

UNIVERSIDADE FEDERAL DE PERNAMBUCO
CENTRO DE FILOSOFIA E CIÊNCIAS HUMANAS
DEPARTAMENTO DE CIÊNCIA POLÍTICA

YURI SAGAN LUIZ GARCÊS

**REGULAÇÃO E CIBERSEGURANÇA: UMA REVISÃO
SISTEMÁTICA DA LITERATURA ACERCA DAS REGULAÇÕES
DO CIBERESPAÇO NA ÚLTIMA DÉCADA.**

Recife

2025

YURI SAGAN LUIZ GARCÊS

**REGULAÇÃO E CIBERSEGURANÇA: UMA REVISÃO SISTEMÁTICA DA
LITERATURA ACERCA DAS REGULAÇÕES DO CIBERESPAÇO NA
ÚLTIMA DÉCADA.**

Trabalho de conclusão de curso apresentado ao
Bacharelado em Ciência Política da Universidade
Federal de Pernambuco, como requisito parcial para
obtenção do título de Bacharel em Ciência Política.

Orientador: Prof. Dr. Marcos Aurelio Guedes de
Oliveira

Recife
2025

Ficha de identificação da obra elaborada pelo autor,
através do programa de geração automática do SIB/UFPE

Garcês, Yuri Sagan Luiz.

REGULAÇÃO E CIBERSEGURANÇA: UMA REVISÃO SISTEMÁTICA DA
LITERATURA ACERCA DAS REGULAÇÕES DO CIBERESPAÇO NA
ÚLTIMA DÉCADA. / Yuri Sagan Luiz Garcês. - Recife, 2025.

38 p. : il., tab.

Orientador(a): Marcos Aurélio Guedes de Oliveira

Trabalho de Conclusão de Curso (Graduação) - Universidade Federal de
Pernambuco, Centro de Filosofia e Ciências Humanas, Ciência Política, 2025.

Inclui referências, apêndices, anexos.

1. Ciberespaço. 2. Regulação. 3. Cibersegurança. 4. Governança da internet. 5.
Revisão da literatura . 6. Relações internacionais . I. Oliveira, Marcos Aurélio
Guedes de. (Orientação). II. Título.

320 CDD (22.ed.)

YURI SAGAN LUIZ GARCÊS

**REGULAÇÃO E CIBERSEGURANÇA: UMA REVISÃO SISTEMÁTICA DA
LITERATURA ACERCA DAS REGULAÇÕES DO CIBERESPAÇO NA ÚLTIMA
DÉCADA.**

Trabalho de conclusão de curso apresentado ao
Bacharelado em Ciência Política da
Universidade Federal de Pernambuco, como
requisito parcial para obtenção do título de
Bacharel em Ciência Política.

Aprovado em: 15/04/2025

BANCA EXAMINADORA

Prof. Dr. _____
(Orientador) Departamento de Ciência Política - UFPE

Prof. Dr. _____
(Examinador Interno) Departamento de Ciência Política - UFPE

(Examinador Interno)
Departamento de Ciência Política – UFPE

AGRADECIMENTOS

Primeiramente, agradeço à minha família, minha mãe, que ainda no início da minha vida, sempre me guiou a desenvolver o amor e o interesse aos estudos, pois com toda sua experiência, sabia da importância da educação na vida de todo ser humano. Minha avó, que sempre acreditou em mim, que eu alcançaria qualquer que fosse meu objetivo, que também me criou e me cercou de todo o amor, paciência, carinho e responsabilidade, para que eu viesse a me tornar um homem decente para ter uma boa vida.

Foram muitos anos de vida universitária, muito investimento físico, psicológico para ser resiliente diante das adversidades e financeiro para chegar até aqui. Muitas abdições foram feitas para que eu pudesse concluir minhas obrigações na vida, mas nada seria possível sem as amizades que eu fiz durante meu tempo na universidade. Cercado de seres humanos incríveis que sempre me impulsionaram a ser melhor, a me dedicar, que sempre acreditaram em mim e que tornaram minha passagem pela academia o mais saudável e leve que poderia ser, sempre estiveram ao meu lado e os levarei comigo por toda minha vida.

Sendo assim, agradeço à Esdras, Davi, Marcelo, Rickiã Rodrigues e Vinicius Cruz, menciono esses dois últimos com certa honraria, pois sendo exímios pesquisadores detentores de uma carreira brilhante na Ciência Política, me inspiraram e me ajudaram a concluir este trabalho com toda a paciência, aconselhamento e parceria que verdadeiros amigos poderiam ser.

Agradeço ao meu orientador Marcos Guedes, que se propôs a estar comigo e me orientar nessa reta final de curso. Por fim, agradeço a todos que passaram pela minha vida desde o início da minha vida acadêmica, pessoas de bem, que me fizeram ter forças para seguir em frente e a superar meus limites, bem como, aqueles que nunca enxergaram futuro em mim ou que me fizeram algum mal, pois cada uma dessas pessoas, se tornaram “combustíveis”, dando-me energia para ir além e a provar que eu poderia conseguir realizar todos os meus sonhos.

Deposite sua energia em si mesmo, nunca falhe em acreditar em si mesmo, não se justifique demais, nem se abale com elogios ou críticas, aqueles que te amam, não precisarão de explicações para estar ao seu lado e acreditar em você, mas aqueles que já lhe odeiam, de nada adiantarão seus esforços no fim.

