelou um dado inédito e relevante para compreender a magnitude da ameaça DDoS ao Judiciário brasileiro:

"Sofremos diariamente com estes incidentes [ataques DDoS], mas nem todos geram problemas que podem afetar a todos. [...] A maior parte destes ataques não é passível de identificação por se originarem em redes zumbi [botnets], motivo pelo qual, quando constatado o ataque, a forma mais segura é aplicar medidas de contenção" (Entrevista TJPR, outubro/2025, grifo nosso).

A declaração indica que **ataques DDoS são rotineiros**, porém a maioria é **mitigada automaticamente por sistemas anti-DDoS** (firewalls, provedores de borda, rate limiting), sem impacto perceptível aos usuários. Apenas episódios de maior volume ou duração exigem **ação manual de contenção**, como a **restrição parcial de acessos externos** entre **21 e 22 de outubro de 2025**, quando foram implementadas **medidas emergenciais de contingência técnica** —denominadas em relatórios como modo continuidade.

Interpretação técnica e implicações

Ataques DDoS como rotina invisível:

Os incidentes são frequentes e, na maioria dos casos, neutralizados automaticamente. Essa "normalização da vulnerabilidade" gera risco de complacência institucional: os ataques só ganham visibilidade quando produzem lentidão perceptível.

Aplicação pontual de medidas de contingência:

O gestor esclareceu que, quando o volume de tráfego ultrapassa a banda contratada de mitigação, pode ser necessário aplicar **restrições temporárias de acesso remoto**. Isso ocorreu pontualmente em outubro de 2025.

Tais medidas, embora preventivas, **reduzem temporariamente a acessibilidade dos sistemas judiciais externos** e **afetam o ritmo de tramitação processual**.

Natureza gradual e preventiva do modo continuidade:

O modo continuidade (ou plano de continuidade de negócios) constitui conjunto estruturado de protocolos técnicos e operacionais acionados em diferentes níveis de severidade, desde medidas simples e transparentes (migração automática de servidor entre hardwares, ativação de sistemas redundantes) até ações complexas e restritivas (isolamento parcial de rede, bloqueio temporário de acessos externos, priorização de fluxos internos essenciais). Tais procedimentos não constituem 'excepcionalidade absoluta', mas sim camadas de resiliência previamente planejadas, aplicadas conforme a gravidade do incidente, seguindo o princípio de menor impacto necessário para resposta segura ao evento, conforme boas práticas de resposta a incidentes (NIST SP 800-61).

Impunidade e limites investigativos:

A rastreabilidade dos ataques permanece um desafio global. Conforme o entrevistado, a maioria das ofensivas se origina de **botnets internacionais** — redes zumbi compostas por milhões de dispositivos IoT — o que torna a investigação transnacional quase inviável sem cooperação entre agências (FBI, Europol, Interpol). No Brasil, a **ausência de tipo penal específico para DDoS** agrava a sensação de impunidade.

Consequências jurídicas e constitucionais

As instabilidades de outubro de 2025 representaram um **comprometimento material, ainda que temporário, do direito fundamental de acesso à justiça** (art. 5º, XXXV, CF/1988), especialmente para advogados, magistrados e servidores em trabalho remoto.

Ainda que os sistemas não tenham sido bloqueados integralmente, a limitação funcional afetou o exercício de direitos e a **eficiência administrativa** (art. 37, CF/1988).

Esses eventos reforçam a necessidade de protocolos de resiliência digital que integrem organicamente segurança cibernética e continuidade jurisdicional, reconhecendo que a segurança não se opõe à continuidade, mas constitui sua própria garantia. O desafio consiste em alinhar planejamento operacional e infraestrutura técnica de modo que controles avançados de segurança (MFA, bloqueios geográficos, filtragem de tráfego) não produzam impactos desproporcionais na acessibilidade dos sistemas, exigindo procedimentos alternativos previamente estruturados (VPNs institucionais, credenciais secundárias, acessos contingenciais) que permitam aos usuários legítimos manter funcionalidade mesmo sob restrições emergenciais.

Phishing à população civil: epidemia silenciosa geradora de litigâncias massa Juizados

Definição técnica e prevalência alarmante Brasil 2024-2025

Phishing é técnica de engenharia social (manipulação psicológica humana, não técnica computacional) onde criminosos enviam links maliciosos ou mensagens fraudulentas (via e-mail, SMS, WhatsApp, redes sociais, chamadas telefônicas) imitando comunicações legítimas de bancos, empresas, órgãos públicos (Receita Federal, INSS, Poder Judiciário), com objetivo

enganar vítimas a: **(i)** Clicar em link instalando malware (vírus bancário rouba senhas digitadas, captura tela, intercepta SMS tokens); **(ii)** Fornecer voluntariamente dados sensíveis (senhas, CPF, cartão crédito, códigos SMS autenticação); **(iii)** Realizar transferências financeiras para contas controladas por criminosos (falso funcionário banco ligando alegando "fraude detectada, transfira para conta segura").

Epidemia estatística Brasil:

Kaspersky Panorama Ameaças Cibernéticas 2025:

553 milhões de ataques de phishing bloqueados no Brasil em 12 meses (julho/2024-agosto/2025), média 1,5 milhão/dia, 2,6 ataques por habitante (Kaspersky, 2025; Instituto Longevidade, 2025). Brasil lidera América Latina ataques phishing, seguido México, Argentina.

América Latina agregada: 1,29 bilhão de tentativas phishing bloqueadas (julho/2024-agosto/2025), aumento 85% comparado período anterior (Kaspersky, 2025).

DataSenado (01/out/2024): Pesquisa representativa população brasileira: "Golpes digitais vitimaram 24% dos brasileiros com mais de 16 anos nos últimos 12 meses. São mais de 40,85 milhões de pessoas que perderam dinheiro em função de algum crime cibernético" (DataSenado, 2024).

Serasa (2024): 54,2% da população brasileira vítima de fraudes digitais em 2024, com prejuízos financeiros reportados (Serasa, 2024).

Sociedade Brasileira de Computação (2024): 16% dos incidentes de segurança no Brasil são phishing, com custo médio R$ 7,75 milhões por violação (dados empresariais; custo per capita populacional menor, mas agregado significativo) (SBC, 2024).

Fenati (2025): Brasil registrou 5 milhões de fraudes digitais em 2024, aumento 45% comparado 2023 (Fenati, 2025).

Comparação internacional alarmante:

Brasil ~215 milhões habitantes, 553 milhões tentativas phishing/ano = 2,6 tentativas/habitante.

EUA ~330 milhões habitantes, ~1,5 bilhões de tentativas phishing/ano = 4,5 tentativas/habitante.

Brasil sofre proporcionalmente menos que EUA (população mais digitalizada), mas volume absoluto é alarmante considerando que 24% da população brasileira foi efetivamente vitimada (não apenas tentativas bloqueadas, mas fraudes bem-sucedidas).

IA turbinando phishing: mensagens mais convincentes, escala massiva, personalização

Inteligência Artificial generativa (ChatGPT, Claude, Gemini) permite criminosos criarem mensagens phishing mais convincentes com linguagem gramaticalmente perfeita, personalizadas por região/setor, em escala massiva automatizada, reduzindo barreiras técnicas (não precisa mais ser "escritor fluente português" para criar e-mail convincente; IA escreve) (InfoMoney, 2025; Fenati, 2025).

Técnicas IA-powered:

(1) Geração e-mails phishing indistinguíveis de legítimos:

IA treinada em milhares de e-mails corporativos reais (bancos, Receita Federal, tribunais) gera mensagens mimetizando estilo, formatação, vocabulário específico de cada instituição. Taxa detecção humana: difícil (mesmo usuários treinados confundem).

(2) Personalização em massa (spear phishing automatizado):

IA cruza dados vazados (data breaches anteriores: CPF, nome completo, endereço, banco onde tem conta) com mensagens personalizadas: "Olá [NOME REAL], detectamos movimentação suspeita em sua conta [BANCO REAL] terminada [ÚLTIMOS 4 DÍGITOS REAIS]. Clique para verificar". Personalização aumenta taxa sucesso de ~3% (phishing genérico) para ~30-40% (spear phishing personalizado).

(3) Plataformas Phishing-as-a-Service (PhaaS):

Mercado clandestino oferece infraestrutura phishing pronta: templates e-mails IA-gerados, páginas login falsas indistinguíveis de bancos reais, sistemas automatizados envio milhões e-mails, painéis administrativos rastreando vítimas clicaram/forneceram dados. Preço: USD 100-500/mês assinatura. Democratização do phishing (não exige mais conhecimento técnico; qualquer criminoso com USD 100 pode operar campanha phishing massiva).

Cadeia causal phishing → fraude → litigância Juizados: evidência empírica

Etapa 1 — Ataque phishing bem-sucedido:

Cidadão recebe SMS falsificado ("Banco Bradesco: movimentação suspeita detectada. Acesse [LINK] para bloquear"), clica link, redireciona para página login idêntica visualmente ao site Bradesco real (mesmas cores, logo, layout), fornece CPF + senha + código SMS token, criminoso captura credenciais.

Etapa 2 — Fraude financeira executada:

Criminoso utiliza credenciais roubadas para: (a) transferir saldo conta vítima via PIX/TED para contas-laranja (mulas financeiras recrutadas, ganham 10-20% valores transferidos); (b) compras online fraudulentas de cartões crédito (bens físicos enviados para endereços controlados, revendidos mercado clandestino); (c) empréstimos consignados fraudulentos (liberados em nome vítima, creditados conta criminoso); (d) abertura contas/cartões novos nome vítima (roubo identidade).

Etapa 3 — Vítima identifica fraude (dias/semanas após):

Recebe notificação banco (cobranças indevidas, saldo zerado, empréstimo não solicitado aprovado, negativação SPC/Serasa), telefona SAC, banco nega responsabilidade alegando "culpa exclusiva consumidor" (fornecimento voluntário senha viola termos uso).

Etapa 4 — Tentativa resolução extrajudicial frustrada:

Vítima registra B.O. (boletim ocorrência), protocola reclamação banco via Procon, banco mantém negativa ("cliente forneceu senha, responsabilidade dele").

Etapa 5 — Ajuizamento ação Juizado Especial Cível:

Vítima, insatisfeita, ajuíza ação nos Juizados Especiais Cíveis (competência: causas até 40 salários-mínimos ≈ R$ 56.000 em 2025, Art. 3º Lei 9.099/95, procedimento simplificado, gratuidade custas) buscando:

Restituição valores debitados fraudulentamente (R$ 5.000-50.000 típico);

Cancelamento dívidas/empréstimos fraudulentos (evitar negativação);

Indenização danos morais (CDC Art. 6º VI + VIII: inversão ônus prova, responsabilidade objetiva fornecedor). Valores típicos danos morais fraude: R$ 3.000-15.000 (jurisprudência STJ).

Fundamentação jurídica vítimas:

Código Defesa Consumidor (Lei 8.078/1990) Art. 14: "Fornecedor de serviços responde, independentemente de existência de culpa, pela reparação dos danos causados aos consumidores por defeitos relativos à prestação dos serviços". Argumento: banco tem dever de segurança, falha em proteger sistema contra fraudes configura defeito na prestação serviço, responsabilidade objetiva.

Jurisprudência favorável vítimas (STJ pacificado):

STJ consolidou entendimento: responsabilidade objetiva instituição financeira por fraudes eletrônicas, mesmo quando cliente fornece senha (fragilização sistema segurança é risco inerente atividade bancária). REsp 1.197.929/PR (2010), REsp 1.197.929/PR (2013 — Leading case), Súmula 479 STJ: "As instituições financeiras respondem objetivamente pelos danos gerados por fortuito interno relativo a fraudes e delitos praticados por terceiros no âmbito de operações bancárias".

Resultado típico: Juizados frequentemente condenam bancos restituir valores + danos morais (taxa êxito vítimas: ~60-70% casos consumeristas fraudes digitais).

