

Governança Pública e Digital: uma análise de incidentes cibernéticos

Public and Digital Governance: an analysis of cyber incidents

Gobernanza pública y digital: un análisis de incidentes cibernéticos

Grupo temático 10 - Pensamento Social Brasileiro, Reforma Administrativa e Inovação

Gabriella Pinheiro Rezende, Instituto Serzedello Corrêa/Tribunal de Contas da União – ISC/TCU

Hugo Leonardo Menezes de Carvalho, Instituto Serzedello Corrêa/Tribunal de Contas da União – ISC/TCU

RESUMO

Este artigo tem por objetivo analisar, em perspectiva comparada, como diferentes dimensões de governança, capital humano e desenvolvimento econômico se relacionam com a incidência de ataques cibernéticos em países do G20, no período 2020-2024. Ancorado na *Cyber-Routine Activity Theory*, o estudo interpreta os ataques como resultado da convergência entre alvos valiosos, capacidades de proteção e contextos institucionais específicos. A governança digital é operacionalizada por meio do *Global Cybersecurity Index* (GCI), de indicadores de integridade (*Corruption Perception Index*), estabilidade política (*Political Stability and Absence of Violence/Terrorism*) e participação cidadã (*Voice and Accountability*), enquanto o ambiente digital e socioeconômico é captado pelo *Mobile Connectivity Index* (MCI), expectativa média de escolaridade, PIB per capita (PPC) e PIB total (PIB).

Metodologicamente, emprega-se regressão linear múltipla com 95 observações país/ano. O modelo apresenta bom ajuste ($R^2 = 0,6531$; R^2 ajustado = 0,6209), indicando que cerca de 65% da variação nos incidentes cibernéticos é explicada pelo conjunto de variáveis. Os resultados mostram que riqueza econômica aumenta de forma significativa a incidência de ataques, ao passo que melhor percepção de corrupção e maior estabilidade política associam-se a sua redução. *Voice and Accountability* apresenta efeito positivo significativo, sugerindo que regimes mais abertos e responsivos registram mais incidentes por disporem de guardiões institucionais mais capazes de detectá-los. A expectativa média de escolaridade exerce efeito protetivo, reduzindo a incidência observada. Já GCI e MCI não se mostram significativos quando controladas as demais dimensões.

As principais limitações decorrem da natureza transversal dos dados, da dependência de registros oficiais sujeitos a subnotificação e da ausência de medidas mais finas de capacidade operacional em ciberdefesa. Ainda assim, o estudo contribui ao integrar, em um mesmo modelo, governança, fatores digitais, capital humano e riqueza, oferecendo evidências sobre como esses elementos moldam a exposição e a visibilidade dos ataques no setor público. Sugere-se, para pesquisas futuras, o uso de modelos em painel, equações estruturais e estudos de caso que aprofundem os mecanismos identificados, especialmente à luz da transparência, do debate emergente sobre soberania digital e seus impactos na governança pública e controles que cooperem na mitigação de riscos cibernéticos.

Palavras-chave: governança digital, ataques cibernéticos, G20, *Cyber-Routine Activity Theory* (CRAT)

ABSTRACT

This article aims to analyze, from a comparative perspective, how different dimensions of governance, human capital, and economic development relate to the incidence of cyberattacks in G20 countries between 2020 and 2024. Anchored in Cyber Routine Activity Theory, the study interprets attacks as the result of the convergence between valuable targets, protection capabilities, and specific institutional contexts. Digital governance is operationalized through the Global Cybersecurity Index (GCI), indicators of integrity (Corruption Perception

Index), political stability (Political Stability and Absence of Violence/Terrorism), and citizen participation (Voice and Accountability), while the digital and socioeconomic environment is captured by the Mobile Connectivity Index (MCI), average expected years of schooling, GDP per capita (PPP), and total GDP (GDP).

Methodologically, multiple linear regression with 95 country/year observations is used. The model fits well ($R^2 = 0.6531$; adjusted $R^2 = 0.6209$), indicating that about 65% of the variation in cyber incidents is explained by the set of variables. The results show that economic wealth significantly increases the incidence of attacks, while a better perception of corruption and greater political stability are associated with its reduction. Voice and Accountability have a significant positive effect, suggesting that more open and responsive regimes record more incidents because they have institutional guardians that are better able to detect them. Average expected years of schooling has a protective effect, reducing the observed incidence. GCI and MCI, however, are not significant when controlling for other dimensions.

The main limitations stem from the cross-sectional nature of the data, the dependence on official records subject to underreporting, and the absence of more refined measures of operational capacity in cyber defense. Nevertheless, the study contributes by integrating governance, digital factors, human capital, and wealth into a single model, providing evidence on how these elements shape the exposure and visibility of attacks in the public sector. For future research, we suggest the use of panel models, structural equations, and case studies that delve deeper into the mechanisms identified, especially in light of transparency, the emerging debate on digital sovereignty and its impacts on public governance, and controls that cooperate in mitigating cyber risks.

Keywords: digital governance, cyber attacks, G20, Cyber-Routine Activity Theory (CRAT)

RESUMEN

El objetivo de este artículo es analizar, desde una perspectiva comparativa, cómo las diferentes dimensiones de la gobernanza, el capital humano y el desarrollo económico se relacionan con la incidencia de los ciberataques en los países del G20, en el período 2020-2024. Basándose en la Cyber Routine Activity Theory (CRAT), el estudio interpreta los ataques como el resultado de la convergencia entre objetivos valiosos, capacidades de protección y contextos institucionales específicos. La gobernanza digital se opera mediante el Global Cybersecurity Index (GCI), indicadores de integridad (Corruption Perception Index), estabilidad política (Political Stability and Absence of Violence/Terrorism) y participación ciudadana (Voice and Accountability), mientras que el entorno digital y socioeconómico se capta mediante el Mobile Connectivity Index (MCI), la expectativa media de escolaridad, el PIB per cápita (PPC) y el PIB total (PIB).

Metodológicamente, se emplea una regresión lineal múltiple con 95 observaciones por país/año. El modelo presenta un buen ajuste ($R^2 = 0,6531$; R^2 ajustado = 0,6209), lo que indica que alrededor del 65 % de la variación en los incidentes cibernéticos se explica por el conjunto de variables. Los resultados muestran que la riqueza económica aumenta significativamente la incidencia de los ataques, mientras que una mejor percepción de la corrupción y una mayor estabilidad política se asocian con su reducción. Voice and Accountability tiene un efecto positivo significativo, lo que sugiere que los regímenes más abiertos y receptivos registran más incidentes porque cuentan con guardianes institucionales más capaces de detectarlos. La expectativa media de escolaridad ejerce un efecto protector, reduciendo la incidencia observada. Por su parte, el GCI y el MCI no resultan significativos cuando se controlan las demás dimensiones.