RESUMO

Como tem se dado o debate da literatura acerca da regulação do ciberespaço da última década? A crescente dependência de infraestruturas digitais e a proliferação de ameaças cibernéticas, desde crimes digitais a ataques contra Estados e infraestruturas críticas, evidenciam a urgência de compreender os mecanismos de regulação neste ambiente. Este trabalho tem como objetivo mapear e sistematizar o debate na literatura acadêmica sobre a regulação do ciberespaço na última década (2015-2025). Para tal, realizou-se uma revisão sistemática da literatura, analisando 26 artigos científicos em português e inglês, coletados em bases como Google Scholar, SciELO e ProQuest, com auxílio dos softwares Harzing's Publish or Perish, Zotero, Microsoft Excel e Datawrapper. A análise dos dados codificados revela que a produção acadêmica se concentra nos temas de Relações Internacionais, Estudos de Segurança e Direito Internacional, com foco predominante nos atores estatais e na União Europeia. Os níveis de regulação mais abordados são o Internacional e o Nacional, seguidos pelo Regional (UE) e transnacional. A análise documental destaca-se como principal metodologia. Os resultados também apontam lacunas significativas, como a escassez de estudos focados em outras regiões (Mercosul, CPLP, África, América Latina) e em atores não-estatais. Conclui-se que, embora haja um crescente interesse acadêmico, o debate ainda é centrado em perspectivas tradicionais, havendo oportunidades para pesquisas futuras que explorem contextos geopolíticos e atores diversos, contribuindo para uma compreensão mais abrangente da governança global do ciberespaço.

Palavras-chave: ciberespaço; regulação; cibersegurança; governança da internet; revisão da literatura.

ABSTRACT

How has the literature debated the regulation of cyberspace over the past decade? The growing reliance on digital infrastructures and the proliferation of cyber threats, from digital crimes to attacks against states and critical infrastructures, highlight the urgency of understanding regulatory mechanisms in this environment. This study aims to map and systematize the academic literature debate on cyberspace regulation over the past decade (2015–2025). To this end, a systematic literature review was conducted, analyzing 26 scientific articles in Portuguese and English, collected from databases such as Google Scholar, SciELO, and ProQuest, with the aid of Harzing's Publish or Perish, Zotero, Microsoft Excel, and Datawrapper software. The analysis of the coded data reveals that academic production focuses on topics within International Relations, Security Studies, and International Law, with a predominant emphasis on state actors and the European Union. The most addressed regulatory levels are International and National, followed by Regional (EU) and Transnational. Document analysis stands out as the main methodology. The results also indicate significant gaps, such as the lack of studies focused on other regions (Mercosul, CPLP, Africa, Latin America) and non-state actors. It is concluded that, although academic interest is growing, the debate remains centered on traditional perspectives, leaving room for future research that explores diverse geopolitical contexts and actors, thus contributing to a more comprehensive understanding of global cyberspace governance.

Keywords: cyberspace. regulation; cybersecurity; internet governance; literature review.

LISTA DE ILUSTRAÇÕES

Gráfico 1 - Número de publicações por tipo de documento	22
Gráfico 2 - Número de publicações por escopo geográfico	22
Gráfico 3 - Número de publicações por anos	23
Gráfico 4 – Temas mais frequentes	24
Gráfico 5 - Tipos de metodologias utilizadas	26
Gráfico 6 - Nível de regulação	31

LISTA DE TABELAS

Tabela 1 – Setores e atores mais envolvidos na literatura	25
Tabela 2 - Impactos das áreas temáticas e relevância dos autores em determinados estudos	27
Tabela 3 - Gaps e Oportunidades de Pesquisa	30

LISTA DE QUADROS

Quadro 1 - Descrição metodológica	17
Quadro 2 Critérios de Seleção para Revisão Sistemática	19
Quadro 3 – Dimensão e descrição das variáveis	20

SUMÁRIO

1. INTRODUÇÃO	11
2. REVISÃO DA LITERATURA	13
2.1 Cibersegurança nas Relações Internacionais	13
2.2 Regulação do Ciberespaço e Governança Global	15
2.3 Ciberespaço e Dinâmicas Internacionais: Conflito, Cooperação e Diplomacia	16
3. METODOLOGIA	17
3.1 Coleta e Critérios de seleção	19
4. RESULTADOS	22
4.1 Número de publicações por tipo de documento	22
4.2 Número de publicações por escopo geográfico	22
4.3 Número de publicações por ano	23
4.4 Temas mais frequentes	24
4.5 Setores e atores mais envolvidos na literatura	25
4.6 Tipos de metodologias utilizadas	26
4.7 Impactos das áreas e relevância dos autores em determinados estudos	27
4.8 Gaps e Oportunidades de Pesquisa	30
4.9 Nível de regulação	31
5. Limitações	31
6. CONCLUSÃO	32
7. REFERÊNCIAS	35

1. INTRODUÇÃO

Com a crescente digitalização de serviços públicos, infraestruturas críticas e interações sociais, os Estados se tornaram mais dependentes e, consequentemente, mais vulneráveis a ameaças cibernéticas. Esses riscos variam desde crimes digitais e vazamento de dados até ataques coordenados capazes de paralisar hospitais, bancos ou redes elétricas. Por isso, o ciberespaço deixou de ser apenas uma rede de informação para se tornar um novo domínio estratégico, com implicações diretas na segurança e na geopolítica internacional (CAVELTY, 2022).

Nas Relações Internacionais, os temas da cibersegurança e da regulação do ciberespaço ganharam relevância justamente por revelarem uma nova dimensão de poder, conflito e cooperação. Hoje, ataques cibernéticos podem ser utilizados por governos e grupos como instrumentos de espionagem, sabotagem, manipulação de informação e influência política. Esse cenário levanta questões fundamentais sobre responsabilidade internacional, direito, diplomacia e os limites da soberania num espaço que, por natureza, não reconhece fronteiras fixas (VALERIANO; MANESS, 2015; RIORDAN, 2019).

Um dos principais desafios está na ausência de uma estrutura jurídica internacional sólida e amplamente aceita que regule o comportamento dos atores nesse ambiente. O ataque cibernético sofrido pela Estônia em 2007¹, por exemplo — considerado o primeiro grande ataque virtual contra um Estado —, mostrou como o sistema internacional ainda estava (e, em muitos sentidos, continua) despreparado para lidar com esse tipo de ameaça.

Outros episódios, como a invasão da Sony Pictures atribuída à Coreia do Norte (2014), os ciberataques à infraestrutura da Ucrânia por meio do malware NotPetya (2017)² e as interferências digitais nas eleições dos EUA em 2016, evidenciam a complexidade crescente dos conflitos cibernéticos (NYE, 2010; KITTICHAISAREE, 2017).