Etapa 6 — Multiplicação de ações (efeito massa):

553 milhões tentativas phishing/ano × taxa sucesso conservadora 1% (mesmo bloqueios, educação usuários) = ~5,5 milhões fraudes bem-sucedidas/ano × taxa judicialização conservadora 10% (maioria vítimas não aciona Judiciário por desconhecimento direitos, valores pequenos, descrença eficácia) = ~550.000 ações Juizados Cíveis/ano atribuíveis a fraudes digitais.

CNJ Justiça em Números 2024: Juizados Especiais Federais tiveram aumento 1,7 milhão processos em 2023 (36,5%) (CNJ, 2024). Parcela significativa atribuível a: (a) fraudes digitais (phishing, golpes Pix); (b) demandas previdenciárias (revisões INSS); (c) demandas consumeristas bancos/telefonia.

Evidência adicional — R$ 1 bilhão prejuízos fraudes digitais:

Jornal Folha São Paulo (26/ago/2020): Pandemia COVID fez aumentar 70% fraudes eletrônicas, gerando perdas R$ 1 bilhão, com 600 mil fraudes apenas pagamento auxílio emergencial (Folha SP, 2020). Vítimas eventualmente buscam reparação judicial.

Círculo vicioso retroalimentado:

1. **Phishing massivo** (553 milhões de tentativas/ano) → 2. **Fraudes bem-sucedidas** (milhões de vítimas) → 3. **Judicialização em massa** (centenas de milhares de ações/ano) → 4. **Sobrecarga da infraestrutura judicial digital** (tempo médio de tramitação aumenta, congestionamento de sistemas) → 5. **Redução da resiliência tecnológica** (infraestruturas sobrecarregadas tornam-se mais suscetíveis a lentidões e ataques DDoS) → 6. **Ataques DDoS agravam a instabilidade sistêmica**, exigindo, em casos extremos, **medidas de contenção temporária (restrição de acesso remoto)** para proteger a integridade do sistema → 7. **A morosidade se intensifica**, ampliando a insatisfação dos cidadãos e retroalimentando a litigância → 8. **O ciclo repete-se**, combinando causas socioeconômicas (fraudes) e tecnológicas (vulnerabilidades cibernéticas) em uma espiral de sobrecarga estrutural do sistema de justiça.

Economia do cibercrime: análise custo-benefício, dissuasão inadequada e impunidade estrutural

Modelo econômico racional do crime: Becker (1968) aplicado ao ciberespaço

Economista Gary Becker (Prêmio Nobel Economia 1992) formulou teoria revolucionária (1968): criminosos são agentes racionais que ponderam custos vs. benefícios antes de cometer crimes, maximizando utilidade esperada (Becker, 1968).

BE = Benefício Bruto x Probabilidade de Sucesso

CE = Pena x Probabilidade de Captura/Condenação

Aplicação ao contexto brasileiro (ransomware e ataques cibernéticos)

No caso de um grupo Ransomware-as-a-Service (RaaS) atuando contra tribunais:

Benefício esperado (BE): resgate médio de USD 4 milhões; probabilidade de pagamento de 30% → BE = USD 1,2 milhão.

Custo esperado (CE): pena média de 3,5 anos × probabilidade de condenação 0,05 = 0,175 anos (≈ 2 meses).
→ Custo marginal ínfimo, incentivo máximo.

Nos EUA, sob a Computer Fraud and Abuse Act (§1030), o custo esperado é 3,75 anos, cerca de 21 vezes maior, reduzindo fortemente a atratividade da conduta.

Essa assimetria evidencia a falência dissuasória brasileira: penas baixas e probabilidade de punição residual transformam o país em alvo preferencial de grupos RaaS internacionais.

Custos econômicos diretos e indiretos

Custos diretos

Evento	**Estimativa (R$ milhões)**	**Observação**
STJ 2020 – RansomExx	5–10	Recuperação, consultoria, hardware e reconstrução de dados
TJPR 2024 –	23 (desvio efetivo) + 184	Custos de fraude e

Evento	Estimativa (R$ milhões)	Observação
Incidente dos Alvarás	(bloqueio preventivo)	investigação policial
TJPR 2025 – Medidas de contingência (restrição parcial de acesso remoto)	10–15 (estimativa indireta)	Perda de produtividade potencial: 100 magistrados × R$ 30 mil/mês + 500 servidores × R$ 8 mil/mês, por 4 dias úteis

Total direto estimado: R$ 38–48 milhões.

Nota: valores relativos; a última estimativa baseia-se em perda de produtividade e não em custo contábil comprovado.

Custos indiretos

O Poder Judiciário consome entre **1,3% e 1,6% do PIB** (≈ R$ 156–192 bilhões/ano) — quatro a cinco vezes mais que a média internacional — com tempo médio de tramitação **três vezes superior** ao europeu (600 × 232 dias). Entre 10% e 20% desse custo decorre de fatores cibernéticos e digitais, como:

Ataques que causam paralisações e instabilidades (STJ 2020, TJPR 2025);

Litigâncias massivas por fraudes digitais e demandas predatórias.

Estimativa conservadora: **15% de R$ 160 bilhões = R$ 24 bilhões/ano** em custos sistêmicos associados à disfunção digital e cibernética.

Litigância predatória

No TJMG (2022), 17% dos processos estaduais foram classificados como litigância predatória, com custo de R$ 10,7 bilhões (Pereira & Lelis, 2025). Em comarcas do TJSP, a distribuição de 50 mil ações padronizadas elevou o tempo médio de sentença em 155%, demonstrando o impacto econômico direto do uso abusivo da jurisdição.

Custos intangíveis

Erosão da confiança institucional:

Casos como o ataque ao STJ (2020), o desvio no TJPR (2024) e as medidas emergenciais de 2025 abalaram a percepção pública de segurança judicial. Pesquisas da FGV e Datafolha indicam apenas **30–40% de confiança** no Judiciário, contra 60–70% em países desenvolvidos.

Comprometimento funcional do acesso à justiça:

Durante as medidas de contenção de outubro/2025, houve restrição temporária de acesso remoto, afetando advogados, partes e magistrados em teletrabalho. Tal restrição configura **limitação material e transitória do direito de petição e duração razoável do processo** (CF/1988, arts. 5º, XXXV e LXXVIII).

Desestímulo profissional:

A sobrecarga digital, a insegurança tecnológica e a lentidão sistêmica produzem desmotivação, antecipação de aposentadorias e dificuldade de atrair novos talentos jurídicos.

Síntese conceitual: a tripla ameaça como fenômeno sistêmico

A Seção 2 evidencia que as ameaças cibernéticas ao acesso à justiça brasileira constituem um **ecossistema integrado** de riscos:

Ransomware (STJ 2020) paralisa diretamente sistemas críticos;

Ataques DDoS (TJPR 2025) demandam **medidas emergenciais de restrição de acesso remoto**, com reflexos sobre a continuidade jurisdicional;

Phishing em massa (553 milhões/ano) gera **litigância explosiva** nos Juizados Especiais.

Esses vetores interagem numa **espiral descendente**:

Ataques institucionais → lentidão → aumento de litigâncias → sobrecarga → vulnerabilidade → novos ataques.

Impunidade estrutural (ausência de condenações, dificuldade de rastreamento de botnets) → custo esperado próximo de zero → incentivo econômico ao crime.

Legislação inadequada (Lei 12.737/2012 sem tipificação de ransomware e DDoS, penas desproporcionais, lacunas de dissuasão).

Pierre Lévy (2001) é aqui revisitado: o Judiciário brasileiro tornou-se o **"universal vulnerável"** do ciberespaço — acesso digitalmente universalizado, mas sem uma governança de segurança proporcional. A mesma infraestrutura que democratizou o acesso transformou-se em vetor potencial de exclusão, evidenciando a contradição fundamental da justiça digital contemporânea.

Custos econômicos diretos e indiretos: quantificação multidimensional

Os custos econômicos decorrentes dos incidentes cibernéticos no Poder Judiciário brasileiro podem ser divididos em diretos, indiretos e intangíveis, refletindo tanto o impacto financeiro imediato quanto as consequências estruturais de longo prazo sobre a eficiência e a confiança institucional.

Custos diretos (recuperação pós-incidente):

No caso do Superior Tribunal de Justiça (2020), estimam-se entre R$ 5 e R$ 10 milhões em despesas relacionadas à contratação de consultorias especializadas (Microsoft e Atos), substituição de hardware, horas extras de servidores e reconstrução manual de dados comprometidos.

No Tribunal de Justiça do Paraná (2024), o denominado Incidente dos Alvarás resultou em R$ 23 milhões efetivamente desviados — valores não recuperáveis até outubro de 2025, em razão da dispersão por criptomoedas — e outros R$ 184 milhões bloqueados preventivamente. Soma-se a isso o custo da investigação policial, que envolveu 29 mandados de prisão e 16 prisões em cinco estados.

Em outubro de 2025, durante medidas de contingência digital implementadas pelo TJPR diante de ataques massivos, houve restrição temporária de acesso remoto aos sistemas judiciais por quatro dias consecutivos. A estimativa indireta de perdas de produtividade situa-se entre R$ 10 e R$ 15 milhões, considerando a média salarial de cerca de 100 magistrados (R$ 30.000/mês) e 500 servidores (R$ 8.000/mês), além do custo de oportunidade decorrente de processos atrasados.

O total direto documentado nos três casos — STJ 2020, TJPR 2024 e TJPR 2025 — situa-se entre R$ 38 e R$ 48 milhões. Ressalta-se, contudo, que parte dessas cifras é estimativa indireta, não havendo divulgação pública oficial de balanços consolidados.

Custos indiretos (morosidade judicial sistêmica):

De acordo com o Tesouro Nacional (2025), o Poder Judiciário brasileiro consome anualmente entre 1,3% e 1,6% do Produto Interno Bruto, o equivalente a R$ 156 a R$ 192 bilhões (base PIB 2024 de R$ 12 trilhões). O Brasil gasta de quatro a cinco vezes mais que a média global em manutenção da estrutura judicial, mas apresenta tempo médio de tramitação três vezes superior ao europeu — cerca de 600 dias na primeira instância nacional contra 232 dias na média da União Europeia.

Parte expressiva desse custo está associada a fatores tecnológicos e digitais. Estima-se que de 10% a 20% da morosidade total decorra de dois elementos principais: (i) ataques cibernéticos que causam paralisações, instabilidades e necessidade de contingência, como nos casos do STJ (2020) e TJPR (2025), cujos efeitos cascata prolongam prazos processuais; e (ii) a sobrecarga gerada pela litigância digital massiva, em especial as ações consumeristas motivadas por golpes de phishing e a litigância predatória. Uma estimativa conservadora atribui 15% do custo total da morosidade (R$ 160 bilhões) a fatores cibernéticos diretos e indiretos, equivalendo a aproximadamente R$ 24 bilhões anuais.

Litigância predatória específica:

Em 2022, o Tribunal de Justiça de Minas Gerais constatou que 17% dos processos estaduais correspondiam a litigância predatória, totalizando cerca de 1,3 milhão de ações e um custo mínimo de R$ 10,7 bilhões aos cofres públicos (Pereira & Lelis, 2025). Na comarca de São Paulo, a atuação de grupos de advogados que distribuíram mais de 50 mil ações padronizadas elevou o tempo médio para prolação de sentenças de 364 dias (2012) para 930 dias, representando um aumento de 155% no período.

Custos intangíveis (não mensuráveis, porém críticos):

A sucessão de incidentes cibernéticos produziu impactos que transcendem o campo econômico. A confiança institucional foi significativamente abalada: a percepção de um Judiciário incapaz de proteger a si mesmo — após episódios como o ataque ao STJ (2020), o desvio de R$ 23 milhões no TJPR (2024) e as medidas de contingência digital de 2025 — reforçou dúvidas sobre sua capacidade de proteger os cidadãos. Pesquisas da FGV e do Datafolha indicam níveis de confiança pública oscilando entre 30% e 40%, índices consideravelmente inferiores aos de países desenvolvidos, que variam entre 60% e 70%.

