III CONGRESSO INTERNACIONAL DE DIREITO, POLÍTICAS PÚBLICAS, TECNOLOGIA E INTERNET

DIREITO, POLÍTICAS PÚBLICAS, TECNOLOGIA E INTERNET II (ON-LINE) II

D598
Direito, políticas públicas, tecnologia e internet II – online II [Recurso eletrônico on-line] organização III Congresso Internacional de Direito, Políticas Públicas, Tecnologia e Internet: Faculdade de Direito de Franca – Franca;

Coordenadores: Viviane Coêlho de Séllos Knoerr e José Luiz Faleiros – Franca: Faculdade de Direito de Franca, 2025.

Inclui bibliografia
ISBN: 978-65-5274-365-7
Modo de acesso: www.conpedi.org.br em publicações
Tema: Governança, regulação e o futuro da inteligência artificial.
1. Direito. 2. Políticas Públicas. 3. Tecnologia. 4. Internet. I. III Congresso Internacional de Direito, Políticas Públicas, Tecnologia e Internet (1:2025 : Franca, SP).

CDU: 34

III CONGRESSO INTERNACIONAL DE DIREITO, POLÍTICAS PÚBLICAS, TECNOLOGIA E INTERNET

DIREITO, POLÍTICAS PÚBLICAS, TECNOLOGIA E INTERNET II (ON-LINE) II

Apresentação

Franca recebeu o III Congresso Internacional de Direito, Políticas Públicas, Tecnologia e Internet. O evento reuniu acadêmicos, profissionais, pesquisadores e estudantes, promovendo o debate interdisciplinar sobre o impacto das inovações tecnológicas no campo jurídico e nas políticas públicas. A programação envolveu Grupos de Trabalho (GTs) organizados para aprofundar temas específicos, abordando desde o acesso à justiça até as complexidades da regulação tecnológica, com ênfase na adaptação do sistema jurídico aos avanços da inteligência artificial e da automação.

O GT 11 analisa as interfaces entre o direito, a tecnologia e as políticas públicas em uma perspectiva de governança democrática. As pesquisas tratam da transformação digital do Estado, da participação cidadã e das estratégias de inclusão social mediadas por tecnologia. O grupo propõe uma reflexão sobre os caminhos do direito na consolidação de uma sociedade digital justa, transparente e participativa.

CIBERATAQUES A ÓRGÃOS PÚBLICOS: VULNERABILIDADES INSTITUCIONAIS E DESAFIOS JURÍDICOS NA GOVERNANÇA DA SEGURANÇA DIGITAL ESTATAL

CYBERATTACKS ON PUBLIC AGENCIES: INSTITUTIONAL VULNERABILITIES AND LEGAL CHALLENGES IN THE GOVERNANCE OF STATE DIGITAL SECURITY

Valter Moura do Carmo
Francisco Céu Pereira de Oliveira Dantas
Caio Rodrigo Maciel de Freitas Ribeiro

Resumo

Este estudo analisa os principais ciberataques contra órgãos públicos brasileiros entre 2020 e 2024, com destaque para os casos do STJ, Ministério da Saúde e sistemas fiscais municipais. A pesquisa investiga causas, impactos e desafios jurídicos relacionados à segurança digital estatal, evidenciando a fragilidade das infraestruturas públicas diante de ameaças cibernéticas. Com base em dados empíricos e análise normativa, conclui-se que a proteção digital do Estado deve ser tratada como prioridade estratégica, exigindo coordenação institucional e marcos regulatórios mais robustos.

Palavras-chave: Cibersegurança, Órgãos públicos, Ciberataques, Responsabilidade estatal

Abstract/Resumen/Résumé

This study analyzes major cyberattacks on Brazilian public agencies between 2020 and 2024, focusing on cases involving the STJ, the Ministry of Health, and municipal tax systems. It investigates the causes, impacts, and legal challenges related to digital security, highlighting the fragility of public infrastructures in the face of cyber threats. Based on empirical data and regulatory analysis, the research concludes that protecting state digital systems must be a strategic priority, requiring institutional coordination and stronger regulatory frameworks.