Las principales limitaciones se derivan de la naturaleza transversal de los datos, de la dependencia de registros oficiales sujetos a subnotificación y de la ausencia de medidas más precisas de la capacidad operativa en ciberdefensa. Aun así, el estudio contribuye al integrar, en un mismo modelo, la gobernanza, los factores digitales, el capital humano y la riqueza, ofreciendo pruebas sobre cómo estos elementos configuran la exposición y la visibilidad de los ataques en el sector público. Se sugiere, para futuras investigaciones, el uso de modelos de panel, ecuaciones estructurales y estudios de caso que profundicen en los mecanismos identificados, especialmente a la luz de la transparencia, el debate emergente sobre la soberanía digital y sus impactos en la gobernanza pública y los controles que cooperan en la mitigación de los riesgos cibernéticos.

Palabras clave: gobernanza digital, ciberataques, G20, Cyber-Routine Activity Theory (CRAT)

1. Introdução

A preservação da autonomia tecnológica e a eficácia da proteção do domínio informacional dependem da solidez das estratégias de governança digital adotadas pelos Estados (Floridi, 2020). De acordo com a *Cyber-Routine Activity Theory* (CRAT), a criminalidade no ciberespaço é explicada pela convergência entre agressores motivados, alvos adequados e a ausência de guardiões capazes (Leukfeldt & Yar, 2016). Sob esse prisma teórico, a governança digital pode ser compreendida como o exercício da capacidade institucional para monitorar dados e infraestruturas, atuando como moderadora de riscos (Pierucci, 2025). Tal estrutura de controle estatal é essencial para mitigar vulnerabilidades sistêmicas e assegurar a resiliência nacional frente a ofensivas externas (Kaloudis, 2021).

A governança digital de uma nação é frequentemente operacionalizada por meio de indicadores de maturidade que avaliam o compromisso institucional com a cibersegurança (*International Telecommunication Union*, 2024). Essa capacidade pode ser mensurada a partir de dimensões que incluem o arcabouço legal, medidas técnicas, estruturas organizacionais e cooperação internacional (*International Telecommunication Union*, 2024). O *Global Cybersecurity Index* (GCI) consolida-se como uma *proxy* importante e consistente de controle e governança, representando a presença de "guardiões capazes" no ambiente virtual (Liyanage et al., 2024). Assim, a maturidade refletida pelo GCI correlaciona-se com a prontidão do Estado em formular políticas de proteção para infraestruturas críticas (Büyükoçkan & Güler, 2025).

A literatura acadêmica contemporânea enfatiza que a intensificação da conectividade digital tende a elevar a exposição estrutural dos países a ameaças cibernéticas (Chen et al., 2023). Estudos empíricos sugerem que o fortalecimento dos mecanismos de controle não reduz necessariamente o volume de ataques, mas qualifica a capacidade de detecção institucional (Goldoni et al., 2024). Observa-se que a soberania digital, enquanto projeto de governança, atua na mediação da visibilidade dos incidentes captados pelas estatísticas oficiais (Hummel et al., 2021). Nesse sentido, o papel da governança institucional é fundamental para gerenciar o impacto das ofensivas, independentemente da frequência observada (Sheikh, 2022).

A atratividade de um alvo no ciberespaço está intrinsecamente ligada a sua centralidade econômica e à densidade de seus ativos digitais (Bruce et al., 2024). Nações com elevado Produto Interno Bruto (PIB) oferecem mais oportunidades e recompensas estratégicas para agressores motivados (Chen et al., 2023). A CRAT aponta que a concentração de riqueza informacional torna certas economias alvos preferenciais em contextos de conflitos híbridos (Polido, 2024). Além disso, o nível de escolaridade e o capital humano influenciam tanto a extensão da superfície de ataque quanto a competência de monitoramento estatal (Yalamancheli, 2025).

Apesar da relevância do tema, ainda persistem lacunas sobre como a governança institucional afeta as métricas de ataques reportados sob a perspectiva da CRAT (Kaloudis, 2021). A teoria sugere que a presença de guardiões qualificados, representados pelo GCI, pode elevar o registro formal de incidentes em vez de os suprimir (Leukfeldt & Yar, 2016). São incipientes as pesquisas que examinam sistematicamente como o paradoxo da maturidade se manifestam em agrupamentos econômicos distintos (Broeders, 2023). Por essa razão, há uma necessidade de testar empiricamente se a eficácia da governança digital é um preditor positivo da incidência observada de ataques (Goldoni et al., 2024).

Ante esse cenário, surge o seguinte problema de pesquisa: Qual a relação entre ataques e governança digital dos países? Desse modo, o objetivo deste trabalho é analisar a relação entre ataques e governança digital dos países. Para tanto, a metodologia utilizada foi de natureza quantitativa, com a estimação de um modelo de regressão com dados em painel, com dados do período de 2020 a 2024, dos países do G20.

Desta forma, em termos práticos espera-se que os resultados do estudo possam incentivar o aprimoramento de políticas públicas voltadas a governança digital nacional para evidenciar a relevância atual dessa temática e seus impactos no cotidiano das nações. Já em termos teóricos avança em aplicar os pressupostos da *Cyber-Routine Activity Theory* como perspectiva de análise relacionadas a causalidade de ataques digitais ao reinterpretar as estatísticas de ataques como reflexos da capacidade de detecção institucional (Broeders, 2023), ampliando o escopo de conhecimento sobre a literatura do tema.

2. Revisão da Literatura e Hipóteses

2.1 *Cyber-Routine Activity Theory* e os Ataques Cibernéticos

A teoria das atividades rotineiras (RAT) postula que a ocorrência de um crime exige a convergência de um agressor motivado, um alvo adequado e a ausência de um guardião capaz (Leukfeldt & Yar, 2016).

Originalmente concebida para o espaço físico, essa perspectiva foi transposta para o ambiente virtual através da *Cyber-Routine Activity Theory* (CRAT) para explicar a vitimização online (Choi, 2008). A premissa central é que as rotinas digitais dos usuários e instituições criam janelas de oportunidade para a exploração criminosa (Leukfeldt & Yar, 2016). Nesse contexto, o crime cibernético é analisado como um fenômeno sociotécnico dependente da interação entre agentes e infraestruturas (Yar, 2005). Essa abordagem permite identificar como o comportamento cotidiano em rede influencia o risco de ataques (Leukfeldt & Yar, 2016).