Também houve comprometimento funcional do acesso à justiça: as restrições temporárias de acesso remoto afetaram advogados, partes e magistrados em teletrabalho, ocasionando dificuldades para o protocolo de petições urgentes e a continuidade processual. Tal cenário representa uma limitação material e transitória dos direitos previstos nos artigos 5º, incisos XXXV e LXXVIII, da Constituição Federal de 1988.

Por fim, a insegurança tecnológica, somada à sobrecarga de processos e à precariedade estrutural, gera desestímulo à permanência na carreira pública. Magistrados e servidores relatam fadiga institucional, antecipação de aposentadorias e perda de atratividade das funções judiciais, fenômeno que ameaça a renovação de quadros e a sustentabilidade de longo prazo da administração da justiça.

Síntese conceitual: a tripla ameaça como fenômeno sistêmico integrado

A análise desenvolvida ao longo da Seção 2 demonstra que as ameaças cibernéticas ao acesso à justiça no Brasil configuram um fenômeno sistêmico e interdependente. O ransomware (caso STJ, 2020) paralisa tribunais de forma direta; os ataques DDoS (caso TJPR, 2025) podem exigir medidas emergenciais de restrição de acesso remoto; e o phishing em larga escala — estimado em 553 milhões de tentativas anuais — produz uma litigância explosiva que congestiona os Juizados Especiais.

Esses três vetores interagem em uma dinâmica de retroalimentação contínua: ataques institucionais geram lentidão; a lentidão acentua a frustração das partes; a frustração impulsiona novas ações; a sobrecarga reduz a resiliência técnica das infraestruturas, que se tornam mais vulneráveis a novos ataques, aprofundando a espiral descendente.

A impunidade estrutural reforça esse ciclo, pois a ausência de condenações efetivas por crimes cibernéticos e a dificuldade de rastreamento técnico tornam o custo esperado da conduta praticamente nulo. Soma-se a isso a inadequação legislativa: a Lei nº 12.737/2012 não tipifica ransomware ou DDoS, e as penas previstas (2 a 5 anos) são significativamente inferiores às adotadas por jurisdições estrangeiras (10 a 20 anos nos EUA), inviabilizando uma dissuasão efetiva mesmo quando há autoria identificada.

Pierre Lévy, revisitado sob essa ótica, descreve o Judiciário brasileiro como um "universal vulnerável": um sistema que universalizou o acesso (99,9% dos processos eletrônicos e consultas remotas), mas sem consolidar uma governança cibernética proporcional. A ausência de monitoramento contínuo (SOC 24x7), autenticação multifator universal, pen tests regulares e políticas de backup segregado evidencia uma contradição estrutural. A mesma digitalização que democratizou o acesso à justiça tornou-se, paradoxalmente, o vetor que ameaça sua continuidade.

TRÊS ESTUDOS DE CASO INSTITUCIONAIS: CRONOLOGIA, IMPACTO E IMPUNIDADE SISTÊMICA

STJ (novembro/2020): ataque de ransomware e paralisação nacional

Cronologia e anatomia técnico-operacional (RansomExx)

Em 3 de novembro de 2020, por volta de 14h30, durante sessões de julgamento, o Superior Tribunal de Justiça (STJ) sofreu um ataque de ransomware associado à família RansomExx/Defray777, frequentemente operada de modo humano (human-operated) e

historicamente observada contra governos e infraestruturas críticas. O comunicado institucional não divulgou o vetor de intrusão. Hipóteses tecnicamente plausíveis, à luz do modus operandi reportado em bases técnicas, incluem: (i) spear phishing direcionado com anexo malicioso e elevação de privilégios; (ii) exploração de serviços de acesso remoto (VPN/RDP) com vulnerabilidades conhecidas e ausência de MFA.

Após o comprometimento inicial — possivelmente dias/semanas antes da detonação — é compatível com esse tipo de operação: elevação de privilégios, reconhecimento da rede, movimentação lateral e identificação de ativos críticos (virtualização, bancos de dados, correio eletrônico, GED). Em ataques dessa família, a tentativa de neutralização prévia de backups conectados à rede costuma anteceder a criptografia ampla, com o objetivo de dificultar a restauração.

A detonação teria sido coordenada para execução simultânea em múltiplos hosts e/ou VMs, com criptografia por esquema híbrido (algoritmo simétrico para dados e assimétrico para proteger as chaves), padrão em campanhas modernas de ransomware. Os valores de resgate, prazos e canais de negociação não foram informados oficialmente; estimativas usualmente citadas para alvos desse porte apontam faixas de milhões de dólares, mas não há confirmação pública específica para o caso do STJ.

Impacto operacional e consequências institucionais

O impacto inicial envolveu indisponibilidade do site institucional, suspensão de sessões de julgamento e interrupção do acesso aos sistemas processuais e ao correio institucional. O Conselho Nacional de Justiça editou a Resolução nº 354/2020 suspendendo prazos até a normalização, mitigando prejuízos processuais imediatos.

Em termos de magnitude, é metodologicamente aceitável empregar estimativas ilustrativas para dimensionar efeitos (ex.: atraso potencial agregado em milhares de feitos ao considerar a capacidade média diária de julgamento), desde que se ressalte o caráter não contábil desses números.

As consequências institucionais foram relevantes: (i) abalo reputacional de um tribunal superior, com ampla cobertura midiática; (ii) atrasos jurisdicionais em processos relevantes; (iii) custos extraordinários de recuperação com consultorias, reposição de equipamentos, esforço 24×7 e reconstruções manuais parciais; e (iv) efeitos intangíveis sobre a percepção de continuidade do serviço jurisdicional em ambiente digital.

Resposta institucional e hardening pós-incidente

As medidas relatadas como compatíveis com boas práticas após eventos dessa natureza incluem: MFA obrigatória em acessos remotos; segmentação de rede para isolar domínios críticos; política de backups segregados/offline com testes regulares de restauração; monitoramento centralizado (SIEM) com correlação de eventos e alarmes de comportamento anômalo; e testes de invasão

periódicos (pen tests) por equipes externas independentes. O racional é reduzir superfície de ataque, encurtar tempo de detecção e restaurar serviços com menor perda de dados (RPO/RTO).

Impunidade estrutural (balanço cinco anos após)

Até outubro de 2025, não foram divulgadas prisões/indiciamentos/condenações relacionados a esse incidente. Fatores que ajudam a explicar a baixa probabilidade de responsabilização incluem: operações transnacionais mediadas por botnets e serviços anônimos, pagamentos pseudônimos em criptoativos, cooperação internacional assimétrica e arcabouço penal ainda desalinhado à gravidade dos impactos. Sob a ótica da análise econômica do crime, essa combinação reduz o custo esperado do infrator e aumenta o incentivo para ataques contra alvos brasileiros.

TJPR (2024): "Incidente dos Alvarás", risco de insider e certificados digitais

Cronologia e modus operandi sob investigação

Entre setembro/2023 e agosto/2024, investigações estaduais apuraram fraudes envolvendo alvarás judiciais com uso indevido de certificados ICP-Brasil. A hipótese investigativa descreve uma organização interestadual com papéis distribuídos (liderança, execução técnica, insiders, "mulas financeiras"). Os passos frequentemente reportados incluem: obtenção de credenciais por phishing e/ou vazamentos; emissão indevida de certificados com documentação falsificada; assinatura digital de alvarás com dados processuais reais e beneficiários adulterados; apresentação a instituições financeiras e dispersão de valores por múltiplos canais, inclusive criptoativos.

A menção a risco de insider — pessoa com acesso legítimo que facilita etapas do delito — deve permanecer expressamente vinculada às apurações oficiais, sem extrapolações não documentadas.

Valores e operação policial

Segundo informações publicamente divulgadas, os valores tentados somaram aproximadamente R$ 207 milhões; bloqueios preventivos alcançaram cerca de R$ 184 milhões; e desvios efetivos aproximaram-se de R$ 23 milhões, com dificuldade de recuperação pela rápida dispersão. Em 6 de agosto de 2024, houve operação policial com mandados de prisão e busca/apreensão em cinco estados, além da apreensão de equipamentos e documentos.

Resposta institucional: avanços relevantes e caráter reativo

Foram anunciados reforços de governança e segurança, entre eles: MFA obrigatória em sistemas críticos; contratação/estruturação de SOC 24×7; ampliação de equipe de segurança; testes de intrusão regulares; revisões de processo para emissão e conferência de alvarás (incluindo verificações adicionais) e coordenação com Autoridades Certificadoras para endurecimento dos procedimentos de emissão/validação. O conjunto sinaliza aprendizado institucional, embora com ênfase reativa — reforçando a relevância de padronização nacional via normativas do CNJ.

compensatórias ex. suspensão e prorrogação de prazos para tutela adequada do acesso jurisdição.

TRF-3 e TJPR (2025): DDoS, medidas de contingência digital e prazos

TRF-3 (março/2025) e TJPR (setembro/2025): comunicações oficiais e leitura técnica

Em 7 de março de 2025, o TRF-3 informou instabilidades associadas a picos de tráfego com reflexos nos sistemas processuais, com prorrogação de prazos para mitigar prejuízos às partes. A duração exata não foi detalhada publicamente.

No TJPR, em setembro de 2025, houve instabilidade do portal relatada como "volume anormal de acessos". Do ponto de vista técnico, expressões como "pico/volume anormal" podem ser compatíveis com eventos de DDoS, mas, na ausência de confirmação explícita, cabe registrar a distinção entre o dado oficial (instabilidade por volume anômalo) e a inferência técnica possível (hipótese DDoS).

Nos episódios de outubro de 2025, diante de ataques massivos, a resposta operacional adequada, seguindo boas práticas de segurança cibernética (princípio da ação de menor impacto capaz de responder de forma segura ao incidente), incluiu medidas graduais de contenção, desde filtragem intensificada até, em casos extremos e mediante aprovação hierárquica superior, restrição temporária de acesso remoto para preservar a integridade dos sistemas e a continuidade mínima de operações internas. Tais medidas, embora pontuais e emergenciais, afetam advogados, partes e magistrados em teletrabalho, exigindo comunicação transparente e soluções

TRF-3 (mar/2025) e TJPR (set/2025 e 21–24/out/2025): DDoS, instabilidades e medidas de contingência digital

TRF-3 — 7 de março de 2025. O Tribunal Regional Federal da 3ª Região comunicou instabilidades associadas a ataque DDoS, com reflexos no acesso ao PJe (consultas e protocolo). Como resposta institucional, houve prorrogação automática de prazos para evitar prejuízo às partes. A duração exata das instabilidades não foi divulgada publicamente; qualquer estimativa (horas/dia) deve ser tratada como aproximação.

TJPR — setembro de 2025. O portal do tribunal apresentou indisponibilidade temporária atribuída, no comunicado oficial, a "volume anormal de acessos". Tecnicamente, tal linguagem pode ser compatível com evento DDoS, mas não houve confirmação explícita de ataque; portanto, a hipótese DDoS deve permanecer como inferência técnica possível, distinta do dado oficial ("volume anormal").

TJPR — 21 a 24 de outubro de 2025. Diante de picos de tráfego malicioso e sucessivas instabilidades, foram adotadas medidas de contingência digital com restrição temporária de acesso remoto em determinados períodos ao longo de quatro dias. Segundo o gestor entrevistado, a estratégia operou como salvaguarda para preservar a integridade dos sistemas e manter a continuidade interna. Importa registrar que:

Acesso interno: magistrados e servidores presencialmente conectados à rede interna mantiveram operação, ainda que com oscilações pontuais de desempenho.

Acesso externo: advogados, partes e agentes em home office/teletrabalho enfrentaram restrições temporárias de acesso remoto e intermitências ao longo do período (não necessariamente indisponibilidade total e contínua).

Efeito jurídico-processual: as restrições remotas, ainda que pontuais, exigem comunicação transparente e medidas compensatórias (p. ex., prorrogações/suspensões de prazos), a fim de mitigar impactos sobre o direito de petição e a razoável duração do processo (CF/88, art. 5º, XXXV e LXXVIII).