Keywords/Palabras-claves/Mots-clés: Cybersecurity, Public agencies, Cyberattacks, State responsibility

1 Introdução

A intensificação do uso de tecnologias digitais no setor público brasileiro trouxe avanços importantes na gestão e na oferta de serviços, mas também ampliou substancialmente os riscos associados à segurança da informação. Nos últimos anos, diferentes órgãos estatais enfrentaram incidentes cibernéticos que expuseram falhas estruturais e comprometeram a prestação de serviços essenciais, revelando a fragilidade da proteção digital do Estado. Casos como os incidentes ao Superior Tribunal de Justiça e ao Ministério da Saúde evidenciam a gravidade do problema e demandam respostas urgentes. Este estudo busca compreender as causas, impactos e implicações jurídicas desses episódios, com foco nos anos de 2020 a 2024, propondo medidas para fortalecer a resiliência institucional frente às ameaças digitais que desafiam a soberania e os direitos fundamentais no contexto contemporâneo.

O referente estudo propõe-se a examinar os principais incidentes cibernéticos ocorridos entre 2020 e 2024 em órgãos públicos brasileiros, com atenção especial às consequências jurídicas, técnicas e institucionais. A pesquisa busca compreender as fragilidades que permitiram tais ocorrências, além de discutir alternativas normativas e políticas voltadas à proteção das estruturas estatais no ambiente digital.

Em um cenário global marcado pela complexidade tecnológica e pela intensificação das ameaças digitais, a proteção das infraestruturas públicas ultrapassa a esfera técnica e adquire relevância estratégica. Investigar os limites da atuação estatal diante dessas ameaças é essencial para fortalecer a soberania digital e assegurar a continuidade dos serviços públicos em tempos de instabilidade.

2 Objetivos e metodologia

O objetivo central desta pesquisa é analisar criticamente os ciberincidentes mais relevantes ocorridos em órgãos públicos brasileiros entre os anos de 2020 e 2024, com ênfase nas implicações jurídicas, tecnológicas e institucionais decorrentes desses incidentes. Diante da intensificação das ameaças cibernéticas direcionadas ao setor público, esta investigação busca compreender como a estrutura estatal tem respondido — ou falhado em responder — a essas ocorrências, e quais medidas normativas e políticas

são necessárias para reforçar a resiliência institucional frente ao cenário de progressiva complexidade digital.

Como objetivos específicos, propõe-se descrever e contextualizar os principais incidentes cibernéticos sofridos por órgãos estatais no período estudado, com destaque para o STJ (2020), o Ministério da Saúde (2021-2022) e sistemas fiscais municipais (2022-2024), identificar fragilidades técnicas, estruturais e jurídicas na prevenção e resposta a esses incidentes, avaliar a atuação dos órgãos de controle, como o Tribunal de Contas da União e o Gabinete de Segurança Institucional, na governança da segurança cibernética e propor diretrizes de atuação baseadas em marcos internacionais, como a Convenção de Budapeste e a Estratégia de Cibersegurança da União Europeia.

A metodologia aplicada é de natureza qualitativa e de caráter exploratório-descritivo. A escolha por uma abordagem qualitativa justifica-se pela complexidade do fenômeno estudado, que envolve variáveis interdisciplinares como Direito, ciência da computação, políticas públicas e relações internacionais. A pesquisa documental baseou-se na análise de fontes primárias e secundárias, incluindo relatórios do Centro de Tratamento e Resposta a Incidentes Cibernéticos da Administração Pública Federal (CTIR-Gov), estudos da Controladoria-Geral da União (CGU), pareceres técnicos do Tribunal de Contas da União (TCU) e dados do Boletim de Conjuntura da Autoridade Nacional de Proteção de Dados (ANPD). Complementarmente, foram consultadas matérias jornalísticas verificadas (UOL, G1, Agência Brasil), artigos científicos indexados em periódicos da área jurídica e tecnológica, além de conteúdos técnicos publicados por especialistas em cibersegurança, como Gustavo Palazolo e Solange Ghernaouti. A utilização de dados empíricos extraídos de bancos oficiais foi fundamental para estabelecer o escopo e a incidência dos incidentes, enquanto os documentos normativos — como o Marco Civil da Internet (Lei nº 12.965/2014), a LGPD (Lei nº 13.709/2018) e o PL nº 2.310/2021 — foram utilizados para análise jurídica do problema.

Adotou-se ainda um recorte temporal que inicia em 2020 — ano do ataque ao STJ — e se estende até 2024, período marcado por um aumento expressivo de notificações de incidentes cibernéticos em instituições públicas, conforme demonstrado em relatórios do CTIR-Gov (2024). A análise foi orientada pelo princípio da interdisciplinaridade, visando dialogar com diferentes campos do conhecimento e construir uma abordagem integradora

que reflita a complexidade dos desafios contemporâneos da cibersegurança no setor público.