No ecossistema digital, o agressor motivado possui habilidades técnicas para navegar em redes complexas e identificar brechas de segurança (Leukfeldt & Yar, 2016). A motivação desses agentes pode ser impulsionada por interesses financeiros, ideológicos ou geopolíticos (Choi, 2008). Diferentemente do crime tradicional, o agressor cibernético opera sem a necessidade de contiguidade física com sua vítima (Yar, 2005). A arquitetura da internet proporciona anonimato e facilita a persistência de ofensivas transnacionais (Leukfeldt & Yar, 2016). Assim, a onipresença de ameaças torna a análise dos alvos e dos guardiões ainda mais crítica para a defesa nacional (Leukfeldt & Yar, 2016).

A adequação do alvo no ciberespaço é definida pela sua visibilidade, valor estratégico e acessibilidade técnica (Leukfeldt & Yar, 2016). Nações com infraestruturas altamente digitalizadas oferecem uma superfície de ataque expandida para criminosos (Chen et al., 2023). Alvos de alto valor incluem sistemas financeiros, redes de energia e bancos de dados governamentais (Sheikh, 2022). A centralidade econômica de um país aumenta a probabilidade de ele ser selecionado como alvo estratégico em conflitos híbridos (Polido, 2024). Portanto, a atratividade do alvo é uma variável diretamente proporcional ao desenvolvimento digital da nação (Bruce et al., 2024).

O guardião capaz no ambiente digital refere-se a mecanismos técnicos e humanos que impedem a consumação do ataque (Leukfeldt & Yar, 2016). Estes guardiões podem ser softwares de proteção, protocolos de criptografia ou equipes de resposta a incidentes (Choi, 2008). A eficácia da guarda depende da capacidade de monitoramento constante e da rapidez na detecção de anomalias (Goldoni et al., 2024). Em nível estatal, a governança institucional atua como o principal guardião estratégico das infraestruturas críticas (Sheikh, 2022). Contudo, a ausência de guardiões qualificados é o fator que mais contribui para o sucesso de investidas cibernéticas (Leukfeldt & Yar, 2016).

A relação entre desenvolvimento socioeconômico e cibercrime sugere que países mais ricos são vitimizados com maior frequência (Chen et al., 2023). A concentração de ativos digitais e financeiros em economias desenvolvidas atrai uma maior densidade de agressores motivados (Bruce et al., 2024). A penetração da internet e o uso intensivo de tecnologias de informação criam outras rotinas de exposição para o Estado (Leukfeldt & Yar, 2016). Esse cenário evidencia que a riqueza nacional atua como um preditor da atratividade do alvo (Chen et al., 2023). Assim, a exposição estrutural é uma consequência intrínseca da centralidade digital global (Bruce et al., 2024).

Estudos empíricos indicam que a maturidade institucional em cibersegurança pode paradoxalmente levar ao aumento do registro de ataques (Goldoni et al., 2024). Guardiões mais sofisticados possuem maior capacidade de identificar e reportar incidentes que antes passariam despercebidos (Goldoni et al., 2024). A transparência nas estatísticas de ataques é, portanto, um reflexo da prontidão estatal e não apenas da fragilidade técnica (Sheikh, 2022). Esse fenômeno reforça a necessidade de distinguir entre o volume de incidentes e a vulnerabilidade real (Bruce et al., 2024). Desta forma, o paradoxo da governança reside na visibilidade que a proteção confere às ameaças (Goldoni et al., 2024).

A incidência observada de ataques cibernéticos é resultado da interação dinâmica entre os elementos da CRAT no tempo e espaço (Leukfeldt & Yar, 2016). O volume de dados transacionados e a integração de sistemas aumentam as oportunidades para delitos informacionais (Hummel et al., 2021). A eficácia da governança nacional é o que define se a convergência entre agressor e alvo resultará em impacto sistêmico (Sheikh, 2022). A proteção do espaço virtual exige, portanto, um fortalecimento contínuo da capacidade de guarda estatal (Yalamancheli, 2025). Assim, a incidência de ataques torna-se um indicador da complexidade do ambiente digital nacional (Bruce et al., 2024).

Diante do exposto, argumenta-se que a governança institucional atua como o moderador central do risco cibernético estatal (Floridi, 2020). Países com maior maturidade normativa e técnica estão melhor preparados para monitorar e mitigar ofensivas (Kaloudis, 2021). No entanto, o nível de riqueza econômica permanece como o principal motor da atratividade para agressores externos (Chen et al., 2023). A integração desses fatores fundamenta a análise sobre como o controle institucional interage com a criminalidade (Sheikh, 2022). Com base nessas premissas, formulou-se a seguinte hipótese de pesquisa: H0: A governança digital é positiva e

estatisticamente significativa para explicar a incidência observada de ataques cibernéticos devido à maior capacidade de detecção.

2.2 Governança Digital

A governança digital é definida como a capacidade de um Estado de exercer autoridade e controle sobre seus sistemas de informação e fluxos de dados (Floridi, 2020). Este conceito abrange o desenvolvimento de infraestruturas técnicas, marcos regulatórios e competências humanas (Pierucci, 2025). Para além da regulação, a governança busca garantir a resiliência das instituições frente a ameaças transnacionais e crises cibernéticas (Kaloudis, 2021). A eficácia governamental no domínio digital é fundamental para a preservação da estabilidade política e econômica nacional (Sheikh, 2022). Nesse sentido, a governança digital não é apenas um projeto técnico, mas uma dimensão da capacidade estatal contemporânea (Falkner et al., 2024).

Os fundamentos da governança digital repousam sobre a articulação entre políticas públicas e segurança de infraestruturas críticas (Sheikh, 2022). A governança eficaz requer a colaboração entre o setor público, privado e atores internacionais para enfrentar ameaças distribuídas (*International Telecommunication Union*, 2024). A gestão de riscos cibernéticos torna-se, assim, uma prioridade estratégica para governos que buscam autonomia tecnológica (Pierucci, 2025). A proteção de dados e a integridade de sistemas de comunicação são pilares essenciais para o funcionamento da sociedade moderna (Hummel et al., 2021). Portanto, a robustez da governança digital determina a competitividade do país no sistema internacional (Falkner et al., 2024).

Esta perspectiva enfatiza que a capacidade estatal no domínio digital não é um atributo fixo ou binário, mas sim uma construção institucional contingente, que se expressa por meio de políticas, estratégias, arcabouços regulatórios e capacidades técnicas e humanas (Floridi, 2020). Diversos autores têm contribuído para a conceitualização da governança digital como fenômeno multidimensional. Hummel et al. (2021), em revisão abrangente da literatura, identificam que a capacidade de governança no ambiente digital envolve múltiplas dimensões inter-relacionadas: controle sobre dados, capacidade regulatória, proteção de infraestruturas críticas, desenvolvimento de competências técnicas e estabelecimento de mecanismos de cooperação internacional. Os autores enfatizam que estas dimensões não operam isoladamente, mas constituem um sistema integrado cuja efetividade depende da coerência e coordenação entre seus elementos.