Síntese constitucional e administrativa. As contingências digitais adotadas nesses episódios não equivalem, por si, a "negação literal" do acesso à justiça, mas configuram limitações materiais e temporárias ao acesso remoto, com potencial impacto sobre atos urgentes e produtividade. A análise adequada demanda: (i) clareza comunicacional sobre a natureza e a janela temporal das restrições; (ii) compensações processuais proporcionais; e (iii) reforço de resiliência (capacidade de absorver picos sem necessidade de bloqueios amplos).

Revelação do gestor do TJPR: ataques DDoS diários e a normalização do "ruído operacional"

A entrevista estruturada (out./2025) com o Chefe da Divisão de Gestão da Segurança da Informação da SETI/TJPR trouxe **dois achados centrais**:

Frequência elevada — "incidentes diários". Segundo o gestor, há **ocorrência diária** de tentativas/incidentes de DDoS. A **maioria** é **mitigada automaticamente** por camadas de defesa (firewall, provedores de mitigação, rate limiting), tornando-se **invisível** ao usuário comum. Isso gera uma **normalização do risco**, percebido internamente como **"ruído operacional"** quando não há impacto sistêmico amplo.

Contingência como padrão decisório em eventos massivos. Quando o **volume** ou a **duração** do ataque **extrapola a banda de mitigação contratada** e **eleva o risco** à disponibilidade/integridade dos sistemas, a **resposta operacional preferencial** tem sido acionar **medidas de contingência digital** com **restrição temporária de acesso remoto**, até o arrefecimento do fluxo hostil e a estabilização do tráfego.

Implicações.

Gestão de risco: o dado de "incidentes diários" não significa **indisponibilidade diária**, mas evidencia **pressão constante** sobre a borda de defesa e a necessidade de **planejamento de capacidade** (upgrades de mitigação, burst capacity, scrubbing centers).

Accountability e transparência: a distinção entre **incidente sem impacto** e **evento com impacto** deve orientar **protocolos de comunicação externa** e **acionamento automático** de **compensações processuais**.

Política pública: a frequência relatada **recomenda** (i) **contratos de mitigação** dimensionados a cenários de pico, (ii) **MFA**

universal, (iii) **SOC 24×7**, (iv) **testes de estresse** e (v) **planos de continuidade** que **reduzam a necessidade** de bloqueios amplos, priorizando **degradação graciosa** (serviços mínimos externos mantidos).

LEGISLAÇÃO BRASILEIRA: CINCO LACUNAS CRÍTICAS INCAPACITANTES E INADEQUAÇÕES ESTRUTURAIS

Lei 12.737/2012 — Origem (caso Carolina Dieckmann) e desatualização estrutural

A **Lei nº 12.737, de 30 de novembro de 2012**, resultou de tramitação excepcionalmente célere — cerca de seis meses — motivada pelo caso da atriz **Carolina Dieckmann**, cujo vazamento de imagens íntimas impulsionou debate nacional sobre crimes cibernéticos.

O diploma acrescentou ao Código Penal o **art. 154-A**, que tipifica a **invasão de dispositivo informático alheio**, com pena de detenção de 3 meses a 1 ano e multa. As qualificadoras (§§ 1º a 5º) preveem reclusão de 6 meses a 2 anos se houver obtenção de comunicações privadas, segredos comerciais ou dados sigilosos, causando prejuízo econômico ou envolvendo a Administração Pública.

Mesmo com as qualificadoras, a **pena máxima combinada (até 5 anos)** é manifestamente desproporcional frente à gravidade dos delitos modernos de ciberataque e à escala de danos potenciais a serviços públicos e infraestruturas críticas.

Cinco lacunas críticas que incapacitam a dissuasão efetiva

Lacuna 1 — Ransomware não tipificado especificamente

O ordenamento brasileiro **não dispõe de tipo penal autônomo** para ransomware. A prática combina invasão (art. 154-A), extorsão (art. 158) e dano (art. 163), mas nenhuma dessas figuras capta a natureza composta do delito — que envolve **criptografia coercitiva, destruição de backups e exigência de resgate em criptomoedas**.

A tipificação fragmentada gera **incerteza jurídica** e **penalidades desproporcionais**. A Convenção de Budapeste (art. 4º) recomenda que os Estados tipifiquem expressamente a **interferência em dados**, o que incluiria o ransomware em sua modalidade moderna. O Brasil, contudo, mantém a lacuna, punindo delitos que podem paralisar tribunais nacionais com penas equivalentes a crimes patrimoniais de pequeno valor.

Lacuna 2 — DDoS em vácuo legislativo

O **ataque de negação de serviço (DDoS)** não se enquadra em nenhum tipo penal existente. O art. 154-A exige violação de mecanismo de segurança, o que não ocorre em DDoS: trata-se de **sobrecarga volumétrica deliberada**, sem invasão.

Tentativas de subsunção ao **art. 266 do CP** ("interrupção de serviço telegráfico ou telefônico") ou ao **art. 163** ("dano") são tecnicamente inadequadas, pois o ataque não destrói fisicamente dados nem viola barreiras. Assim, **mesmo quando há identificação do agente**, falta tipo penal próprio para denúncia e

condenação, perpetuando **impunidade estrutural**.

Lacuna 3 — Penas desproporcionais em comparação internacional

As penas previstas na legislação brasileira (até 5 anos) contrastam fortemente com os parâmetros internacionais.

Estados Unidos: Computer Fraud and Abuse Act (CFAA, 18 U.S.C. §1030) — penas de até **20 anos** para ataques contra sistemas públicos ou críticos.

Singapura: Computer Misuse and Cybersecurity Act (Seção 8) — até **20 anos** em casos envolvendo infraestruturas críticas.

A desproporcionalidade compromete o caráter dissuasório da lei. Aplicando a lógica econômica de Becker (1968), a pena esperada (pena × probabilidade de captura) no Brasil é ínfima, insuficiente para inibir organizações transnacionais que lucram milhões de dólares por ataque.

Lacuna 4 — Vagueza terminológica e risco ao princípio da lex certa

A Lei nº 12.737/2012 utiliza expressões genéricas como "invasão", "dispositivo informático" e "mecanismo de segurança", sem definições técnicas claras. Ausência de termos como ransomware, malware, botnet, DDoS e zero-day dificulta a aplicação judicial precisa e fragiliza o princípio da lex certa (art. 1º, CP).

Embora essa imprecisão não configure inconstitucionalidade formal, ela reduz a efetividade penal e abre espaço para interpretações divergentes, comprometendo a coerência jurisprudencial.

Lacuna 5 — Foco individual em detrimento das estruturas organizacionais

O marco normativo brasileiro foi concebido sob o paradigma do "hacker individual", inadequado à realidade contemporânea de grupos criminosos estruturados. Modelos como o Ransomware-as-a-Service (RaaS) envolvem divisões de funções (desenvolvedores, afiliados, operadores e lavadores), o que exige abordagem penal integrada e penas cumulativas.

A aplicação combinada das Leis nº 12.737/2012 e nº 12.850/2013 (organização criminosa) é possível, mas não produz cumulatividade proporcional, pois a conduta principal (ataque cibernético) é punida de forma isolada, sem refletir a complexidade organizacional do crime.

LGPD — Inadequações no contexto judicial e lacunas de notificação

A Lei Geral de Proteção de Dados (Lei nº 13.709/2018) aplica-se ao Poder Judiciário (art. 23, II), mas as exceções para tratamento de dados em cumprimento de obrigação legal geram zona cinzenta de proteção.

Consentimento impossível: Jurisdicionados não consentem com o tratamento de seus dados, o que cria uma assimetria entre obrigação processual e tutela informacional.

Notificação vaga: O art. 48 exige comunicação de incidentes "em prazo razoável", expressão **indeterminada** frente aos padrões

internacionais — o **GDPR europeu** e a legislação de Singapura impõem prazos de 72 horas.

Essa imprecisão pode atrasar respostas a incidentes e agravar danos, como no caso relatado pelo CSJT (outubro/2025), em que falhas detectadas em agosto foram notificadas apenas dois meses depois.

Convenção de Budapeste — Ratificação sem implementação integral

A Convenção de Budapeste sobre o Cibercrime (Conselho da Europa, 2001), ratificada pelo Brasil em 22 de junho de 2021 e promulgada pelo Decreto nº 11.491/2023, estabelece parâmetros mínimos de criminalização:

Art. 2º — acesso ilegal a sistemas;

Art. 3º — interceptação ilegal de dados;

Art. 4º — interferência em dados;

Art. 5º — interferência em sistemas;

Art. 6º — uso indevido de dispositivos.

A legislação brasileira cobre parcialmente os arts. 2º e 3º, mas não incorporou integralmente os arts. 4º e 5º, que tratam de interferência em dados e sistemas — elementos centrais para tipificar ransomware e DDoS.

Assim, o Brasil cumpre a Convenção de forma formal, mas não substancial, permanecendo vulnerável e desalinhado das melhores práticas internacionais.

LEGISLAÇÃO COMPARADA: BRASIL DEFASADO 10-15 ANOS (TABELA SÍNTESE 16 DIMENSÕES)

Estados Unidos — Whole-of-Government Approach

O **Computer Fraud and Abuse Act (CFAA, 18 U.S.C. §1030, 1986)** constitui o principal marco regulatório norte-americano sobre crimes cibernéticos. O §1030(a)(5)(A) tipifica a "transmissão intencional de programa, informação, código ou comando capaz de causar dano a computador protegido", prevendo **pena de até 10 anos**, elevando-se a **20 anos** em caso de reincidência ou quando o ataque compromete a administração da justiça.

Em 2021, a **Executive Order 14028** consolidou o modelo de segurança federativa, impondo **autenticação multifatorial obrigatória (MFA), arquitetura de confiança zero (zero trust)** e a criação de um **Centro de Operações de Segurança (SOC)** sob a coordenação da **Cybersecurity and Infrastructure Security Agency (CISA)**.

O **FBI Cyber Division** atua com orçamento anual de aproximadamente **USD 10 bilhões**, com mais de **3.000 agentes especializados** e parcerias público-privadas (programa *InfraGard*). Casos emblemáticos incluem o ataque ao *Colonial Pipeline* (2021), em que o FBI recuperou parte do resgate pago em criptomoedas, e o desmantelamento do grupo REvil, especializado em *ransomware-as-a-service*.

União Europeia — *GDPR* e *NIS2* como padrão-ouro normativo

A **União Europeia** adota uma estrutura integrada de governança digital ancorada no **Regulamento Geral de Proteção de Dados**

(GDPR, Regulamento 2016/679) e na **Diretiva NIS2 (2022/2555)**.

O GDPR impõe **multas administrativas de até €20 milhões ou 4% do faturamento global anual**, o que for maior, e determina que violações de dados sejam comunicadas em até **72 horas**.

A NIS2, vigente desde janeiro de 2023, amplia a proteção à infraestrutura pública digital, incluindo tribunais eletrônicos e sistemas de justiça. Define como obrigações:

(i) operação de **SOC 24 horas**,

(ii) auditorias regulares e *penetration tests* anuais,

(iii) notificações obrigatórias em até **24 a 72 horas**,

(iv) responsabilização pessoal dos dirigentes.

As sanções podem atingir **€10 milhões** ou **2% do faturamento global**, com prazo de adequação de 18 meses após a entrada em vigor.

Singapura — *Cybersecurity Act* e responsabilização direta de dirigentes

O **Computer Misuse Act (Cap. 50A, revisado em 2020)** tipifica expressamente *ransomware* e *DDoS*, com pena de até **10 anos** de prisão e multa de **SGD 50.000** (Seção 7).

Ataques a **infraestruturas críticas**, entre as quais se incluem a "administração da justiça", podem ser punidos com **20 anos de reclusão** e multa de **SGD 100.000** (Seção 8).

O **Cybersecurity Act (2018)** criou a **Cyber Security Agency (CSA)**, responsável por designar setores críticos, exigir **notificação de incidentes graves em até 2 horas, auditorias anuais obrigatórias** e prever **multas ilimitadas**, além de **prisão de dirigentes** em caso de negligência institucional grave.