A estrutura do trabalho foi organizada para garantir coesão entre os objetivos e os dados apresentados, de modo a possibilitar uma leitura crítica e sistematizada dos problemas enfrentados pelas instituições estatais no ambiente digital. Com isso, pretende-se não apenas diagnosticar fragilidades, mas também contribuir com recomendações concretas para a construção de uma política pública de segurança cibernética mais robusta, efetiva e alinhada aos padrões internacionais.

3 Desenvolvimento da pesquisa

No ano de 2020, o Superior Tribunal de Justiça (STJ) sofreu um grave ataque cibernético que interrompeu suas atividades por mais de uma semana, evidenciando exposições técnicas significativas na segurança digital do Poder Judiciário brasileiro. O malware identificado como vetor do ataque foi o ransomware RansomExx, uma ameaça sofisticada que se propaga por meio de fragilidades críticas conhecidas, como a "Zerologon" — uma falha explorada em sistemas Windows Server que permite a elevação de privilégios e o acesso não autorizado a servidores centrais (Palazolo, 2020). Esse ransomware não apenas criptografou os dados do STJ, como também comprometeu os backups institucionais, tornando a recuperação do sistema complexa e demorada. A resposta ao incidente envolveu a Polícia Federal, que liderou a investigação, com apoio técnico da Microsoft e da Força Aérea Brasileira, refletindo a gravidade do ataque e o esforço conjunto do Estado para mitigar seus efeitos (UOL, 2020). Como consequência direta, milhares de processos judiciais ficaram inacessíveis, causando atrasos e prejuízos à prestação jurisdicional.

Outro episódio de relevância ocorreu em dezembro de 2021, quando o sistema ConecteSUS, ligado ao Ministério da Saúde, sofreu um ataque que comprometeu mais de 50 terabytes de dados relacionados ao cadastro de vacinação contra a COVID-19. Este incidente resultou em instabilidades na emissão de certificados digitais, essenciais para a mobilidade social e econômica em meio à pandemia (G1, 2021). Além dos impactos técnicos, o ataque alimentou campanhas de desinformação e narrativas negacionistas,

agravando a crise sanitária e enfraquecendo a confiança da população nos serviços digitais governamentais (Garcia; Ribeiro, 2022).

Em abril de 2024, foi registrada uma tentativa de invasão ao Sistema Integrado de Administração Financeira do Governo Federal (SIAFI), um dos sistemas mais críticos da administração pública brasileira. Embora o ataque tenha sido contido a tempo, a ocorrência expôs deficiências nas credenciais e nos mecanismos de autenticação adotados pelos órgãos centrais do Estado (CTIR-GOV, 2024). Tais lacunas indicam a necessidade de adoção de tecnologias modernas, como autenticação multifator e monitoramento contínuo das redes governamentais.

De acordo com dados oficiais do Centro de Tratamento e Resposta a Incidentes Cibernéticos da Administração Pública Federal (CTIR-Gov), foram notificados 15.132 incidentes de segurança cibernética envolvendo órgãos federais em 2023, com mais de 4.400 ocorrências registradas somente no primeiro semestre de 2024, indicando uma intensificação dos riscos digitais (CTIR-GOV, 2024). Este aumento é acompanhado pela profissionalização dos incidentes, que contam com recursos técnicos sofisticados e objetivos cada vez mais estratégicos, incluindo a paralisação de serviços essenciais e o roubo de informações sensíveis.

A pesquisadora Solange Ghernaouti (2019) ressalta que “os Estados que negligenciam a proteção de seus sistemas digitais comprometem sua soberania e colocam em risco os direitos de seus cidadãos”, enfatizando a importância da segurança cibernética como componente fundamental da governança estatal e proteção social. No âmbito jurídico, embora a promulgação da Lei Geral de Proteção de Dados (Lei nº 13.709/2018) tenha representado um avanço significativo na proteção da privacidade dos cidadãos, ainda não existem normas específicas que estabeleçam padrões obrigatórios de segurança cibernética para órgãos públicos (BRASIL, 2018). O Marco Civil da Internet (Lei nº 12.965/2014), por sua vez, define princípios e garantias gerais relacionados à internet, mas não detalha mecanismos técnicos de defesa para a administração pública (BRASIL, 2014).