Sheikh (2022) propõe uma abordagem em camadas (*layered approach*) para a análise da governança digital, segundo a qual a capacidade estatal deve ser compreendida como um conjunto de competências distribuídas ao longo de diferentes níveis do *stack* digital como infraestrutura, protocolos, aplicações, dados e governança. Esta perspectiva tem a vantagem de reconhecer que diferentes dimensões da governança podem apresentar níveis distintos de desenvolvimento em um mesmo país, e que a efetividade global depende da articulação entre estas camadas.

Já Falkner et al. (2024) demonstram que discursos sobre autonomia digital frequentemente antecedem, mas nem sempre se traduzem em políticas públicas concretas e capacidades operacionais. Os autores identificam uma lacuna significativa entre intenções declaradas e implementação efetiva, sugerindo que a análise da governança digital deve focalizar indicadores concretos de capacidade institucional, em vez de declarações de princípio. Nesta mesma linha, Moerel e Timmers (2021) argumentam que a governança digital abrange não apenas sistemas técnicos e dados, mas também valores democráticos, arranjos econômicos, autonomia regulatória e proteção de infraestruturas críticas. Para os autores, a capacidade de governança manifesta-se na habilidade estatal de formular políticas coerentes, regular plataformas digitais, proteger ativos estratégicos e desenvolver competências tecnológicas internas.

Disso decorre outra vertente emergente, a mensuração da governança digital que pode ser avaliada através de índices multidimensionais que mensuram a prontidão institucional (*International Telecommunication Union*, 2024). Estes indicadores analisam aspectos legais, técnicos, organizacionais, de capacitação e de cooperação (*International Telecommunication Union*, 2024). O fortalecimento da governança pressupõe a existência de estratégias nacionais de cibersegurança claras e atualizadas (Sheikh, 2022). A conformidade com padrões internacionais de segurança digital eleva a confiança nas infraestruturas nacionais (Büyükoçkan & Güler, 2025). Assim, a governança digital manifesta-se como uma função do desenvolvimento institucional e técnico do Estado (Silveira & Xiong, 2025).

O *Global Cybersecurity Index* (GCI) constitui a principal proxy para medir a governança digital em uma perspectiva comparativa *cross-country* (*International Telecommunication Union*, 2024). Este índice reflete o compromisso dos governos com a criação de um ambiente digital seguro e resiliente (Liyanage et al., 2024).

Elevados valores no GCI indicam a presença de estruturas de controle voltadas à mitigação de vulnerabilidades sistêmicas (Büyükoçkan & Güler, 2025). O índice permite monitorar a evolução das capacidades defensivas e a eficácia das políticas nacionais de proteção (*International Telecommunication Union*, 2024). Por essa razão, o GCI é amplamente utilizado na literatura como indicador de maturidade em governança cibernética (Liyanage et al., 2024).

A governança digital fundamentada na transparência institucional promove uma maior eficiência no combate ao cibercrime (Goldoni et al., 2024). Instituições que adotam práticas de reporte e auditoria de sistemas tendem a possuir bases de dados mais precisas sobre incidentes (Sheikh, 2022). A visibilidade estatística dos ataques é, em muitos casos, um subproduto de uma governança madura e responsável (Goldoni et al., 2024). Ao institucionalizar a detecção, o Estado amplia seu conhecimento sobre o ambiente de ameaças (Pierucci, 2025). Desse modo, a qualidade da governança influencia diretamente a métrica de incidentes reportados (Sheikh, 2022).

Outro aspecto central diz respeito ao nível de desenvolvimento econômico como determinante da capacidade de governança (Chen et al., 2023). Nações com maiores recursos financeiros possuem maior capacidade de investimento em tecnologias defensivas e treinamento especializado (Bruce et al., 2024). O Produto Interno Bruto (PIB) correlaciona-se positivamente com a sofisticação das ferramentas de monitoramento cibernético (Chen et al., 2023). No entanto, o mesmo desenvolvimento econômico que financia a governança também amplia a atratividade do país para agressores (Bruce et al., 2024). Por essa razão, faz sentido verificar como a riqueza interage com os indicadores de controle (Chen et al., 2023).

A qualidade e a confiança institucionais potencializam as estratégias de governança digital (Hellvig, 2023). Governos mais eficazes conseguem implementar políticas de segurança de forma mais célere e coordenada (Goldoni et al., 2024). A resiliência cibernética é reforçada quando o arcabouço legal é aplicado de maneira justa e transparente (Falkner et al., 2024). Instituições sólidas reduzem a probabilidade de exploração interna de vulnerabilidades e favorecem a colaboração público-privada (Hellvig, 2023). Assim, integridade institucional e transparência atuam como catalisadores para a eficácia das defesas digitais (Goldoni et al., 2024).

A capacidade de inovação tecnológica é uma força motriz para o aprimoramento contínuo da governança digital (Liyanage et al., 2024). Países na vanguarda tecnológica desenvolvem soluções de ponta para a proteção de infraestruturas críticas (Yalamancheli, 2025). Políticas de incentivo à inovação fortalecem a base industrial de defesa e a autonomia estratégica (Sheikh, 2022). No entanto, a inovação também introduz novas complexidades e riscos que devem ser geridos pela governança (Pierucci, 2025). Desse modo, o equilíbrio entre o fomento à tecnologia e a regulação de riscos é o cerne da governança moderna (Falkner et al., 2024).

O capital humano, representado na dimensão de nível de escolaridade, é a base sobre a qual se constrói a governança digital sustentável (Yalamancheli, 2025). Sociedades mais educadas possuem maior consciência sobre riscos e melhores práticas de higiene digital (Creese et al., 2021). A formação de especialistas em segurança da informação é um componente crítico para a operacionalização da governança estatal (Yalamancheli, 2025). A educação técnica permite que o Estado desenvolva e mantenha suas próprias soluções de proteção contra-ataques (Yalamancheli, 2025). Portanto, o investimento em educação digital é um pilar estruturante do controle governamental sobre o ciberespaço (Creese et al., 2021).