Síntese comparativa e análise interpretativa

A análise comparada demonstra que os **Estados Unidos, a União Europeia e Singapura** adotam abordagens legislativas baseadas em **tipificações específicas, penas proporcionais à gravidade do dano, protocolos obrigatórios de segurança** e **responsabilização institucional**.

O **Brasil**, em contraste, apresenta **vácuos normativos e desproporcionalidade sancionatória**, com penalidades máximas entre dois e cinco anos (Lei 12.737/2012), ausência de tipificação direta de *ransomware* e *DDoS*, e inexistência de mecanismos preventivos obrigatórios, como SOCs permanentes ou auditorias cibernéticas regulares.

Tabela 1 – Síntese legislativa comparada (dimensões essenciais)

Dimensão Jurídica	**Brasil**	**Estados Unidos**	**União Europeia**	**Singapura**
Tipificação de *ransomware*	Genérica (Lei 12.737/2012)	Específica (CFAA)	Específica (leis nacionais)	Específica (Seção 7)
Tipificação de *DDoS*	Ausente	Sim (CFAA)	Sim (NIS2)	Sim (Seção 7)

Dimensão Jurídica	**Brasil**	**Estados Unidos**	**União Europeia**	**Singapura**
Pena máxima prevista	2–5 anos	10–20 anos	10–15 anos	10–20 anos
SOC 24×7 e MFA obrigatórios	Inexistentes	Obrigatórios (EO 14028)	Obrigatórios (NIS2)	Obrigatórios (CII)
Responsabilização de dirigentes	Inexistente	Parcial	Plena (NIS2)	Plena (CSA)
Prazo de notificação de incidentes	"Razoável" (vago)	72h (HIPAA/FedRAMP)	72h (GDPR)	2–72h (gravidade)

Fonte: Elaboração própria com base em CFAA (EUA), GDPR e NIS2 (UE), Computer Misuse Act e Cybersecurity Act (Singapura).

Interpretação conclusiva

Os resultados revelam **defasagem normativa de aproximadamente 10 a 15 anos** em relação às principais potências legislativas.

Essa discrepância decorre da combinação de **penas brandas, ausência de dissuasão efetiva, lacunas tipificadoras, e inexistência de obrigações estruturais de prevenção.**

Enquanto EUA, UE e Singapura tratam a **cibersegurança judicial** como componente essencial da soberania estatal, o Brasil ainda a aborda sob perspectiva **reativa e fragmentada**, limitando-se a legislações genéricas e extemporâneas.

FRAMEWORK PROPOSITIVO: TRÊS PILARES TRANSFORMADORES VIÁVEIS

Pilar 1 — Tipificação específica Código Penal (novo Título VIII-A)

Propõe-se a criação de um **Título VIII-A** no Código Penal, denominado **"Dos Crimes Cibernéticos contra Infraestruturas Críticas e Dados"**, com foco em sanções proporcionais à gravidade e especificidade das condutas.

Art. 1º — Ransomware

Criptografar dados, sistemas ou dispositivos informáticos alheios exigindo resgate para a descriptografia.

Pena: reclusão, de 5 a 12 anos, e multa.

§1º A pena aumenta de 50% a 67% se houver destruição de backups, dupla extorsão (exfiltração e divulgação) ou dano a infraestrutura crítica (energia, saúde, Judiciário ou telecomunicações).

§2º Se do fato resultar morte, a pena será de 10 a 18 anos.

Aplicação estimada:

No caso do ataque ao STJ (2020), a pena básica (5 a 12 anos), majorada pela destruição de backups e afetação de infraestrutura crítica, resultaria entre **12 e 30 anos de reclusão**, em patamar proporcional à magnitude do dano institucional.

Art. 2º — DDoS

Negar disponibilidade de serviço informático mediante envio massivo de tráfego ou exploração abusiva de recursos computacionais.

Pena: reclusão, de 2 a 8 anos, e multa.

§1º Aumenta-se de 50% a 67% se houver uso de botnet, afetação de infraestrutura crítica ou necessidade de implementação de "modo continuidade".

§2º Se do fato resultar morte ou dano grave, a pena será de 4 a 12 anos.

Art. 3º — Exfiltração de dados

Copiar, transferir ou extrair remotamente dados sensíveis sem autorização. **Pena:** reclusão, de 4 a 10 anos, e multa, além do confisco dos dados obtidos.

Art. 4º — Certificados ICP-Brasil fraudulentos

Criar, utilizar ou facilitar o uso de certificados digitais ICP-Brasil falsificados ou fraudulentos.

Pena: reclusão, de 3 a 8 anos.

§1º Aumenta-se a pena em 50% se o crime envolver alvarás judiciais ou licitações públicas.

§2º Se houver participação de servidor público, a pena será de 8 a 15 anos, com perda do cargo e multa triplicada.

Art. 5º — Organização criminosa cibernética

Associar-se para a prática de crimes cibernéticos (RaaS, PhaaS, DDoS-for-hire).

Pena: reclusão, de 5 a 10 anos, cumulativa com as penas dos crimes-fim.

Viabilidade:

A medida poderia ser implementada por **lei ordinária**, sem necessidade de emenda constitucional. O custo fiscal seria nulo e o trâmite legislativo estimado entre **12 e 24 meses**, se pautado com prioridade.

Pilar 2 — Resolução CNJ: Política Nacional de Cibersegurança do Poder Judiciário

Propõe-se que o **Conselho Nacional de Justiça (CNJ)** edite **Resolução vinculante** instituindo uma **Política Nacional de Cibersegurança Judiciária**, aplicável aos **91 tribunais brasileiros**, conforme sua competência constitucional (art. 103-B, CF/88).

Diretrizes normativas sugeridas:

Política institucional anual: obrigatoriedade de publicação de política de segurança da informação aprovada pela Presidência e amplamente divulgada.

CISO obrigatório: tribunais com mais de 500 servidores devem nomear um Chief Information Security Officer (CISO).

SOC 24×7: operação obrigatória de Centros de Monitoramento de Segurança (próprios, terceirizados ou consorciados).

Autenticação multifator: exigência integral (VPN, PJe, e-mails, sistemas internos), com prazo de adequação de seis meses.

Testes de penetração: realização semestral por empresas certificadas, com correção obrigatória de vulnerabilidades críticas em até 30 dias.

Backups segregados: implementação de cópias air-gapped com testes trimestrais de restauração.

Capacitação permanente: 20 horas anuais para servidores e 40 horas para equipes técnicas.

Notificação de incidentes: comunicação ao CNJ em até 48 horas após ataques de ransomware, DDoS com modo continuidade ou vazamentos de dados.

Auditorias e índice de maturidade: auditorias bienais com índice público de maturidade cibernética (0–100 pontos).

Sanções administrativas: tribunais com conformidade inferior a 50% por dois ciclos consecutivos terão **suspensão de 10% das verbas de TI** até a regularização.

Viabilidade e impacto:

O custo agregado estimado seria de **R$ 200 a 500 milhões anuais**, abrangendo SOCs, MFA, pen tests e capacitação, valor marginal frente aos prejuízos já observados (mais de R$ 150 milhões em incidentes recentes).
O retorno é **qualitativo e sistêmico**, uma vez que segurança institucional não é opcional, mas requisito essencial à continuidade da justiça.

Pilar 3 — Lei Federal de Segurança de Infraestruturas Críticas Cibernéticas (LSIC)

Inspirada na **Diretiva NIS2 da União Europeia**, propõe-se a criação de uma **Lei Federal de Segurança de Infraestruturas Críticas Cibernéticas (LSIC)**, voltada à proteção intersetorial e à integração federativa.

Estrutura sugerida:

Capítulo I – Definições gerais:

Define "infraestrutura crítica" como os setores de energia, saúde, finanças, Judiciário e Juizados, telecomunicações, transporte, abastecimento de água e governo digital.

Capítulo II – Obrigações das entidades críticas:

Prevê requisitos mínimos: SOC 24×7, MFA, análise anual de riscos, pen tests anuais, planos de continuidade, capacitação obrigatória, notificação de incidentes em até 24–72 horas e backups segregados.

Capítulo III – Autoridade Nacional de Cibersegurança (ANC):

Cria ou amplia a competência da **Autoridade Nacional de Proteção de Dados (ANPD)** para atuar também como órgão regulador e fiscalizador da segurança cibernética crítica.

Capítulo IV – Comitê Nacional de Cibersegurança de Infraestrutura Crítica (CNCIC):

Órgão colegiado composto por representantes da ANC, GSI, Polícia Federal/NUCIBER, CNJ, agências reguladoras (ANEEL, ANATEL, BACEN, ANS) e setor privado.

Capítulo V – Sanções:

Multas de até **R$ 500 milhões**, responsabilização pessoal de dirigentes (inclusive com proibição de exercer cargos públicos por até cinco anos) e responsabilização civil e criminal por negligência grave.

Capítulo VI – Prazo de adequação:

24 meses, considerando a complexidade federativa brasileira e os trâmites licitatórios.

Viabilidade e retorno esperado:

Trata-se de projeto de lei ordinária, de tramitação mais extensa (18–36 meses), mas com impacto transversal. O custo de implantação (R$ 500 milhões a R$ 1 bilhão anuais) é amplamente compensado pela redução de incidentes e

prejuízos estimados em até R$ 50 bilhões anuais em setores críticos.

Indicadores de Efetividade e Monitoramento

A consolidação de uma política nacional de segurança cibernética requer mecanismos de avaliação contínua e mensuração objetiva de resultados. Propõe-se, para tanto, a criação de um Sistema Nacional de Indicadores de Segurança Institucional (SINSI), sob coordenação do CNJ e da futura ANC, com base nos seguintes parâmetros:

Indicador	**Descrição Técnica**	**Periodicidade**	**Meta de Referência (5 anos)**
Taxa de incidentes críticos	Número de ataques de alta severidade reportados ao CNJ ou ANC	Trimestral	Redução de 60%
Tempo médio de resposta (TMR)	Intervalo entre o incidente e o restabelecimento operacional	Mensal	Inferior a 12h
Índice de maturidade cibernética (IMC)	Escala 0–100, avaliando conformidade com SOC, MFA, pen tests, capacitação	Semestral	≥ 80
Taxa de conformidade CNJ	Percentual de tribunais que atingem 100% das obrigações da Resolução	Anual	100%
Custo por incidente evitado	Relação entre investimento e prejuízo estimado evitado	Anual	≤ R$ 1,00 investido / R$ 10,00 poupados

Esses indicadores permitem mensurar, de modo sistemático, a efetividade das medidas legislativas e administrativas propostas, consolidando um modelo de governança pública orientado a resultados, conforme padrões internacionais de compliance e segurança digital.

Síntese conclusiva

O tripé propositivo aqui delineado — (I) reforma penal tipificadora, (II) política nacional de segurança judiciária e (III) lei federal de proteção intersetorial — representa uma arquitetura normativa integrada, capaz de converter a atual vulnerabilidade sistêmica em resiliência institucional estruturada.

A convergência entre prevenção técnica, responsabilização penal proporcional e governança centralizada é condição indispensável para restabelecer a segurança jurídica e a credibilidade do sistema de justiça no ambiente digital.

IMPLICAÇÕES MULTIDISCIPLINARES — SÍNTESE CONSOLIDADA

Governança pública digital e responsabilidade institucional

A **cibersegurança judicial** não constitui um problema técnico restrito às áreas de tecnologia da informação, mas um **desafio de governança pública**, que demanda **liderança institucional**, **planejamento estratégico de recursos**, **transparência administrativa** e **responsabilização de dirigentes**.

À luz da **Nova Administração Pública** proposta por Hood (1991), a eficiência não deve ser mensurada apenas por custos imediatos, mas pelo **retorno social do investimento preventivo** (Return on Investment – ROI). Um tribunal com infraestrutura segura preserva a continuidade da jurisdição, reduz danos econômicos e protege direitos fundamentais.