A Estratégia Nacional de Segurança Cibernética (E-Ciber), lançada em 2020 pelo Gabinete de Segurança Institucional da Presidência da República, constitui um marco

importante ao estabelecer diretrizes para a proteção das infraestruturas críticas do país e a coordenação de esforços entre órgãos públicos e privados. Contudo, esta estratégia ainda carece de um órgão regulador autônomo e com competência técnica para a sua efetiva implementação e fiscalização (BRASIL, 2020). O Brasil ainda não ratificou a Convenção de Budapeste sobre o Cibercrime, o que dificulta a cooperação internacional em investigações e na responsabilização de agentes envolvidos em incidentes cibernéticos, dado o caráter transnacional dessas ameaças (COUNCIL OF EUROPE, 2001).

Em tramitação no Congresso Nacional, o Projeto de Lei nº 2.310/2021 propõe a criação de um marco regulatório específico para a segurança das infraestruturas críticas de informação, visando estabelecer requisitos mínimos de proteção e a criação de uma Autoridade Nacional de Segurança Cibernética com poderes regulatórios e sancionatórios (CÂMARA DOS DEPUTADOS, 2021).

4 Conclusões

Os incidentes cibernéticos analisados neste estudo evidenciam que a estrutura de segurança digital do setor público brasileiro é frágil, despadronizada e carente de coordenação institucional. O número progressivo de incidentes, aliado à sofisticação das ferramentas utilizadas pelos atacantes, expõe não apenas falhas técnicas, mas também limitações jurídicas, políticas e administrativas.

A resposta do Estado tem sido reativa e fragmentada, o que dificulta a prevenção de novos incidentes. É necessário implementar medidas estruturantes, como a padronização de protocolos de segurança para todos os entes públicos, capacitação continuada de servidores, fortalecimento de parcerias internacionais para troca de informações e investigações, além de aprovação de legislação específica sobre segurança cibernética institucional.

Conclui-se que a segurança cibernética no setor público deve ser tratada como política de Estado e componente estratégico da soberania nacional. A ausência de respostas

efetivas coloca em risco não apenas a integridade dos dados, mas a funcionalidade dos próprios serviços públicos e a confiança da população. O enfrentamento dos desafios aqui descritos exige ação coordenada, investimento técnico e compromisso político com a proteção digital do Estado e da cidadania.

5 Referências

BRASIL. **Estratégia Nacional de Segurança Cibernética – E-Ciber**. Brasília: Gabinete de Segurança Institucional da Presidência da República, 2020. Disponível em: https://www.gov.br/gsi/pt-br/assuntos/cyberseguranca/e-ciber. Acesso em: 23 jun. 2025.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Marco Civil da Internet. Diário Oficial da União: seção 1, Brasília, DF, p. 1, 24 abr. 2014.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União: seção 1, Brasília, DF, p. 1, 15 ago. 2018.

CÂMARA DOS DEPUTADOS. **Projeto de Lei nº 2.310/2021**. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2306187. Acesso em: 15 maio. 2025.

COUNCIL OF EUROPE. **Convention on Cybercrime** (Budapest Convention). Budapest, 2001. Disponível em: https://www.coe.int/en/web/cybercrime/the-budapest-convention. Acesso em: 20 mar. 2025.

CTIR-GOV. **CTIR-Gov em números**. Brasília: Governo Federal, 2024. Disponível em: https://www.gov.br/ctir. Acesso em: 09 jul. 2025.

G1. Conecte SUS é alvo de ataque hacker e sai do ar. **G1**, 10 dez. 2021. Disponível em: https://g1.globo.com. Acesso em: 10 jul. 2025.

GHERNAOUTI, Solange. **Cyberpower**: Crime, Conflict and Security in Cyberspace. Lausanne: EPFL Press, 2019.

PALAZOLO, Gustavo. RansomExx: Análise técnica do ransomware utilizado no ataque ao STJ. **Medium**, 2020. Disponível em: https://gustavopalazolo.medium.com. Acesso em: 10 jul. 2025.

TRIBUNAL DE CONTAS DA UNIÃO (Brasil). **Lista de alto risco**: segurança da informação e segurança cibernética. Brasília: TCU, 2023. Disponível em: https://sites.tcu.gov.br/listadealtorisco/seguranca_da_informacao_e_seguranca_cibernetica.html. Acesso em: 09 jul. 2025.

UOL. Ransomware que atingiu STJ também atacou TJ-PE e outros países. **UOL Tilt**, 7 nov. 2020. Disponível em: https://www.uol.com.br/tilt. Acesso em: 10 jul. 2025.