Nota-se que elementos como riqueza econômica, qualidade institucional e capital humano interagem de maneira sistêmica com a governança digital (Chen et al., 2023). Embora a literatura aponte caminhos para a resiliência, ainda são necessários testes sobre como esses fatores impactam o volume de ataques (Goldoni et al., 2024). A integração de múltiplas *proxies* de desenvolvimento permite uma visão holística da maturidade institucional de um país (Kaloudis, 2021). Ao analisar o GCI em conjunto com variáveis estruturais, o estudo busca elucidar a eficácia real das defesas estatais (Silveira & Xiong, 2025). Diante disso, estabeleceu-se a seguinte hipótese:

H1: A riqueza econômica do país é positiva e estatisticamente significativa para explicar a incidência de ataques cibernéticos em razão da maior atratividade do alvo.

3. Procedimentos Metodológicos

Este estudo adota uma abordagem quantitativa, de natureza explicativa, orientada pelo arcabouço da *Cyber Routine Activity Theory* (CRAT) para investigar a relação entre governança, desenvolvimento socioeconômico e incidência de ataques cibernéticos em países do G20. A estratégia empírica baseia-se na estimação de um modelo de regressão linear múltipla com dados secundários em nível país/ano, cobrindo o período de 2020 a 2024. As variáveis foram coletas em sites eletrônicos oficiais, operacionalizadas a partir de indicadores

internacionais, como o *Global Cybersecurity Index* (GCI), o *Mobile Connectivity Index* (MCI), indicadores de governança mundiais de estabilidade política e *accountability* cidadão componentes do *World Governance Indicators*, além de dados socioeconômicos e de capital humano, de modo a permitir a comparabilidade entre países e alinhamento conceitual com as dimensões teóricas e controle institucional.

Os dados estatísticos e econômicos foram extraídos de fontes oficiais e bases públicas internacionais (ITU – *The International Telecommunication Union*, GSM Association, *Transparency International*, *World Bank*, UNDP – *United Nations Development Programme*, entre outras) e consolidados em planilha própria. Todas as análises foram realizadas em ambiente de planilha eletrônica (Excel) e em software estatístico (Jasp), com emprego de estatísticas descritivas, análises de correlações e regressão linear múltipla.

3.1 Definição da amostra e coleta de dados

Para o estudo foram utilizados dados dos 19 países componentes do G20, a saber: África do Sul, Alemanha, Arábia Saudita, Argentina, Austrália, Brasil, Canadá, China, Coreia do Sul, Estados Unidos, França, Índia, Indonésia, Itália, Japão, México, Reino Unido, Rússia e Turquia. A escolha desse grupo se deu pela relevância e diferenciação econômica e geográfica (Sheraz, M., Deyi, X., Ahmed, J. et al., 2021).

A amostra é composta por 95 observações relativas a dados do G20. A variável dependente está representada pela quantidade de incidentes cibernéticos com proporções políticas sofridos por cada país. As variáveis independentes abrangem as dimensões de governança, digital, educacional, social e econômica. Isso posto, configura-se um conjunto integrado de dados relacionados a fatores que possibilitam uma análise sistêmica da maturidade institucional desses países (Kaloudis, 2021).

Tabela 1

Variáveis do Modelo

Variável	Proxy	Mensuração	Fonte
Cyber Incidents (CI)	Incidentes Cibernéticos	Quantidade de incidentes cibernéticos com dimensões políticas por país/ano	EuRepoC ^a
Global Cybersecurity Index (GCI)	Governança	Índice quanto ao compromisso com a segurança cibernética por país/ano	ITU ^b
Mobile Connectivity Index (MCI)	Digital	Índice de desempenho na adoção da internet móvel por país/ano	GSMA ^c
Corruption Perceptions Index (CPI)	Governança	Índice do nível percebido de corrupção no setor público por país/ano	TI ^d
Political Stability and Absence of Violence/Terrorism (PS)	Governança	Índice relativo à probabilidade de instabilidade política e/ou violência por motivos políticos por país/ano	WB ^e
Voice and Accountability (VA)	Governança	Índice referente à participação dos cidadãos no governo e à liberdade de expressão por país/ano	WB ^f
Expected Years of Schooling (EYS)	Social/Educacional	Quantidade esperada de anos escolares da população por país/ano	UN ^g
GDP per capita (PPC)	Social/Econômica	Valor do Produto Interno Bruto per capita em dólares por país/ano	WB ^h
GDP (PIB)	Econômica	Valor do Produto Interno Bruto em milhões de dólares por país/ano	WB ⁱ

Nota.

^a<https://eurepoc.eu/dashboard/>

^b<https://www.itu.int/en/ITU-D/Cybersecurity/pages/global-cybersecurity-index.aspx>

^c<https://www.mobileconnectivityindex.com/index.html>

^d<https://transparency.org.au/>

^e<https://data.worldbank.org/indicator/PV.EST>

^f<https://data.worldbank.org/indicator/VA.EST>

^g<https://hdr.undp.org/data-center/documentation-and-downloads>

^h<https://data.worldbank.org/indicator/NY.GDP.PCAP.CD>

ⁱ<https://data.worldbank.org/indicator/NY.GDP.MKTP.CD>

Fonte: Elaborada pelos autores.

3.2 Técnica de Estimação e Especificação do Modelo

Estimou-se um modelo de regressão linear múltipla para examinar as associações condicionais entre a variável dependente relativa à quantidade de incidentes cibernéticos (CI) e as variáveis dependentes, conforme especificação do modelo dada por:

$$CI_i = \beta_1 + \beta_2 GCI_i + \beta_3 MCI_i + \beta_4 CPI_i + \beta_5 PS_i + \beta_6 VA_i + \beta_7 EYS_i + \beta_8 PPC_i + \beta_9 PIB_i + \varepsilon_i,$$

Onde:

CI_i : incidência de ataques cibernéticos no país i ;

β_1 : intercepto do modelo, corresponde à constante, ou seja, o lugar onde a linha intercepta o eixo y ;

$\beta_2 GCI_i$: governança digital/maturidade cibernética;

$\beta_3 MCI_i$: maturidade digital móvel;

$\beta_4 CPI_i$: qualidade e confiança institucionais;

$\beta_5 PS_i$: estrutura e segurança político-social;

$\beta_6 VA_i$: manifestação cidadã e *accountability*;

$\beta_7 EYS_i$: desenvolvimento do capital humano;

$\beta_8 PPC_i$: condições econômicas per capita;

$\beta_9 PIB_i$: centralidade econômica;

ε_i : termo de erro, perturbação da relação.

Essa especificação permite identificar o efeito de cada *proxy* dimensionada sobre a incidência de ataques, mantendo constantes as demais covariáveis. O modelo estimado com base em dados transversais deve ser interpretado de maneira associativa, não causal. Foram analisados indicadores de ajuste global (R , R^2 , R^2 ajustado, teste F) e diagnósticos de multicolinearidade (tolerância e Fator de Inflação da Variância - FIV), apresentados na seção de resultados.