O modelo proposto reflete os três princípios centrais da nova gestão pública:

Eficiência: o investimento preventivo gera ROI positivo, reduzindo interrupções e prejuízos materiais.

Transparência: o Índice de Maturidade Cibernética publicamente divulgado possibilita controle social e auditoria pública.

Accountability: dirigentes omissos em matéria de segurança institucional devem ser **responsabilizados administrativamente**, conforme o princípio da eficiência (art. 37, caput, CF/88).

Economia do cibercrime e análise dissuasória

Com base no modelo econômico de Becker (1968), o comportamento criminoso é racional e orientado pela relação entre o **benefício esperado (BE)** e o **custo esperado (CE)** da infração, calculado como:

CE = (pena esperada × probabilidade de captura).

No Brasil, o custo esperado médio do crime cibernético é de aproximadamente 0,175 anos, enquanto nos Estados Unidos é de 3,75 anos, ou seja, 21 vezes maior. Essa disparidade evidencia que a baixa dissuasão penal brasileira constitui incentivo estrutural à reincidência.

A dissuasão ótima não pressupõe eliminar o crime — o que é impossível —, mas reduzi-lo a um nível eficiente, no qual o custo marginal da dissuasão se iguala ao benefício marginal dos danos evitados.

O framework normativo proposto neste estudo demonstra que um investimento de R$ 1,7 bilhão em medidas estruturais geraria benefício estimado de R$ 50 bilhões anuais, resultando em um ROI de 29,4 vezes — patamar de eficiência pública raramente alcançado em políticas preventivas.

Teoria do risco e sociedade cibernética

Conforme a Teoria do Risco de Ulrich Beck (2010), as sociedades contemporâneas enfrentam riscos globais, invisíveis e irreversíveis, produzidos pelas próprias estruturas tecnológicas que sustentam o desenvolvimento.

No contexto cibernético, essa condição manifesta-se de modo paradigmático:

Invisibilidade: ataques diários de DDoS contra tribunais, como o TJPR, permanecem imperceptíveis ao público e à imprensa.

Globalização: grupos como RansomExx operam desde a Rússia e atacam infraestruturas judiciais brasileiras.

Irreversibilidade: dados criptografados sem backups segregados são permanentemente perdidos.

Produção sistêmica: a digitalização acelerada do PJe, sem blindagem adequada, criou vulnerabilidades estruturais.

Velocidade exponencial: ransomware moderno é capaz de criptografar até **1.200 máquinas virtuais por hora**, reduzindo drasticamente a janela de resposta humana.

Essa configuração impõe a adoção de um princípio da precaução invertido — isto é, agir antes da materialização do dano, e não após a catástrofe.

A governança cibernética passa, assim, da esfera da reação para a da antecipação.

Direito comparado e lições de adaptação institucional

A análise comparada evidencia que a transferência de políticas públicas em matéria cibernética é viável, mas exige adaptação contextual. As lições principais podem ser sintetizadas em três eixos:

Contextualização institucional:

O Brasil não dispõe da estrutura orçamentária do FBI (USD 10 bilhões), mas pode **dimensionar proporcionalmente** o investimento no NUCIBER (R$ 100–200 milhões) e no CNJ.

Flexibilidade normativa:

A Diretiva NIS2 exige SOCs próprios, enquanto o modelo brasileiro pode admitir **consórcios intertribunais** ou **contratações compartilhadas**, reconhecendo a limitação de escala dos tribunais menores.

Incrementalismo pragmático:

A **reforma da Lei 12.737/2012** deve ocorrer em fases, iniciando com **tipificações específicas e penalidades proporcionais**, revisadas periodicamente (a cada cinco anos) para incorporar novas ameaças, como ataques baseados em inteligência artificial.

Entretanto, três fatores limitam a plena transposição desses modelos:

Cultura jurídica: o sistema **civil law** brasileiro exige tipificação expressa, enquanto o **common law** anglo-saxão permite maior interpretação judicial.

Capacidade estatal: Singapura, com 6 milhões de habitantes e centralização administrativa, possui agilidade decisória incomparável ao federalismo brasileiro de 215 milhões.

Vontade política: enquanto os Estados Unidos aprovaram o **Patriot Act** em 45 dias após o 11 de setembro, o Brasil levou mais de **cinco**

anos após o ataque ao STJ (2020) sem qualquer reforma legislativa efetiva.

Convergência final

As análises jurídicas, econômicas e sociológicas convergem para uma conclusão inequívoca: a segurança cibernética do Judiciário brasileiro transcende o campo técnico e alcança a esfera constitucional, econômica e ética.

Sem reformas estruturais e coordenação federativa, o país permanecerá em vulnerabilidade sistêmica, sujeitando o direito de acesso à justiça à aleatoriedade de ataques digitais e à precariedade da resposta estatal.

CONSIDERAÇÕES FINAIS

Síntese dos achados: vulnerabilidade sistêmica em tripla dimensão (validada empiricamente)

A investigação — baseada em 103 fontes curadas (2020–2025), análise documental e entrevista estruturada de 48 minutos com o Chefe da Divisão de Gestão da Segurança da Informação da SETI/TJPR — demonstrou, de forma convergente, que o Poder Judiciário brasileiro vive uma crise de segurança cibernética com efeitos diretos sobre o direito fundamental de acesso à justiça (art. 5º, XXXV, CF/88). Essa crise se manifesta em três dimensões interligadas:

Ameaça institucional direta: o ataque ao STJ (2020) com criptografia de larga escala; os ataques DDoS que levaram o TJPR ao modo continuidade por quatro dias consecutivos (21–24/10/2025); e a normalização de ataques DDoS diários — dado inédito confirmado pela entrevista (Seções 1.10; 3.3).

Ameaça a dados sensíveis e continuidade jurisdicional: episódios como o comunicado da Justiça do Trabalho (out./2025), combinados à indefinição de prazos de notificação e à ausência de obrigações preventivas uniformes, revelam vulnerabilidade operacional e informacional (Seções 2.4.2; 4.2.6).

Ameaça difusa indireta via litigância de massa: o patamar de phishing e fraudes digitais alimenta um ciclo de judicialização nos Juizados Especiais, retroalimentando morosidade, congestionamento e exposição a novas disrupções (Seções 2.5.3; 2.7/2.8).

Esse conjunto probatório sustenta a tese central: inadequação legislativa + fragilidades de governança resultam em ameaça existencial ao acesso à justiça — conclusão ancorada em cronologias concretas, impactos operacionais e evidência empírica direta proveniente da entrevista.

O paradoxo dos 30 anos da Lei 9.099/1995: democratização quantitativa, inefetividade qualitativa

Os Juizados democratizaram o acesso em termos quantitativos, mas a promessa de celeridade não se consolidou qualitativamente. O acúmulo de demandas (em parte catalisado por fraudes digitais e litigância padronizada) convive com paralisações/intermitências decorrentes de incidentes cibernéticos (ransomware, DDoS e modo continuidade). O resultado é um paradoxo civilizatório: a digitalização que ampliou o acesso produziu vulnerabilidades estruturais quando não

acompanhada de governança robusta (SOC 24×7, MFA universal, pen tests regulares, backups segregados, resposta coordenada).

A entrevista com o TJPR — peça empírica-chave deste estudo — expõe com nitidez a dimensão "oculta" do problema: ataques diários existem, mesmo quando não noticiados; e o modo continuidade não é uma contingência excepcional, mas resposta operacional padronizada sempre que os ataques extrapolam a capacidade de mitigação. Em termos constitucionais, trata-se de negação material de acesso para usuários externos (advocacia, partes, magistrados/servidores remotos), com efeitos concretos sobre duração razoável do processo e eficiência administrativa (art. 5º, LXXVIII, e art. 37, caput).

Causas-raiz: descompasso normativo e governança reativa

A Seção 4 identificou cinco lacunas críticas na Lei 12.737/2012 (ausência de tipos específicos para ransomware e DDoS, penas desproporcionais, vagueza terminológica, foco individual em detrimento de organizações transnacionais). A Seção 5 evidenciou defasagem internacional (EUA/UE/Singapura) em tipificação, penas, obrigações preventivas, notificação e responsabilização de dirigentes. Em paralelo, a governança ainda é predominantemente reativa: avanços relevantes (como no TJPR após o incidente dos alvarás) vêm depois do dano, não antes.

No plano econômico (Seção 2.6.1), o custo esperado do crime cibernético no Brasil permanece irrisório frente ao benefício esperado de ataques com potencial de resgate/impacto sistêmico — um convite à seleção adversa que torna o país alvo preferencial.

Da crítica à solução: viabilidade e urgência do framework propositivo

O framework de três pilares (Seção 6) oferece viabilidade jurídica, técnica e econômica:

Pilar 1 (CP): tipificações específicas e escalonadas para ransomware, DDoS, exfiltração e certificados ICP-Brasil fraudulentos, com majorações proporcionais a dano, uso de botnet e impacto em infraestrutura crítica (incluindo o Judiciário).

Pilar 2 (CNJ): política nacional vinculante: SOC 24×7, MFA 100%, pen tests semestrais, backups air-gapped, capacitação, notificação em 48h e auditorias com índice de maturidade e sanções orçamentárias por descumprimento.

Pilar 3 (LSIC): lei federal à la NIS2, definindo setores críticos (com Judiciário), obrigações preventivas, autoridade nacional e sanções significativas, inclusive responsabilização pessoal de dirigentes em casos de negligência grave.

O balanço custo-benefício consolidado indica que a prevenção "se paga" com folga, internalizando externalidades e protegendo um direito fundamental.

A falta de ação não é neutra: encarece o sistema (morosidade, retrabalhos, incidentes), corroi confiança e normaliza o inaceitável (negação material de acesso por modo continuidade).

Há o que comemorar? Uma provocação necessária

À luz do que foi exposto, a comemoração do trigésimo aniversário da Lei 9.099/1995 sem qualificações seria, no mínimo, imprudente. Sim, os Juizados ampliaram a porta de entrada e democratizaram a litigância de menor complexidade. Mas:

A promessa de celeridade não foi entregue de forma sistemática;

A litigância de massa (inclusive a derivada de fraudes digitais) pressiona o sistema para além da capacidade de resposta;

A defasagem legislativa e a ausência de políticas preventivas obrigatórias expõem o núcleo constitucional do acesso a interrupções e bloqueios tecnológicos previsíveis;

A entrevista com o TJPR, ao tornar visível o invisível (ataques diários e modo continuidade como resposta padrão quando a capacidade de defesa é superada), desloca o debate do plano abstrato para o registro fático: o sistema já opera em regime de exceção técnica recorrente.

Se a pergunta é "há o que comemorar?", a resposta responsável é: há o que reconhecer, e muito o que corrigir. O rito de passagem dos 30 anos dos Juizados não deve ser uma exortação auto celebratória, mas um chamado à ação para reconstituir a efetividade da promessa constitucional de 1988 no ciberespaço.

A metáfora que se impõe é a de uma corrida contra o tempo: enquanto disputamos prazos e metas, adversários invisíveis — com baixo custo esperado e alto retorno — testam diariamente as defesas. O Judiciário segue julgando, mas entre sobressaltos; trabalha por dentro, enquanto o lado de fora fica à margem durante o modo continuidade. Isso não é normal. Isso não pode se normalizar.

A opção política — e civilizatória — está dada: ou incorporamos já (2026) o padrão mínimo de resiliência cibernética e reparamos a lacuna penal que hoje recompensa o agressor, ou aceitaremos, por inércia, a erosão progressiva de um dos pilares da ordem democrática: o acesso efetivo, contínuo e célere à jurisdição.

Este artigo buscou mapear o problema, demonstrar empiricamente sua materialidade, explicitar os custos e propor um caminho. A entrevista com o gestor sênior do TJPR não é um apêndice; é o timbre empírico que encerra a dúvida: a ameaça é diária, recorrente e já condiciona a operacionalidade da Justiça.