No entanto, os problemas não se limitam à segurança. O ciberespaço também levanta debates urgentes sobre privacidade, proteção de dados, liberdade de expressão e o papel das grandes empresas de tecnologia. Iniciativas como o Regulamento Geral de Proteção de Dados

¹ O ataque foi realizado após tensões políticas com a Rússia e envolveu o uso de botnets para derrubar sites governamentais, bancários e de comunicação estonianos.

² O NotPetya foi um malware inicialmente disfarçado de ransomware, mas projetado para destruir dados e paralisar sistemas, com impactos globais em empresas como Maersk e Merck.

da União Europeia (GDPR) e a Lei Geral de Proteção de Dados brasileira (LGPD)³ representam tentativas de estabelecer limites e garantias mínimas para os usuários, ao mesmo tempo que impõem responsabilidades às plataformas e empresas que operam no ambiente digital (GREENLEAF, 2018).

Em razão de compreender como anda a literatura acerca do debate sobre as regulações do ciberespaço, este trabalho objetiva-se responder a pergunta: Como tem se dado o debate da literatura acerca da regulação do ciberespaço na última década?

O objetivo deste trabalho é relatar e sistematizar a literatura acerca do debate regulatório do ciberespaço. Codificando os dados encontrados e gerar uma análise sistematizada do estado da literatura acerca do tema. Sendo assim, foi realizada uma revisão sistemática de 26 artigos em grande parte, artigos em português e inglês publicadas entre 2015 e 2025. Foi utilizado os softwares *Harzing's Publish or Perish 8.8*, *Zotero* e *Microsoft Office Excel* e bem como, o software *Datawrapper* para coleta, filtragem dos artigos através das palavras-chave, e para produção dos gráficos, respectivamente. Além disso, uma pesquisa personalizada e individual em outros repositórios e base de dados objetivando abranger ainda mais as fontes para além do tradicional *Google Scholar*.

Ainda, foi feita uma adaptação os critérios de seleção dos manuais de revisão sistemática da literatura como Papaioannou et al, (2016) e também Petticrew and Roberts, (2006)⁴ tendo em vista que os manuais mencionados são de cunha geral, adequando a esta revisão sistemática da literatura com categorias elaboradas pela leitura exploratória dos artigos coletados.

A estrutura deste trabalho está dividida em cinco seções. A primeira delas é a introdução, responsável por situar o tema e apresentar os objetivos da pesquisa. Em seguida, a segunda parte traz a revisão da literatura, com foco nas principais discussões teóricas e estudos já realizados sobre o assunto. A terceira seção trata da metodologia, explicando o processo utilizado na condução da revisão sistemática. A quarta parte apresenta os resultados, com base na análise das variáveis levantadas. Por fim, a quinta e última seção reúne as considerações finais, nas quais são discutidas as interpretações dos dados e as contribuições da pesquisa, além de suas limitações.

³ O GDPR foi aprovado em 2016 e entrou em vigor em 2018 na União Europeia. A LGPD, baseada parcialmente no modelo europeu, foi sancionada em 2018 no Brasil e passou a valer em 2020.

⁴ Ambos os manuais são amplamente utilizados para construção de revisões sistemáticas na área de Ciências Sociais Aplicadas, ainda que não se restrinjam a essa disciplina.

2. REVISÃO DA LITERATURA

2.1 Cibersegurança nas Relações Internacionais

A cibersegurança vem como um dos principais temas na agenda internacional contemporânea, refletindo o impacto crescente da tecnologia da informação sobre a segurança dos Estados, corporações e cidadãos. No âmbito das Relações Internacionais, o conceito de cibersegurança não se restringe apenas à proteção de sistemas informáticos e dados, mas também, para uma arena geopolítica onde a informação, a comunicação e a soberania digital passam a ter papel estratégico (VALERIANO; MANESS, 2015)⁵.

A definição de cibersegurança compreende um conjunto de práticas, tecnologias e políticas destinadas a proteger redes, sistemas e informações contra acessos não autorizados, ataques cibernéticos, danos ou desastres. Esse conceito está intrinsecamente ligado à ideia de "poder cibernético"⁶, isto é, a capacidade de um ator (estatal ou não estatal) de exercer influência ou coerção através de meios digitais (VALERIANO; MANESS, 2015).

Segundo Dunn Cavelty (2022)⁷, a cibersegurança deve ser entendida como um fenômeno político, permeado por transformações sócio-técnicas e fragmentação de atores. A autora destaca que, mais do que uma questão meramente técnica, a cibersegurança reflete disputas por narrativas, prioridades e formas de regulação em um ambiente global interconectado.

No campo teórico, a Escola de Copenhague⁸ trouxe uma valiosa contribuição ao ampliar o escopo da segurança internacional para além das ameaças militares tradicionais. Ao propor uma abordagem multissetorial, ela identifica cinco setores principais que podem ser objetos de securitização: militar, político, econômico, social e ambiental (DUQUE, 2009). Essa ampliação do olhar permite considerar que ameaças à segurança podem surgir em diferentes dimensões da

⁵ Brandon Valeriano e Ryan C. Maness são pesquisadores reconhecidos na área de ciberconflitos e desenvolveram o conceito de “coerção cibernética” em sua obra “Cyber War versus Cyber Realities: Cyber Conflict in the International System” (2015).

⁶ Entende-se por “poder cibernético” a habilidade de um ator influenciar o comportamento de outros no ciberespaço por meio de capacidades digitais, como espionagem, sabotagem ou disseminação de informação.

⁷ Referência à obra “Cyber-Security Politics: Socio-Technological Transformations and Political Fragmentation” de Myriam Dunn Cavelty.

⁸ A Escola de Copenhague foi desenvolvida por Barry Buzan, Ole Wæver e Jaap de Wilde, e é conhecida por seu enfoque na construção social da segurança.

vida contemporânea. O ciberespaço, por sua natureza transversal e dinamicidade, desafiou até mesmo essa estrutura ampliada.

Hansen e Nissenbaum (2009)⁹, ao reconhecerem essas especificidades, sugeriram a criação de um sexto setor de análise, o setor cibernético, que contemplaria a complexidade e as particularidades dos riscos e vulnerabilidades digitais. Sua proposta expande a teoria da securitização ao reconhecer o ciberespaço como um domínio em que ameaças reais e percebidas afetam diretamente infraestruturas críticas e, por consequência, a segurança nacional.