4 Apresentação e Análise dos Resultados

4.1 Análise descritiva

As estatísticas descritivas das principais variáveis do modelo indicam um cenário heterogêneo entre os países analisados. O número médio de incidentes cibernéticos por país-ano é de 16,3368 ($DP = 35,1866$), com valores variando entre 0 e 248. A mediana igual a 7 sugere forte assimetria positiva, indicando que alguns países concentram um volume elevado de incidentes enquanto a maioria registra ocorrências relativamente mais baixas. Esse padrão é compatível com a literatura que aponta a concentração de ataques em economias mais digitalizadas e centrais no sistema internacional (Bruce et al., 2024).

Do ponto de vista da maturidade em segurança digital, o *Global Cybersecurity Index* (GCI) apresenta média elevada (93,3764 em uma escala de 0 a 100; $DP = 11,3717$), com mínimo de 50,12 e máximo de 100,00. De modo semelhante, o *Mobile Connectivity Index* (MCI) apresenta média de 80,9138 ($DP = 8,2102$), indicando um nível alto de conectividade móvel na amostra. Esses resultados sugerem que, embora haja variação entre os países, a maior parte deles já se encontra em patamares relativamente avançados de infraestrutura, políticas de segurança e questões de conectividade (Sheikh, 2022), o que reforça a pertinência de investigar como diferenças marginais nesses indicadores se relacionam com a incidência de ataques.

Os indicadores de governança e contexto institucional revelam maior dispersão. O *score* de percepção de corrupção apresenta média de 53,3895 (DP = 17,4985), com amplitude entre 22 e 80 pontos, o que sinaliza diferenças significativas nos níveis de integridade percebida no setor público. A Estabilidade Política e Ausência de Violência/Terrorismo apresenta média levemente negativa (-0,0239; DP = 0,6622), com valores que variam de -1,14 a 1,03, evidenciando a presença tanto de contextos marcados por instabilidade e violência quanto de ambientes relativamente estáveis. O indicador de *Voice and Accountability* tem média positiva (0,3744; DP = 0,9814), mas com variação ampla, refletindo distintos graus de liberdade de expressão, participação cidadã e *accountability* entre as democracias consolidadas e regimes mais fechados.

As variáveis socioeconômicas e de capital humano também confirmam a heterogeneidade da amostra. A expectativa média de escolaridade situa-se em 16,1237 anos (DP = 2,1051), com países em que se esperam menos de 13 anos de estudo e outros que superam 21 anos. O PIB per capita médio é de 42 441,30 dólares (DP = 21 023,78), enquanto o PIB total médio aproxima-se de $4,14 \times 10^6$ milhões de dólares (DP $\approx 6,24 \times 10^6$), com valores máximos em torno de $2,8751 \times 10^7$ milhões. Esses números evidenciam a presença conjunta de grandes economias avançadas e economias emergentes, oferecendo um campo fértil para explorar como desenvolvimento econômico, governança e capacidade estatal se articulam na exposição e registro de incidentes cibernéticos.

Tabela 2

Estatísticas descritivas

	Média	Mediana	D.P.	Mín.	Máx.
CI	16,3368	7,0000	35,1866	0,0000	248,0000
GCI	93,3764	97,4900	11,3717	50,1200	50,1200
MCI	80,9138	83,8700	8,2102	61,7700	92,6200
CPI	53,3895	53,0000	17,4985	22,0000	80,0000
PS	-0,0239	-0,1000	0,6622	-1,1400	1,0300
VA	0,3744	0,7400	0,9814	-1,6600	1,5100
EYS	16,1237	15,9200	2,1051	12,1300	21,0800
PPC	42441,2964	47395,8400	21023,7790	6966,2800	85809,9000
PIB	$4,1404 \times 10^{+6}$	$2,0224 \times 10^{+6}$	$6,2404 \times 10^{+6}$	337974,6600	$2,8751 \times 10^{+7}$

Nota

Fonte: Elaborada pelos autores

4.2 Análise das correlações

A matriz de correlação revela que os incidentes cibernéticos guardam associações bivariadas mais fortes com variáveis econômicas do que com indicadores de governança. A correlação entre incidentes cibernéticos e PIB total é moderada-alta ($r = 0,6196$; $p < 0,001$), enquanto a correlação com o PIB per capita também é positiva e estatisticamente significativa ($r = 0,4345$; $p < 0,001$). Esses resultados sugerem que países economicamente mais fortes, tanto em termos de tamanho da economia quanto de renda média, tendem a registrar mais incidentes, o que é consistente com a hipótese de que maior riqueza e centralidade econômica aumentam a atratividade e a superfície de ataque no ciberespaço.

Em relação às variáveis de maturidade digital, observa-se correlação positiva entre incidentes cibernéticos e o *Mobile Connectivity Index* ($r = 0,3185$; $p \approx 0,002$), indicando que maior conectividade móvel está associada a maior incidência de ataques. Já a correlação com o GCI é positiva, embora fraca e não significativa ao nível convencional ($r = 0,1558$; $p \approx 0,132$), sugerindo que, na análise bivariada, o índice global de cibersegurança tem papel menos evidente na variação do número de incidentes. As correlações com indicadores de governança (percepção de corrupção, estabilidade política e participação e *accountability* cidadãos) são, em geral, de baixa magnitude na análise bruta, reforçando a necessidade de um modelo multivariado para captar seus efeitos condicionais quando se trabalham fatores econômicos e de capital humano.

Tabela 3

Matriz de correlação das variáveis analisadas

	CI	GCI	MCI	CPI	PS	VA	EYS	PPC	PIB
CI	1								
GCI	0,1558	1							
MCI	0,3185 ^b	0,4368 ^c	1						
CPI	0,1889	0,3565 ^c	0,7653 ^c	1					
PS	0,0542	0,1759	0,7157 ^c	0,8885 ^c	1				
VA	0,1307	0,0052	0,4001 ^c	0,6959 ^c	0,7834 ^c	1			
EYS	-0,0263	-0,1142	0,4684 ^c	0,4317 ^c	0,4095 ^c	0,2649 ^b	1		
PPC	0,4345 ^c	0,3682 ^c	0,8302 ^c	0,7529 ^c	0,6270 ^c	0,3638 ^c	0,5142 ^c	1	
PIB	0,6196 ^c	0,1794	0,3401 ^c	0,1799	0,0061	-0,0972	-0,0606	0,2604 ^a	1

Nota.