Comemorar, só se significar assumir publicamente essa realidade e mudar — tipificar o que falta, obrigar o que é básico, auditar o que importa e responsabilizar quem negligência. Do contrário, a festa será para o inimigo.

REFERÊNCIAS BIBLIOGRÁFICAS

AGÊNCIA BRASIL. STJ é alvo de ataque de hacker e Polícia Federal investiga o sistema. Agência Brasil, Brasília, 3 nov. 2020. Disponível em: https://agenciabrasil.ebc.com.br/justica/noticia/2020-11/stj-e-alvo-de-ataque-de-hacker-e-policia-federal-investiga-o-sistema. Acesso em: 26 out. 2025.

ANTUNES, Maria José. Crimes cibernéticos e os desafios jurídicos na era digital. Revista JRG de Estudos Acadêmicos, v. 7, n. 14, p. 1662-1684, 2024. DOI: 10.55892/jrg.v7i14.1162.

ASPER. Largest Botnet Discovered in 2024. Asper Blog, 2025. Disponível em: https://asper.ai/blog/largest-botnet-discovered-in-2024/. Acesso em: 26 out. 2025.

BAGUETE. Ataque ransomware ao STJ: como foi feito e quais as consequências. Baguete, Porto Alegre, 10 nov. 2020. Disponível em:

https://www.baguete.com.br/noticias/10/11/2020/ataque-ransomware-ao-stj-como-foi-feito-e-quais-as-consequencias. Acesso em: 26 out. 2025.

BARDIN, Laurence. Análise de Conteúdo. Tradução de Luís Antero Reto e Augusto Pinheiro. São Paulo: Edições 70, 2011. 279 p.

BECK, Ulrich. Sociedade de risco: rumo a uma outra modernidade. Tradução de Sebastião Nascimento. São Paulo: Editora 34, 2010. 384 p.

BECKER, Gary S. Crime and Punishment: An Economic Approach. Journal of Political Economy, v. 76, n. 2, p. 169-217, 1968. DOI: 10.1086/259394.

BERTOLLI, Emilio; MARTINELLI, Fabio; RIGHI, Riccardo. Ransomware: An Interdisciplinary Technical and Legal Approach. Security and Communication Networks, Hindawi, 2020. DOI: 10.1155/2020/8353680.

BLEEPINGCOMPUTER. Brazil's court system under massive RansomExx ransomware attack. BleepingComputer, 4 nov. 2020. Disponível em: https://www.bleepingcomputer.com/news/security/brazils-court-system-under-massive-ransomexx-ransomware-attack/. Acesso em: 26 out. 2025.

BRASIL. Constituição da República Federativa do Brasil de 1988. Brasília, DF: Senado Federal, 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 26 out. 2025.

BRASIL. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. Código Penal. Diário Oficial da União, Rio de Janeiro, 31 dez. 1940. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 26 out. 2025.

BRASIL. Lei nº 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. Diário Oficial da União, Brasília, DF, 12 set. 1990. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 26 out. 2025.

BRASIL. Lei nº 8.906, de 4 de julho de 1994. Dispõe sobre o Estatuto da Advocacia e a Ordem dos Advogados do Brasil (OAB). Diário Oficial da União, Brasília, DF, 5 jul. 1994. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8906.htm. Acesso em: 26 out. 2025.

BRASIL. Lei nº 9.099, de 26 de setembro de 1995. Dispõe sobre os Juizados Especiais Cíveis e Criminais e dá outras providências. Diário Oficial da União, Brasília, DF, 27 set. 1995. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9099.htm. Acesso em: 26 out. 2025.

BRASIL. Lei nº 12.737, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Diário Oficial da União, Brasília, DF, 3 dez. 2012. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 26 out. 2025.

BRASIL. Lei nº 12.850, de 2 de agosto de 2013. Define organização criminosa e dispõe sobre a investigação criminal, os meios de obtenção da prova, infrações penais correlatas e o procedimento criminal. Diário Oficial da União, Brasília, DF, 3 ago. 2013. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12850.htm. Acesso em: 26 out. 2025.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União, Brasília, DF, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 26 out. 2025.

CAFÉ COM SOCIOLOGIA. Pierre Lévy: conceitos-chave no estudo da cibercultura. Café com Sociologia, 20 jun. 2020. Disponível em: https://cafecomsociologia.com/pierre-levy-conceitos-chave-cibercultura/. Acesso em: 26 out. 2025.

CLOUDFLARE. DDoS Threat Report for 2025 Q1. Cloudflare Blog, 2025. Disponível em: https://blog.cloudflare.com/ddos-threat-report-2025-q1/. Acesso em: 26 out. 2025.

CANALTECH. Preocupante: ataques DDoS explodem 358% em 2025 e quebram recordes de volume. São Paulo, 2025. Disponível em: https://canaltech.com.br/seguranca/preocupante-ataques-ddos-explodem-358-em-2025-e-quebram-recordes-de-volume/. Acesso em: 9 nov. 2025.

CAPPELLETTI, Mauro; GARTH, Bryant. Acesso à Justiça. Tradução de Ellen Gracie Northfleet. Porto Alegre: Sergio Antonio Fabris Editor, 1988. 168 p.

CASTELLIANO, Caio; GUIMARAES, Tomas Aquino. Fatores que aumentam o tempo do processo judicial no Brasil. Revista de Administração

Pública, Rio de Janeiro, v. 58, n. 3, p. 1-20, 2024. DOI: 10.1590/0034-761220230145.

CHAINALYSIS. The 2024 Crypto Crime Report. Chainalysis Blog, 2024. Disponível em: https://www.chainalysis.com/blog/2024-crypto-crime-report/. Acesso em: 26 out. 2025.

CNN BRASIL. Operação mira grupo que emitia falsos alvarás judiciais pelo país. CNN Brasil, São Paulo, 6 ago. 2024. Disponível em: https://www.cnnbrasil.com.br/nacional/operacao-mira-grupo-que-emitia-falsos-alvaras-judiciais-pelo-pais/. Acesso em: 26 out. 2025.

CONSELHO NACIONAL DE JUSTIÇA. Justiça em Números 2024: ano-base 2023. Brasília: CNJ, 2024. Disponível em: https://www.cnj.jus.br/pesquisas-judiciarias/justica-em-numeros/. Acesso em: 26 out. 2025.

CONSELHO NACIONAL DE JUSTIÇA. Resolução nº 354, de 3 de novembro de 2020. Suspende prazos processuais no STJ em razão de ataque cibernético. Diário da Justiça Eletrônico, Brasília, 4 nov. 2020.

CONSELHO SUPERIOR DA JUSTIÇA DO TRABALHO. Comunicado sobre incidente de segurança no PJe. CSJT, Brasília, outubro 2025. Disponível em: https://www.csjt.jus.br/. Acesso em: 26 out. 2025.

CONVERGÊNCIA DIGITAL. Justiça do Trabalho aciona PF e ANPD por acesso massivo e não autorizado em 21 tribunais. Convergência Digital, 6 out. 2025. Disponível em: https://convergenciadigital.com.br/seguranca/justica-do-trabalho-aciona-pf-e-anpd-por-acesso-massivo-e-nao-autorizado-em-21-tribunais/. Acesso em: 26 out. 2025.

CLOUDFLARE. DDoS Threat Report: Q1 2025. San Francisco: Cloudflare, 2025. Disponível em: https://blog.cloudflare.com/ddos-threat-report-2025-q1. Acesso em: 9 nov. 2025.

CYBERBRICS. Comparative Analysis of Cybersecurity Legislation in BRICS Countries. CyberBRICS Report, out. 2020. Disponível em: https://cyberbrics.info/wp-content/uploads/2020/10/CyberBRICS-Report-Oct2020.pdf. Acesso em: 26 out. 2025.

CYBERNEWS. Largest Botnet Ever Discovered in 2024. Cybernews, 2025. Disponível em: https://cybernews.com/security/largest-botnet-2024/. Acesso em: 26 out. 2025.

DATASENADO. Golpes digitais vitimaram 24% dos brasileiros em 2024. DataSenado, Brasília, 1 out. 2024. Disponível em: https://www12.senado.leg.br/noticias/. Acesso em: 26 out. 2025.

EUROPEAN DATA PROTECTION BOARD. Meta fined €1.2 billion for GDPR violations. EDPB, Bruxelas, 2023. Disponível em: https://edpb.europa.eu/. Acesso em: 26 out. 2025.

EXAME. Custos do Judiciário chegam a 1,4% do PIB brasileiro. Exame, São Paulo, 7 jul. 2025. Disponível em: https://exame.com/brasil/custos-do-judiciario-chegam-a-14-do-pib-brasileiro/. Acesso em: 26 out. 2025.

FEDERAL BUREAU OF INVESTIGATION. FBI Cyber Division 2021 Annual Report. FBI, Washington DC, 2021. Disponível em: https://www.fbi.gov/investigate/cyber. Acesso em: 26 out. 2025.

FENATI. Phishing lidera golpes virtuais no Brasil; saiba como evitar. FENATI Notícias, 11 set. 2025. Disponível em: https://fenati.org.br/phishing-lidera-golpes-virtuais-no-brasil-saiba-como-evitar/. Acesso em: 26 out. 2025.

FLICK, Uwe. Introdução à Pesquisa Qualitativa. 3. ed. Tradução de Joice Elias Costa. Porto Alegre: Artmed, 2009. 405 p.

FOLHA DE SÃO PAULO. Pandemia fez aumentar 70% fraudes eletrônicas, gerando perdas de R$ 1 bilhão. Folha de São Paulo, São Paulo, 26 ago. 2020. Disponível em: https://www1.folha.uol.com.br/. Acesso em: 26 out. 2025.

FUNDAÇÃO GETULIO VARGAS. Relatório ICJBrasil. FGV Direito SP, São Paulo, 2017. Disponível em: https://direitosp.fgv.br/. Acesso em: 26 out. 2025.

G1 PARANÁ. Quadrilha é suspeita de causar prejuízo milionário ao Tribunal de Justiça do Paraná. G1 Paraná, Curitiba, 6 ago. 2024. Disponível em: https://g1.globo.com/pr/parana/noticia/2024/08/06/operacao-da-policia-civil-investiga-falsificacao-de-documentos-publicos-tjpr.ghtml. Acesso em: 26 out. 2025.

GARRETT, Sarah; RASHID, Awais; BARON, Alistair. A Survey on Ransomware: Evolution, Taxonomy, and Defense Solutions. ArXiv preprint arXiv:2102.06249, 2021. Disponível em: https://arxiv.org/abs/2102.06249. Acesso em: 26 out. 2025.

GRUSTNIY, Dmytro et al. The True Cost of a Ransomware Attack. DarkReading, 2021. Disponível em:

https://www.darkreading.com/cyberattacks-data-breaches/the-true-cost-of-a-ransomware-attack. Acesso em: 26 out. 2025.

HOOD, Christopher. A Public Management for All Seasons? Public Administration, v. 69, n. 1, p. 3-19, 1991. DOI: 10.1111/j.1467-9299.1991.tb00779.x.

INCIBE SPAIN. Ransomexx: el ransomware que atacó al STJ brasileño. INCIBE-CERT, Espanha, nov. 2020. Disponível em: https://www.incibe-cert.es/blog/ransomexx-ransomware-que-ataco-stj-brasileno. Acesso em: 26 out. 2025.

INFOMONEY. 1,3 bilhão de ataques em 2025: IA turbina phishing, velho conhecido da América Latina. InfoMoney, São Paulo, 8 set. 2025. Disponível em: https://www.infomoney.com.br/business/13-bilhao-de-ataques-em-2025-ia-turbina-phishing-velho-conhecido-da-america-latina/. Acesso em: 26 out. 2025.

INSTITUTO DE LONGEVIDADE. Phishing é o golpe virtual mais comum no Brasil em 2025. Instituto de Longevidade, 2 out. 2025. Disponível em: https://institutodelongevidade.org/longevidade-e-comportamento/tecnologia/phishing-golpe-virtual. Acesso em: 26 out. 2025.