Portanto, as infra estruturas que sustentam a sociedade contemporânea como energia, comunicações, transportes, bancos e saúde são hoje altamente dependentes de sistemas digitais¹⁰. Qualquer falha ou ataque direcionado a essas estruturas pode desencadear consequências em cadeia, afetando diversas áreas da vida pública e institucional. Diante disso, a segurança cibernética tornou-se um componente essencial da segurança internacional, sendo incorporada de forma crescente às agendas governamentais e aos organismos multilaterais (LOPES, 2016)¹¹.

A cibersegurança, nesse contexto, pode ser entendida como o conjunto de ações e estratégias voltadas à prevenção, proteção e resposta a ameaças no ambiente digital. A União Internacional das Telecomunicações (UIT)¹² define cibersegurança como um conjunto integrado de políticas, procedimentos, capacitações, ferramentas e tecnologias projetadas para salvaguardar ativos e usuários no espaço virtual (UIT, 2008). Essa definição reconhece tanto a dimensão técnica quanto a organizacional e política do fenômeno.

As principais ameaças à segurança cibernética incluem ataques de malware, ransomware, negação de serviço (DDoS), espionagem digital, terrorismo cibernético e guerra cibernética.¹³ Esses fenômenos têm provocado reações estatais como o fortalecimento de

⁹ Hansen e Nissenbaum, em sua proposta, expandem a teoria da securitização da Escola de Copenhague, argumentando que o ciberespaço possui especificidades que o tornam um setor próprio de análise em segurança internacional.

¹⁰ Infraestruturas críticas referem-se a sistemas essenciais cujo funcionamento contínuo é vital para a segurança nacional, saúde pública, segurança econômica ou a ordem pública de um Estado.

¹¹ Lopes (2016) discute como a segurança cibernética foi incorporada a estratégias de defesa nacionais e à atuação internacional de instituições como a ONU, OTAN e OEA.

¹² A definição da UIT consta no relatório “Global Cybersecurity Agenda”, publicado em 2008, e é um dos marcos conceituais para discussões sobre segurança cibernética em fóruns multilaterais.

¹³ Esses termos referem-se a diferentes formas de ataque digital. Por exemplo, DDoS (Distributed Denial of Service) visa indisponibilizar serviços online ao sobrecarregar seus servidores.

capacidades militares no ciberespaço, a criação de doutrinas de defesa cibernética e o investimento em diplomacia especializada (CAVELTY, 2022; VALERIANO; MANESS, 2015; NYE, 2010).

2.2 Regulação do Ciberespaço e Governança Global

Embora frequentemente se associe o ciberespaço a uma realidade puramente virtual, é importante destacar que esse ambiente digital também depende de uma complexa infraestrutura física. Isso inclui servidores, cabos submarinos, satélites e dispositivos conectados, todos interligados por redes de comunicação altamente especializadas. Portanto, o ciberespaço pode ser compreendido não apenas como um domínio abstrato de circulação de dados, mas como uma esfera sociotécnica que articula pessoas, instituições, tecnologias e informações em uma teia global (Mandarino Júnior, 2011)¹⁴.

Ainda do ponto de vista teórico, o conceito moderno de ciberespaço encontra raízes nas formulações de Pierre Lévy (1999)¹⁵, que o descreve como um novo campo de experiências humanas mediadas por tecnologias digitais. Para além do ambiente informacional, ele envolve também práticas sociais e políticas, o que o torna uma arena cada vez mais relevante para os estudos de governança, soberania e cooperação internacional.

Com o avanço da digitalização, a regulação do ciberespaço tornou-se uma prioridade para os Estados e organismos internacionais. A ausência de fronteiras físicas e a natureza descentralizada da internet impuseram desafios significativos ao direito internacional, especialmente quanto à soberania, à jurisdição e à aplicação de sanções (KITICHASAREE, 2017)¹⁶. Kriangsak Kittichaisaree argumenta que a aplicação do direito internacional ao ciberespaço é uma necessidade urgente, mas enfrenta dificuldades práticas quanto à atribuição de responsabilidade por ataques, à definição de limites da soberania digital e à criação de normas universais (KITICHASAREE, 2017; SCHMIDT; COHEN, 2013).

Outro aspecto relevante da regulação é a governança da internet, um processo multissetorial que envolve entidades como a ICANN (Internet Corporation for Assigned Names

¹⁴ Mandarino Júnior defende que o ciberespaço deve ser analisado sob uma perspectiva sociotécnica, reconhecendo a interdependência entre estruturas técnicas e dinâmicas sociais no ambiente digital.

¹⁵ Pierre Lévy foi um dos primeiros pensadores a teorizar o ciberespaço como um novo estágio da inteligência coletiva, mediado por tecnologias da informação e da comunicação.

¹⁶ Kittichaisaree ressalta que a soberania digital é uma extensão da soberania tradicional dos Estados, exigindo adaptações no arcabouço jurídico internacional vigente.

and Numbers)¹⁷, a ITU (International Telecommunication Union) e o Fórum de Governança da Internet (IGF/ONU)¹⁸. Essas organizações tentam articular um modelo de governança que equilibre interesses estatais, empresariais e da sociedade civil (SHANY; MIMRAN, 2021; DE NARDIS, 2014).

A regulação da privacidade e dos dados pessoais é outro pilar importante, representado por legislações como o GDPR europeu e a LGPD brasileira. Essas normas estabelecem parâmetros para a coleta, o armazenamento e o uso de dados por empresas e governos, gerando repercussões jurídicas e diplomáticas significativas (KITICHASAREE, 2017; GREENLEAF, 2018)¹⁹.

2.3 Ciberespaço e Dinâmicas Internacionais: Conflito, Cooperação e Diplomacia

O ciberespaço tornou-se um novo domínio das relações internacionais, onde se desenvolvem tanto conflitos como mecanismos de cooperação. A dificuldade em atribuir a responsabilidade por ataques cibernéticos complica a aplicação do direito internacional humanitário e torna nebulosa a definição de ato de guerra (SHANY; MIMRAN, 2021)²⁰.