^a $p < .05$

^b $p < .01$

^c $p < .001$

Fonte: Elaborada pelos autores

À luz da CRAT e da literatura de governança digital, a Tabela 4 resume a direção esperada das relações com a variável dependente e a direção efetivamente encontrada nos coeficientes da regressão:

Tabela 4

Regressão e Correlações Esperadas X Encontradas

Variável independente	Direção da correlação com a variável dependente		Situação
	Esperada	Encontrada	
GCI	Positiva (maior maturidade → maior capacidade de detecção → maior registro de incidentes)	Negativa Não significativa ($\beta = -0,0309$; $p = 0,911$)	Não confirmada (sem efeito estatístico relevante)
MCI	Positiva (maior conectividade → maior superfície de ataque → mais incidentes)	Negativa Não significativa ($\beta = -0,2736$; $p = 0,685$)	Não confirmada (sem efeito estatístico relevante)
CPI	Negativa (melhor integridade → menos vulnerabilidades → menos incidentes)	Negativa Significativa ($\beta = -0,8874$; $p = 0,025$)	Confirmada (direção e significância)

PS	Negativa (maior estabilidade político-social → menos incidentes)	Negativa Significativa ($\beta = -21,4342$; $p = 0,042$)	Confirmada (direção e significância)
VA	Positiva (mais abertura e <i>accountability</i> → mais incidentes registrados/visíveis)	Positiva Significativa ($\beta = 21,0472$; $p < 0,001$)	Confirmada (direção e significância)
EYS	Negativa (maior escolaridade → maior resiliência → menos incidentes)	Negativa Significativa ($\beta = -3,0001$; $p = 0,043$)	Confirmada (direção e significância)
PPC	Positiva (maior riqueza → maior atratividade como alvo → mais incidentes)	Positiva Significativa ($\beta = 0,0014$; $p < 0,001$)	Confirmada (direção e significância)
PIB	Positiva (maior tamanho e influência da economia → maior exposição → mais incidentes)	Positiva Significativa ($\beta = 0,0014$; $p < 0,001$)	Confirmada (direção e significância)

Nota.

Fonte: Elaborada pelos autores

De maneira geral, as direções observadas são consistentes com as expectativas teóricas para as variáveis institucionais, de capital humano e econômicas, fortalecendo a aderência empírica das hipóteses formuladas.

Para avaliar a presença de multicolinearidade entre os regressores, foram calculados os fatores de inflação da variância (VIF). Os valores variam entre 1,6134 (PIB total) e 9,4726 (Estabilidade Política / Ausência de Violência), com o score de percepção de corrupção (CPI) apresentando VIF de 9,2879. Ainda que esses dois últimos valores sinalizem correlações elevadas entre indicadores de governança, sendo isso esperado, dada a natureza interdependente dessas dimensões, todos os VIF permanecem abaixo do limiar de 10 usualmente adotado como indicativo de multicolinearidade severa.

4.3 Análise dos resultados da regressão

O modelo de regressão linear múltipla apresenta ajuste global robusto. O coeficiente de correlação múltipla é $R = 0,8082$, com $R^2 = 0,6531$ e R^2 ajustado = 0,6209, indicando que aproximadamente 65% da variância no número de incidentes cibernéticos entre os países analisados é explicada conjuntamente pelas variáveis de maturidade digital, governança, capital humano e desenvolvimento econômico. O teste F global é altamente significativo ($F(8, 86) = 20,2426$; $p < 0,001$), demonstrando que o conjunto de regressoras contribui de forma estatisticamente relevante para a explicação da variável dependente.

No nível dos coeficientes individuais, destacam-se como estatisticamente significativos ($p < 0,05$): CPI que representa o score de percepção de corrupção ($\beta = -0,8874$; $p = 0,025$), Estabilidade Política/Ausência de Violência ($\beta = -21,4342$; $p = 0,042$), *Voice and Accountability* ($\beta = 21,0472$; $p < 0,001$), Expectativa Média de Escolaridade ($\beta = -3,0001$; $p = 0,043$), PIB per capita ($\beta = 0,0014$; $p < 0,001$) e PIB total ($\beta = 3,1599 \times 10^{-6}$; $p < 0,001$). Já o GCI e o Mobile Connectivity Index (MCI) apresentam coeficientes não significativos, sugerindo que, após o controle pelas demais variáveis, sua contribuição marginal para a explicação dos incidentes não é estatisticamente distinta de zero.

Do ponto de vista teórico, os resultados dialogam diretamente com as hipóteses e com o referencial bibliográfico. A associação positiva e robusta entre PIB per capita, PIB total e incidentes cibernéticos corrobora a

expectativa de que riqueza e centralidade econômica elevam a atratividade dos países como alvos (Chen et al., 2023; Bruce et al., 2024), em linha com a dimensão de “alvos adequados” na CRAT. Ao mesmo tempo, o efeito negativo da percepção de corrupção e da estabilidade política sugere que contextos de maior integridade institucional e menor instabilidade tendem a reduzir a incidência de ataques reportados, reforçando a importância de arranjos institucionais sólidos e previsíveis para a segurança digital (Goldoni et al., 2024).

O coeficiente positivo de *Voice and Accountability*, por sua vez, apoia a interpretação de um “paradoxo da governança”, no qual países com instituições mais abertas, mecanismos de *accountability* mais fortes e maior liberdade de expressão tendem a registrar mais incidentes, não necessariamente porque sejam mais vulneráveis, mas por disporem de guardiões institucionais mais capazes de monitorar, detectar e reportar eventos adversos (Leukfeldt & Yar, 2016; Hummel et al., 2021). Esse achado está em sintonia com a ideia de que maior maturidade democrática e de controle público aumenta a visibilidade estatística dos ataques. Finalmente, o efeito negativo da expectativa média de escolaridade sugere que o desenvolvimento do capital humano pode funcionar como camada de proteção, seja por meio de maior cultura de segurança digital, seja por maior qualificação técnica dos profissionais envolvidos na gestão de ativos informacionais do Estado.

Tabela 5

Resultados da Regressão

	Coeficientes (β)	Erro padrão	Stat t	Valor-p
Intercepto	58,1555	49,2296	1,1813	0,2407
GCI	-0,0309	0,2756	-0,1120	0,9111
MCI	-0,2736	0,6720	-0,4071	0,6850
CPI	-0,8874	0,3892	-2,2802	0,0251
PS	-21,4342	10,3867	-2,0636	0,0421
VA	21,0472	4,0727	5,1679	<0,0001
EYS	-3,0001	1,4622	-2,0517	0,0432
PPC	0,0014	0,0002	6,2310	<0,0001
PIB	$3,1599 \times 10^{-6}$	$4,5484 \times 10^{-7}$	6,9474	<0,0001

Nota.