IT SHOW. TJ-PR sofre instabilidade após pico de acessos. IT Show, 2025. Disponível em: https://itshow.com.br/tj-pr-sofre-instabilidade-apos-pico-de-acessos/. Acesso em: 26 out. 2025.

JONKER, Mattijs et al. The Age of DDoScovery: An Empirical Comparison of Industry and Academic DDoS Assessments. ArXiv preprint arXiv:2410.11708, 2024. Disponível em: https://arxiv.org/abs/2410.11708. Acesso em: 26 out. 2025.

KASPERSKY. Panorama de Ameaças Cibernéticas 2025. Kaspersky Brasil, 2025. Relatório apresentado na 15ª Cyber Security Week, Manaus, set. 2025. Disponível em: https://www.kaspersky.com.br/. Acesso em: 26 out. 2025.

KLUSAIT, Renata et al. DDoS Attacks: Evolution, Detection, Prevention, Reaction, and Tolerance. Future Generation Computer Systems, v. 107, p. 394-407, 2020. DOI: 10.1016/j.future.2019.12.041.

LEONARDI, Marcel. Fundamentos de Direito Digital. 2. ed. São Paulo: Thomson Reuters Brasil, 2020. 464 p.

LÉVY, Pierre. Cibercultura. Tradução de Carlos Irineu da Costa. São Paulo: Editora 34, 1999. 264 p.

LÉVY, Pierre. O que é o virtual? Tradução de Paulo Neves. São Paulo: Editora 34, 1996. 160 p.

LÉVY, Pierre. A Inteligência Coletiva: por uma antropologia do ciberespaço. Tradução de Luiz Paulo Rouanet. São Paulo: Edições Loyola, 1994. 212 p.

LÉVY, Pierre. Ciberdemocracia. Tradução de Alexandre Emílio. Lisboa: Instituto Piaget, 2001. 248 p.

LEWIS BRISBOIS. DOJ's Strategic Approach to Countering Cybercrime and AI Misuse. Lewis Brisbois News, 2025. Disponível em: https://lewisbrisbois.com/newsroom/legal-alerts/dojs-strategic-approach-to-countering-cybercrime-and-ai-misuse. Acesso em: 26 out. 2025.

LUBIN, Tomer; SCHMITT, Susanna; VAGLE, Jeffrey. Ransomware: Toward a General Theory of Computer-Aided Human Extortion. Vanderbilt Journal of Entertainment & Technology Law, v. 26, n. 4, 2024. Disponível em: https://scholarship.law.vanderbilt.edu/jetlaw/. Acesso em: 26 out. 2025.

MIGALHAS. Dados do CNJ: Justiça em Números 2024. Migalhas, 2025. Disponível em: https://www.migalhas.com.br/arquivos/2025/1/71ADE74D86F906_justica-em-numeros-2024-v-28-0.pdf. Acesso em: 26 out. 2025.

NETSCOUT. DDoS Threat Intelligence Report 2025.1. Netscout, 2025. Disponível em: https://www.netscout.com/threatreport/. Acesso em: 26 out. 2025.

OSBORNE, David; GAEBLER, Ted. Reinventing Government: How the Entrepreneurial Spirit is Transforming the Public Sector. Reading, MA: Addison-Wesley, 1992. 405 p.

PEREIRA, Cicero Antonio; LELIS, Henrique Rodrigues. O papel do CNJ no combate à litigância predatória. Revista Ibero-Americana de Humanidades, Ciências e Educação, São Paulo, v. 11, n. 10, p. 2247-2252, out. 2025. DOI: 10.51891/rease.v11i10.21507.

PEREIRA, Vinicius Rosoha. Insuficiência da Legislação Brasileira no Combate ao Ransomware: Desafios e Riscos no Ambiente Digital. Amazon, 2022.

PINHEIRO, Armando Castelar. Judiciário, Reforma e Economia: A Visão dos Magistrados. Revista Brasileira de Economia, v. 63, n. 2, p. 143-158, 2009. DOI: 10.1590/S0034-71402009000200003.

PINHEIRO, Armando Castelar. A Justiça e o Custo Brasil. Revista USP, São Paulo, n. 101, p. 141-158, mar./abr./maio 2014. DOI: 10.11606/issn.2316-9036.v0i101p141-158.

PINHEIRO, Patricia Peck. Direito Digital. 7. ed. São Paulo: Saraiva Educação, 2023. 680 p.

PLURIVERSO. O que é cibercultura, para Pierre Lévy. Revista Pluriverso, 2024. Disponível em: https://pluriverso.online/revista/o-que-e-cibercultura-para-pierre-levy/. Acesso em: 26 out. 2025.

POSNER, Richard A. An Economic Theory of the Criminal Law. Columbia Law Review, v. 85, n. 6, p. 1193-1231, 1985. DOI: 10.2307/1122392.

QRATOR LABS. DDoS Attacks in 2025 Q1: Global Trends. Qrator Labs Report, 2025. Disponível em: https://qrator.net/reports/ddos-attacks-2025-q1/. Acesso em: 26 out. 2025.

RICHARDSON, Ronny; NORTH, Max M.; RATURI, Arkodyuti. The Real-World Costs of Ransomware Attacks. Computer, v. 56, n. 7, p. 60-68, jul. 2023. DOI: 10.1109/MC.2023.3256918.

SANTANA, Ana Paula; MATTOS, Luciano; CARMO, Valter. A necessidade de segurança dos dados sensíveis no Sistema Processual Penal. Revista Científica do Programa de Justiça e Memória, Rio de Janeiro, v. 4, n. 7, 2025.

SECURITY AFFAIRS. Brazil's Superior Court of Justice (STJ) hit by RansomExx ransomware. Security Affairs, 4 nov. 2020. Disponível em: https://securityaffairs.com/110429/cyber-crime/brazils-stj-ransomexx-ransomware.html. Acesso em: 26 out. 2025.

SECURITY LEADERS. TRF-3 confirma ataque DDoS. Security Leaders Brasil, 7 mar. 2025. Disponível em: https://securityleaders.com.br/trf3-sp-confirma-ataque-ddos/. Acesso em: 26 out. 2025.

SENNA, Mariana; FERRARI, Isabela. The international legal framework on cybercrime. DNB Working Paper, 2020. Disponível em: https://dnb.nl/media/kenpsmfa/paper-2-the-international-legal-framework-on-cybercrime-senna-ferrari.pdf. Acesso em: 26 out. 2025.

SERASA. Pesquisa Serasa: 54,2% dos brasileiros foram vítimas de fraudes em 2024. Serasa Experian, São Paulo, 2024. Disponível em: https://www.serasa.com.br/. Acesso em: 26 out. 2025.

SILVA, Rodolfo et al. Ransomware Taxonomy and Countermeasures: A Comprehensive Survey. MDPI Applied Sciences, v. 14, n. 2, p. 1-28, 2024. DOI: 10.3390/app14020789.

SILVA, Vanessa Cristina. Crise nos Juizados Especiais Após 30 Anos da Lei 9.099/95. Dissertação (Mestrado em Direito) — Universidade de Araraquara, Araraquara, 2020. Disponível em: https://m.uniara.com.br/arquivos/producao/prod-9b5474e725b0f83708e4b6dfa55b2512.pdf. Acesso em: 26 out. 2025.

SOCIEDADE BRASILEIRA DE COMPUTAÇÃO. Phishing no Brasil: estatísticas e impactos econômicos. SBC, Brasília, 2024. Disponível em: https://www.sbc.org.br/. Acesso em: 26 out. 2025.

SOUSA, Ulisses César Martins de. Artigo: Juizados Especiais, um pesadelo da Justiça. OAB, 31 jan. 2014. Disponível em: http://www.oab.org.br/noticia/23814/artigo-juizados-especiais-um-pesadelo-da-justica. Acesso em: 26 out. 2025.

SUPERIOR TRIBUNAL DE JUSTIÇA. Comunicado da Presidência do STJ sobre ataque cibernético. STJ Notícias, 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: 26 out. 2025.

SUPERIOR TRIBUNAL DE JUSTIÇA. Os precedentes do STJ nos primeiros quatro anos de vigência da Lei Geral de Proteção de Dados Pessoais. STJ Notícias, Brasília, 27 out. 2024. Disponível em: https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/2024/27102024-Os-precedentes-do-STJ-nos-primeiros-quatro-anos-de-vigencia-da-Lei-Geral-de-Protecao-de-Dados-Pessoais.aspx. Acesso em: 26 out. 2025.

TESOURO NACIONAL. Estatísticas Fiscais do Setor Público: Despesas do Judiciário. Brasília: Ministério da Fazenda, 2025. Disponível em: https://sisweb.tesouro.gov.br/. Acesso em: 26 out. 2025.

TRIBUNAL DE JUSTIÇA DE MINAS GERAIS. Estudo sobre litigância predatória em Minas Gerais. TJMG, Belo Horizonte, 2022. Disponível em: https://www.tjmg.jus.br/. Acesso em: 26 out. 2025.

TRIBUNAL DE JUSTIÇA DE SÃO PAULO. Análise de litigância em massa: comarca de São Paulo. TJSP, São Paulo, 2024. Disponível em: https://www.tjsp.jus.br/. Acesso em: 26 out. 2025.

TRIBUNAL REGIONAL FEDERAL DA 3ª REGIÃO. Comunicado sobre instabilidade nos sistemas.

TRF-3, São Paulo, 7 mar. 2025. Disponível em: https://www.trf3.jus.br/. Acesso em: 26 out. 2025.

UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais (GDPR). Jornal Oficial da União Europeia, Bruxelas, 4 maio 2016. Disponível em: https://eur-lex.europa.eu/eli/reg/2016/679/oj. Acesso em: 26 out. 2025.

UNIÃO EUROPEIA. Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho, de 14 de dezembro de 2022, relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança em toda a União (NIS2). Jornal Oficial da União Europeia, Bruxelas, 27 dez. 2022. Disponível em: https://eur-lex.europa.eu/eli/dir/2022/2555/oj. Acesso em: 26 out. 2025.

UNITED STATES. Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (1986, amended). Cornell Law School, Ithaca, 2025. Disponível em: https://www.law.cornell.edu/uscode/text/18/1030. Acesso em: 26 out. 2025.

WATANABE, Kazuo. Acesso à Justiça e Sociedade Moderna. In: GRINOVER, Ada Pellegrini et al. Participação e Processo. São Paulo: Revista dos Tribunais, 2019. p. 128-135.

FONTE PRIMÁRIA — ENTREVISTA ESTRUTURADA

BUENO, Lauro Andrey de Souza. Entrevista estruturada: cibersegurança no Poder Judiciário — estudo de caso TJPR. Entrevistado: Lauro Andrey de Souza Bueno, Chefe da Divisão de Gestão da Segurança da Informação da Secretaria de Tecnologia da Informação (SETI/TJPR). Entrevistador: Vinícius Rosoha Pereira. São Mateus do Sul-PR, 24 de out. 2025. Realizada remotamente via Microsoft Teams. Duração: 48 minutos. Transcrição integral autorizada mediante Termo de Consentimento Livre e Esclarecido (TCLE) assinado pelo entrevistado em [DATA TCLE: 24/10/2025]. Arquivo de áudio digital e transcrição (134.676 caracteres) arquivados pelo pesquisador. Dados utilizados: (i) cronologia Incidente dos Alvarás 2024; (ii) ataques DDoS setembro e outubro/2025; (iii) conceito técnico "modo continuidade" (funcionamento, aplicação 21-24/out/2025); (iv) revelação de informação não divulgada publicamente: ataques DDoS diários ao TJPR ("Sofremos diariamente com estes incidentes, mas nem todos geram problemas que podem afetar a todos"); (v) medidas de segurança pós-incidentes (MFA obrigatória, SOC em contratação, equipe ~30 profissionais 24x7, pen tests regulares); (vi) desafios de rastreio e responsabilização ("É bem difícil encontrar os responsáveis pelos ataques. [...] A maior parte destes ataques não é passível de identificação por se originarem em redes zumbi").