Riordan (2019) destaca o papel crescente da diplomacia cibernética²¹, definida como o uso de ferramentas diplomáticas para lidar com questões relacionadas à segurança cibernética, regulação da internet e proteção de direitos no ambiente digital. Ele argumenta que é essencial combinar habilidades diplomáticas tradicionais com o conhecimento técnico para desenvolver uma governança eficaz do ciberespaço. O Council on Foreign Relations (2021)²² salienta a urgência da cooperação internacional para estabelecer normas e protocolos²³ que evitem escaladas de tensão e promovam a estabilidade digital global. Iniciativas como o Grupo de

¹⁷ A ICANN é responsável pela coordenação global do sistema de nomes de domínio da internet (DNS), tendo papel central na governança técnica da rede.

¹⁸ A ITU é uma agência especializada da ONU voltada à padronização global das telecomunicações; o IGF, por sua vez, é um espaço de diálogo multissetorial sobre políticas públicas da internet, criado na Cúpula Mundial da Sociedade da Informação.

¹⁹ Além dos efeitos internos, legislações como o GDPR e a LGPD geram fricções diplomáticas com países cujas leis de privacidade são menos rígidas, influenciando negociações comerciais e acordos internacionais de transferência de dados.

²⁰ A dificuldade em identificar os autores de um ataque cibernético, o chamado “problema da atribuição”, é um dos maiores obstáculos para enquadrar essas ações como atos de guerra nos moldes da Convenção de Genebra.

²¹ Diplomacia cibernética envolve a negociação de normas, tratados e práticas comuns entre Estados e outros atores internacionais com vistas à estabilidade digital e à proteção de direitos no ciberespaço.

²² O Council on Foreign Relations (CFR) é um think tank norte-americano de relevância global que publica análises sobre segurança internacional, incluindo os desafios do ciberespaço.

²³ No âmbito da governança cibernética, há uma predominância de “soft law” (diretrizes não vinculativas) em comparação com normas de “hard law”, dada a ausência de consenso sobre obrigações legais universais.

Peritos Governamentais da ONU (GGE/UN)²⁴ e o Open-Ended Working Group (OEWG/UN) representam esforços multilaterais nesse sentido.

3. METODOLOGIA

A metodologia usada nesta pesquisa seguiu as orientações de Petticrew e Roberts (2006) e Papaioannou et al. (2016) para revisões sistemáticas. As etapas de busca e seleção, definidas com antecedência, estão organizadas nos Quadross 1 e 2. Também foram usados modelos parecidos com os de Silva (2018) e Rodrigues (2023). A Tabela 1 mostra como o método foi estruturado.

Quadro 1 - Descrição metodológica

Pergunta de Pesquisa	Como tem se dado o debate da literatura acerca da regulação do ciberespaço na última década?
Objetivo	Este trabalho realiza uma revisão sistemática por meio de análises qualitativas e quantitativas, utilizando gráficos e tabelas para sintetizar tendências, padrões e lacunas na produção científica sobre o tem
Unidade de Análise	Artigos científicos relacionados à cibersegurança, mais especificamente a área de regulação do ciberespaço.
Delimitação Temporal	2015 - 2025
Técnica	Estatística Descritiva
Fontes	<i>Google Scholar; SCielo; ProQuest</i>
Softwares	<i>Microsoft Office; Harzing's Publish or Perish 8.8; Zotero; Datawrapper e Apple Notes</i>
Repositório de Dados	<i>Open Science Framework (OSF) - https://osf.io/cwnyp/</i>

Fonte: Elaboração própria usando o modelo de Rodrigues (2023)

Como dito na Tabela 1, esse trabalho se propõe a elaborar uma revisão sistemática e será conduzida com base em uma abordagem rigorosa para identificar, selecionar e analisar

²⁴ O GGE da ONU é um grupo limitado a especialistas estatais convidados, enquanto o OEWG permite participação aberta de todos os Estados-membros da ONU, promovendo maior transparência e inclusão.

publicações com relevantes debates sobre a regulação da cibersegurança na promoção do ambiente seguro das relações internacionais.

Iniciou-se com a definição de cibersegurança no contexto internacional, logo em seguida, é discutido sobre o entendimento dos principais autores da literatura no campo e finalmente, utilizando-se das pesquisas científica ao longo da última década, pôde-se extrair respostas para além da pergunta chave, mas através de sua resposta, análises qualitativas e quantitativas de como anda o campo da cibersegurança e sua literatura voltada à sua regulação.

Os dados extraídos dos artigos foram organizados em uma tabela contendo informações como título, autores, ano de publicação, objetivos do estudo, principais achados, observações gerais, entre outras variáveis. Além disso, foram elaboradas tabelas, e gráficos para melhor visualização e entendimento dos resultados. Por fim, uma conclusão com um resumo dos principais achados da revisão sistemática e quais as implicações políticas e estratégicas das regulações do ciberespaço no cenário internacional.

A presente análise foi desenvolvida a partir de uma abordagem mista, combinando métodos qualitativos e quantitativos²⁵, com o objetivo de identificar padrões, tendências recorrentes e lacunas na produção científica sobre o tema. A seleção de publicações foi realizada por meio de buscas em bases de dados acadêmicas amplamente reconhecidas, como *Google Scholar* e *SciELO*.²⁶

A coleta dos dados bibliográficos foi conduzida inicialmente utilizando o software *Harzing's Publish or Perish* (versão 8.8)²⁷, logo após migrada para o *Zotero*²⁸, com uma estratégia de busca ajustada para contornar as limitações da ferramenta. Após a extração, as referências foram organizadas e tabuladas com o uso do gerenciador *Zotero*, sendo posteriormente analisadas no *Microsoft Excel*²⁹.

As variáveis utilizadas na codificação dos dados foram estabelecidas previamente, ainda na etapa de leitura exploratória, seguindo os procedimentos metodológicos sugeridos por

²⁵ Uma abordagem metodológica mista é apropriada para revisões sistemáticas quando se deseja captar tanto padrões numéricos recorrentes quanto interpretações contextuais mais profundas dos estudos analisados.