Fonte: Elaborada pelos autores

5. Considerações Finais

O objetivo geral deste estudo foi analisar, em perspectiva *cross-country*, como diferentes dimensões de governança digital, contexto institucional, capital humano e desenvolvimento econômico se relacionam com a incidência de ataques cibernéticos com impactos políticos no G20, no período compreendido entre 2020 e 2024. Ancorado na *Cyber-Routine Activity Theory*, o trabalho modelou incidentes cibernéticos como resultado da convergência entre alvos valiosos (riqueza e centralidade econômica), níveis diferenciados de proteção institucional (governança, integridade, estabilidade) e capacidades de monitoramento e reporte (participação cidadã e maturidade digital). A metodologia empregada, baseada em regressão linear múltipla com dados secundários em nível país/ano, permitiu testar empiricamente hipóteses derivadas da literatura sobre soberania digital, governança cibernética e geografia dos ataques.

Os resultados indicam que o modelo explica aproximadamente 65% da variação nos incidentes, o que é expressivo para dados comparados entre países. Em termos substantivos, o estudo confirma a relevância das dimensões econômicas, evidenciando que países mais ricos e com maior PIB total tendem a registrar mais ataques, o que reforça a tese de que a atratividade de alvos no ciberespaço responde a incentivos econômicos e à concentração de ativos estratégicos. Ao mesmo tempo, a evidência de que melhor percepção de corrupção e maior estabilidade política se associam a menos incidentes destaca a importância da qualidade institucional para mitigar riscos e fortalecer o controle público sobre a segurança digital. O papel positivo e significativo da variável *Voice and Accountability* relativa à manifestações e participação cidadãs sugere ainda que regimes mais abertos e

responsivos produzem estatísticas mais transparentes sobre incidentes, com implicações diretas para a interpretação de *rankings* e métricas internacionais de cibersegurança.

Do ponto de vista teórico, o artigo contribui ao aproximar a CRAT do debate sobre governança e controle público em ambientes digitais, ao articular dimensões clássicas da teoria (alvos adequados, guardiões capazes, ausência de controle) com indicadores concretos de maturidade cibernética, integridade institucional e desenvolvimento humano. Metodologicamente, o estudo oferece um modelo operacionalizável em futuras pesquisas comparativas, ao combinar dados de diferentes organismos internacionais em um *framework* analítico unificado. Entre as limitações, destacam-se a natureza transversal dos dados, que não permite inferências causais ou explorar dinâmicas temporais, a possível subnotificação de incidentes em contextos menos transparentes, e a ausência de medidas mais detalhadas de capacidade operacional em ciberdefesa (como investimentos específicos, existência de CERTs nacionais ou equipes dedicadas).

Como agenda futura, recomenda-se a ampliação temporal e geográfica da base de dados, de modo a possibilitar o uso de modelos em painel e a identificação de efeitos de longo prazo de reformas institucionais em segurança digital. Sugere-se também o aprofundamento da análise de mecanismos, por meio de abordagens de equações estruturais ou modelos hierárquicos, que permitam explorar como desenvolvimento econômico, capital humano e governança mediam, em conjunto, a exposição e a visibilidade de incidentes. Por fim, estudos de caso qualitativos e análises mistas poderiam complementar a abordagem aqui apresentada, iluminando como arranjos específicos de governança digital e controle público se traduzem, na prática, em diferentes padrões de registro, resposta e aprendizagem institucional diante de ataques cibernéticos e relação com soberania digital.

Referências

- Broeders, D. (2023). In search of digital sovereignty and strategic autonomy: Normative power in the digital age. *Journal of Common Market Studies*, 61(5), 1198–1215. <https://doi.org/10.1111/jcms.13437>
- Bruce, M., et al. (2024). Mapping the global geography of cybercrime. *PLOS ONE*, 19(1), e0297312. <https://doi.org/10.1371/journal.pone.0297312>
- Büyükoçkan, G., & Güler, M. (2025). Cybersecurity maturity model: A systematic review. *Technological Forecasting and Social Change*, 198, 122012. <https://doi.org/10.1016/j.techfore.2025.123996>
- Chen, Z., et al. (2023). Exploring the global geography of cybercrime. *Humanities and Social Sciences Communications*, 10(1), 1–15. <https://doi.org/10.1057/s41599-023-01560-x>
- Falkner, G., et al. (2024). Digital sovereignty – rhetoric and reality. *Journal of European Public Policy*, 31(1), 1–20. <https://doi.org/10.1080/13501763.2023.2260000>
- Floridi, L. (2020). The fight for digital sovereignty. *Philosophy & Technology*, 33(3), 369–378. <https://doi.org/10.1007/s13347-020-00423-6>
- Goldoni, L. R. F., et al. (2024). What is the future of Brazil's cybersecurity governance? *Cadernos Gestão Pública e Cidadania*, 29, e90972. <https://doi.org/10.12660/cgpc.v29.90972.85588>
- Hummel, P., et al. (2021). Data sovereignty: A review. *Big Data & Society*, 8(1). <https://doi.org/10.1177/2053951720982012>
- International Telecommunication Union. (2024). *Global Cybersecurity Index 2024* (5th ed.). <https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx>
- Kaloudis, A. (2021). How can we measure digital sovereignty? SSRN. <https://doi.org/10.2139/ssrn.3822153>
- Leukfeldt, E. R., & Yar, M. (2016). Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis. *Deviant Behavior*, 37(3), 263–280. <https://doi.org/10.1080/01639625.2015.1012491>

ARTIGO

- Liyanage, K., et al. (2024). SoK: Identifying limitations and bridging gaps of CCMMs. *Computers & Security*, 134, 103397. <https://doi.org/10.1016/j.cose.2023.103397>
- Pierucci, F. (2025). Sovereignty in the Digital Era: Rethinking Territoriality and Governance in Cyberspace. *Digital Society*, 4, 27. <https://doi.org/10.1007/s44206-025-00189-4>
- Polido, F. B. P. (2024). Estado, soberania digital e tecnologias emergentes: Interações entre direito internacional, segurança cibernética e inteligência artificial. *Revista de Ciências do Estado*, 9(1), 1–30. <https://doi.org/10.35699/2525-8036.2024.53066>
- Sheikh, S. (2022). European digital sovereignty: A layered approach. *Digital Society*, 1(2). <https://doi.org/10.1007/s44206-022-00025-z>
- Silveira, S., & Xiong, Y. (2025). Índice de soberania digital: o caso do Brasil. Rio de Janeiro: FAPERJ. <https://doi.org/10.18617/liinc.v21i1.7451>
- Yalamancheli, H. (2025). Digital sovereignty meets agile delivery: Empowering governments to own their tech future. *Journal of Computer Science and Technology Studies*, 7(8), 1061–1068. <https://doi.org/10.32996/jcsts.2025.7.8.121>