²⁶ O Google Scholar é uma ferramenta de busca multidisciplinar de literatura acadêmica, enquanto a SciELO é uma biblioteca eletrônica com foco em periódicos científicos da América Latina e Caribe.

²⁷ O software Publish or Perish permite a recuperação e análise de citações acadêmicas com base em diferentes bases de dados, sendo amplamente utilizado para levantamento bibliográfico e análises métricas de produção científica.

²⁸ O Zotero é um gerenciador de referências bibliográficas gratuito que permite a organização, marcação e exportação de dados de forma automatizada e colaborativa.

²⁹ O Microsoft Excel, embora não seja um software específico para análise científica, permite a tabulação de dados e geração de gráficos simples, sendo uma ferramenta útil na análise preliminar de revisões sistemáticas.

Petticrew e Roberts (2006), Papaioannou et al. (2016) e Sampaio e Lycarião (2023)³⁰. A análise buscou manter coerência com os princípios das revisões sistemáticas, com foco na consistência dos critérios de inclusão e categorização.

O Quadro 2 resumirá e especificará os critérios de seleção.

3.1 Coleta e Critérios de seleção

Quadro 2 - Critérios de Seleção para Revisão Sistemática

Critérios	Descrição
Palavras-Chave	Regulação do ciberespaço; cibersegurança; governança cibernética; revisão da literatura
Ferramenta de Pesquisa	<i>Harzing's Publish or Perish 8.8; Zotero;</i>
Trabalhos Excluídos	Artigos focados exclusivamente em aspectos técnicos da cibersegurança relativos às empresas privadas (ex.: criptografia, protocolos de rede). Estudos com escopo muito restrito, ou massivos a ponto de extrapolar a conexão direta com política externa, cibersegurança, ciberespaço, geopolítica, Relações Internacionais e similares. Publicações de fontes não verificáveis (blogs, opiniões pessoais, notícias sem embasamento acadêmico). Trabalhos duplicados ou que não apresentem contribuição original para o tema. Trabalhos com erro na leitura do arquivo. Dissertações, Teses, Monografias, Livros, Resenhas e Trabalhos em idiomas que não o inglês e português.
Critérios de Inclusão	Publicações entre 2015-2025. Estudos que tratam de regulação do ciberespaço, cibersegurança, governança cibernética e Relações Internacionais. Publicações em inglês e português. Relatórios e documentos de organizações internacionais (ONU, OTAN, CSIS, etc.) se achados..
Plataforma de Busca de artigos	<i>Google Scholar; SciELO; ProQuest</i>
Idiomas	Português e Inglês

Fonte: Elaboração Própria usando o modelo de Rodrigues (2023)

Após a definição dos critérios de inclusão e exclusão, foi realizada a etapa de busca dos materiais por meio dos softwares Harzing's Publish or Perish e Zotero, com o uso de palavras-

³⁰ Esses autores oferecem manuais metodológicos amplamente aceitos para a condução de revisões sistemáticas nas ciências sociais, abordando desde critérios de inclusão até técnicas de síntese de resultados.

chave específicas e a aplicação de filtros avançados nas bases de dados Google Scholar e SciELO. Essa etapa inicial resultou em pouco mais de 80 publicações relevantes para o tema proposto.

Na sequência, os artigos foram submetidos a uma triagem em duas etapas, conforme sugerido por Petticrew e Roberts (2006) e Papaioannou et al. (2016)³¹. A primeira etapa consistiu na leitura dos títulos e resumos, permitindo uma filtragem preliminar com base nos objetivos da pesquisa. Já a segunda fase envolveu a leitura integral dos textos previamente selecionados, a fim de verificar de forma mais criteriosa a aderência ao escopo da investigação.

Os documentos que passaram por essa análise mais aprofundada foram classificados no Zotero, sendo marcados como “sim” ou “não”, de acordo com sua pertinência à temática. Para os que foram excluídos, foram adicionadas notas explicativas, justificando a não inclusão. Ao final dessa etapa, 56 artigos foram descartados por não se alinharem aos critérios da pesquisa, restando 26 trabalhos considerados adequados para a fase de codificação e análise.

Na etapa de coleta e organização dos dados desses 26 artigos, foram utilizadas variáveis desenvolvidas com base nos objetivos da pesquisa, com o intuito de realizar uma análise de conteúdo que permita mapear, de forma abrangente, o estado atual da literatura acadêmica sobre a regulação do ciberespaço nas Relações Internacionais. Por fim, utilizou-se o software *Datawrapper*³² para a elaboração nos gráficos e tabelas para melhor visualização e interpretação.

O Quadro 3 especifica as dimensões, as variáveis e as suas respectivas descrições. Vale mencionar que nem todas as variáveis foram utilizadas na pesquisa para elaborar outros tipos de análises, devido a urgência da conclusão do trabalho, mas que podem ser utilizadas para futuras pesquisas acessando o repositório Open Science Framework (OSF)³³ descrito na Tabela 1 sobre a descrição metodológica.

Quadro 3 – Dimensão e descrição das variáveis

Dimensão	Variável	Descrição
----------	----------	-----------

³¹ A triagem em duas etapas é uma técnica padrão em revisões sistemáticas, que visa garantir maior confiabilidade na seleção dos estudos, reduzindo viés de escolha.

³² O Datawrapper é uma ferramenta online voltada para a visualização de dados, amplamente utilizada em projetos de pesquisa e jornalismo de dados por sua interface intuitiva e resultados gráficos interativos.

³³ O OSF (Open Science Framework) é uma plataforma de ciência aberta que permite o compartilhamento de dados, códigos, pré-registros e resultados de pesquisa de forma transparente e acessível.

Formal	ID	Código identificador do artigo na planilha, utilizado para organização.
Formal	Título do Artigo	Nome completo da publicação analisada.
Formal	Autor(es)	Nome(s) do(s) autor(es) responsável(is) pelo texto.
Formal	Ano de Publicação	Ano em que o artigo foi publicado.
Formal	Revista / Fonte	Periódico, plataforma ou veículo acadêmico de publicação.
Formal	Tipo de Publicação	Classificação do material (artigo, capítulo, dissertação, etc.).
Formal	Afiliação Institucional	Instituição à qual o(s) autor(es) está(ão) vinculado(s).
Metodológica	Objetivo Claro?	Indica se os objetivos da pesquisa estão definidos com clareza.
Metodológica	Fundamentação Teórica Relevante?	Verifica se há uma base teórica sólida e pertinente ao tema.
Metodológica	Metodologia Adequada?	Avalia se a metodologia está alinhada aos objetivos propostos.
Metodológica	Apresenta Casos Reais?	Informa se há uso de estudos de caso ou exemplos empíricos.
Substantiva	Enfoque Principal	Tema central abordado no artigo (regulação, segurança, etc.).
Substantiva	Perspectiva Teórica	Enfoque teórico adotado (realismo, liberalismo, etc.).
Substantiva	Escopo Geográfico	Abrangência territorial da análise (nacional, regional, global).
Substantiva	Ator Focal	Principal agente analisado (Estado, empresa, organização internacional).
Substantiva	Dimensão de Segurança	Tipo de segurança discutido (nacional, cibernética, humana, etc.).
Substantiva	Mecanismos Regulatórios	Políticas, normas ou instrumentos regulatórios estudados.
Substantiva	Nível de Regulação	Nível em que se dá a regulação (local, nacional, internacional).
Substantiva	Desafios Apontados	Dificuldades ou problemas identificados no campo da regulação.
Substantiva	Tecnologias Discutidas	Tecnologias abordadas no texto (IA, big data, etc.).
Complementar	Contribuição para RI/Ciberespaço	Relevância da contribuição para os estudos em RI e ciberespaço.

Complementar	Observações Gerais	Comentários livres sobre limitações, observações ou dados relevantes.
--------------	--------------------	---

Fonte: Elaboração própria do autor (2025)

4. RESULTADOS

Gráfico 1 - Número de publicações por tipo de documento

Distribuição entre dissertações, artigos científicos, capítulos de livro etc.

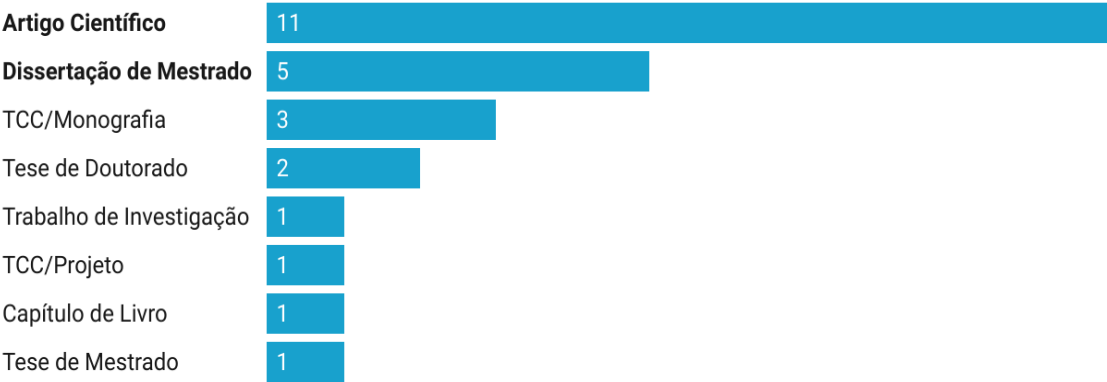


Gráfico: Criando pelo autor • Fonte: Elaboração própria (2025) • Criado com Datawrapper

Fonte: Elaboração própria do autor (2025)

No gráfico 1, a produção acadêmica está mais concentrada em Artigos Científicos, seguidos por Dissertações de Mestrado. Isso sugere que a pesquisa na área é frequentemente divulgada em periódicos científicos e também em trabalhos de pós-graduação.

Gráfico 2 - Número de publicações por escopo geográfico

Distribuição geográfica dos assuntos mais e menos abordados nos artigos.

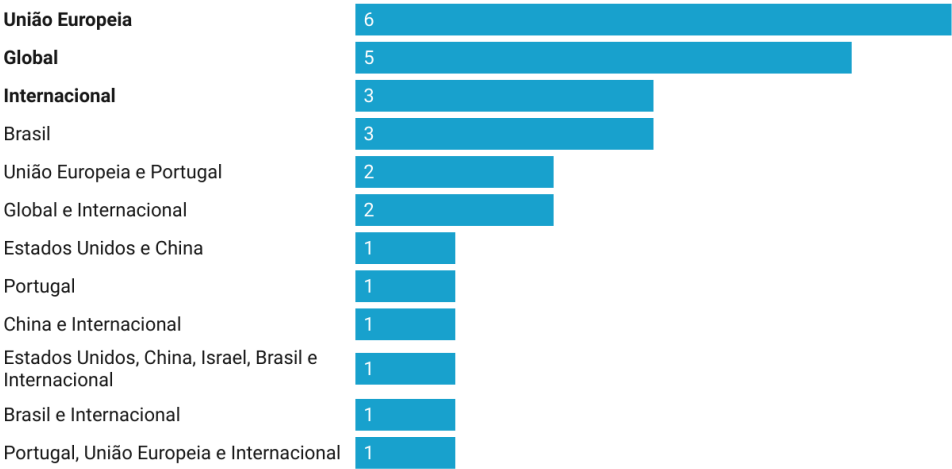


Gráfico: Criando pelo autor • Fonte: Elaboração própria (2025) • Criado com Datawrapper

Fonte: Elaboração própria do autor (2025)

No gráfico 2 a produção tem um foco significativo na União Europeia e em estudos de escopo Global / Internacional. O Brasil também aparece com alguma frequência. Isso indica que a pesquisa pode estar voltada para questões regionais europeias, para o cenário global da cibersegurança e também para o contexto brasileiro.

Gráfico 3 – Número de publicações por ano



Gráfico: Criando pelo autor • Fonte: Elaboração própria (2025) • Criado com Datawrapper

Fonte: Elaboração própria do autor (2025)

Observa-se no gráfico 3 um aumento significativo na produção acadêmica sobre cibersegurança e regulação do ciberespaço nos últimos anos, especialmente após eventos como o ataque NotPetya (2017) e a guerra na Ucrânia (2022)³⁴. Esses marcos reforçaram a centralidade do ciberespaço nas Relações Internacionais, impulsionando discussões sobre segurança digital, soberania e governança multilateral (DEIBERT, 2021).

³⁴ O conflito russo-ucraniano evidenciou o uso coordenado de operações cibernéticas como instrumentos de guerra híbrida, com ataques a sistemas de energia, bancos e canais de informação (Deibert, 2021).

Gráfico 4 - Temas mais frequentes

Categorias de temas mais recorrentes na literatura

- Relações Internacionais (teoria, poder, soberania)
- Estudos de Segurança / Estratégicos / Ciberdefesa
- Direito Internacional / Direito da UE / Direito Digital
- Governança Global / Governança da Internet
- Ciência Política / Integração Europeia / Diplomacia
- Regulação / Jurisdição / Modelos Comparativos
- Outros

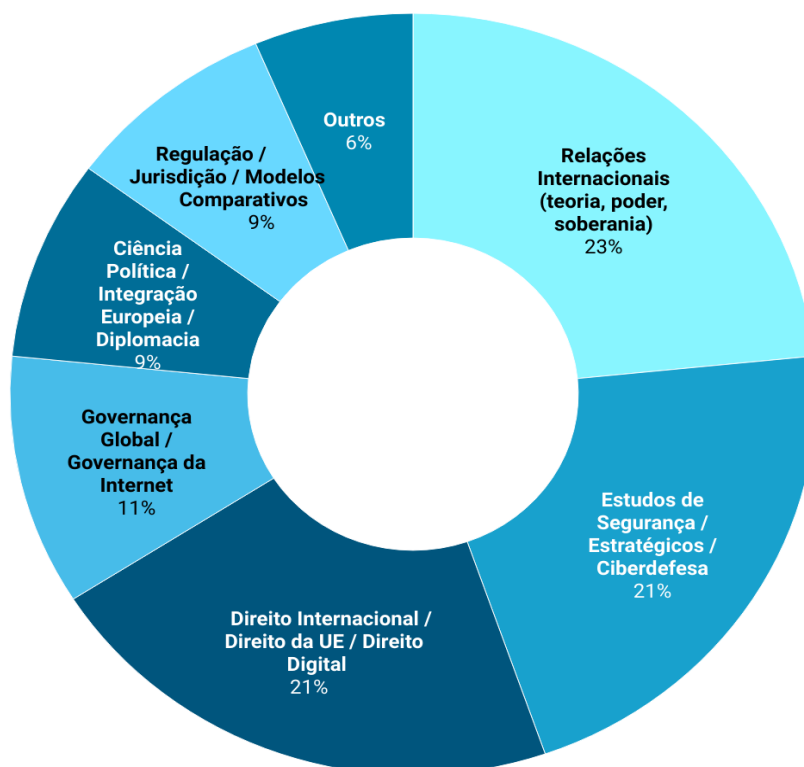


Gráfico: Criando pelo autor • Fonte: Elaboração própria (2025) • Criado com Datawrapper

Fonte: Elaboração própria do autor (2025)

A literatura sobre o ciberespaço e sua regulação tem se concentrado, principalmente, em três grandes áreas: Relações Internacionais, Estudos de Segurança e Direito Internacional. Essas abordagens refletem preocupações com soberania, poder, cibersegurança e a criação de normas jurídicas no ambiente digital. Além disso, temas como governança global, regulação comparada e disputas por modelos de controle também aparecem com frequência. Embora existam contribuições de áreas como Filosofia da Tecnologia, Sociologia e Gestão da Informação, elas ainda são menos recorrentes.

Tabela 1 – Setores e atores mais envolvidos na literatura

Classificação dos principais atores envolvidos e suas categorias

Ator	Aparece quantas vezes com foco nas publicações?	Categoria
Estados Nacionais	16	Governamental
União Europeia	12	Governamental / Regional
Organizações Internacionais (ONU, OCDE, OTAN, IGF, etc.)	9	Internacional / Governança Global
Atores Não-Estatais (ONGs, Hackers, Comunidade técnica, etc.)	7	Civil / Técnico
Instituições Legislativas/Regulatórias	5	Governamental / Regulação
Plataformas Digitais (Meta, TikTok)	2	Privado
Forças Armadas / Ciberdefesa	2	Militar
Indivíduos / Cidadãos	3	Civil
Acadêmicos / Teóricos	2	Civil / Acadêmico
Brasil (como caso nacional)	4	Governamental / Nacional

Tabela: Criando pelo autor. • Fonte: Elaboração própria (2025) • Criado com Datawrapper

Fonte: Elaboração própria do autor (2025)

A análise dos estudos revela que os Estados nacionais e a União Europeia são os atores mais recorrentes nas discussões sobre regulação do ciberespaço, demonstrando um foco claro nas estruturas de poder tradicional e na formulação de políticas públicas. As organizações internacionais também ocupam espaço relevante, especialmente no que diz respeito à coordenação normativa e à governança multilateral da internet.

Além disso, apesar de seu peso real na dinâmica do ciberespaço, o setor privado, representado por grandes plataformas digitais como Meta e TikTok, aparece com menos frequência nas análises³⁵. Já o setor militar, embora presente, tende a ser tratado de forma mais específica, ligado à doutrina estratégica e aos conflitos cibernéticos. Ainda assim, há um número considerável de trabalhos que destacam a atuação de atores não-estatais e da sociedade civil, o que indica uma preocupação crescente com os aspectos participativos e democráticos da regulação digital.

³⁵ Para uma análise do poder estrutural das plataformas digitais, cf. CULPEPER, Roy; CLARKSON, Stephen. "The Rise of the Corporate Digital State". *Global Policy*, 2017.

Gráfico 5 - Tipos de metodologias utilizadas

Quais métodos são mais aplicados (análise documental, entrevistas, estudos de caso, revisões, etc.)

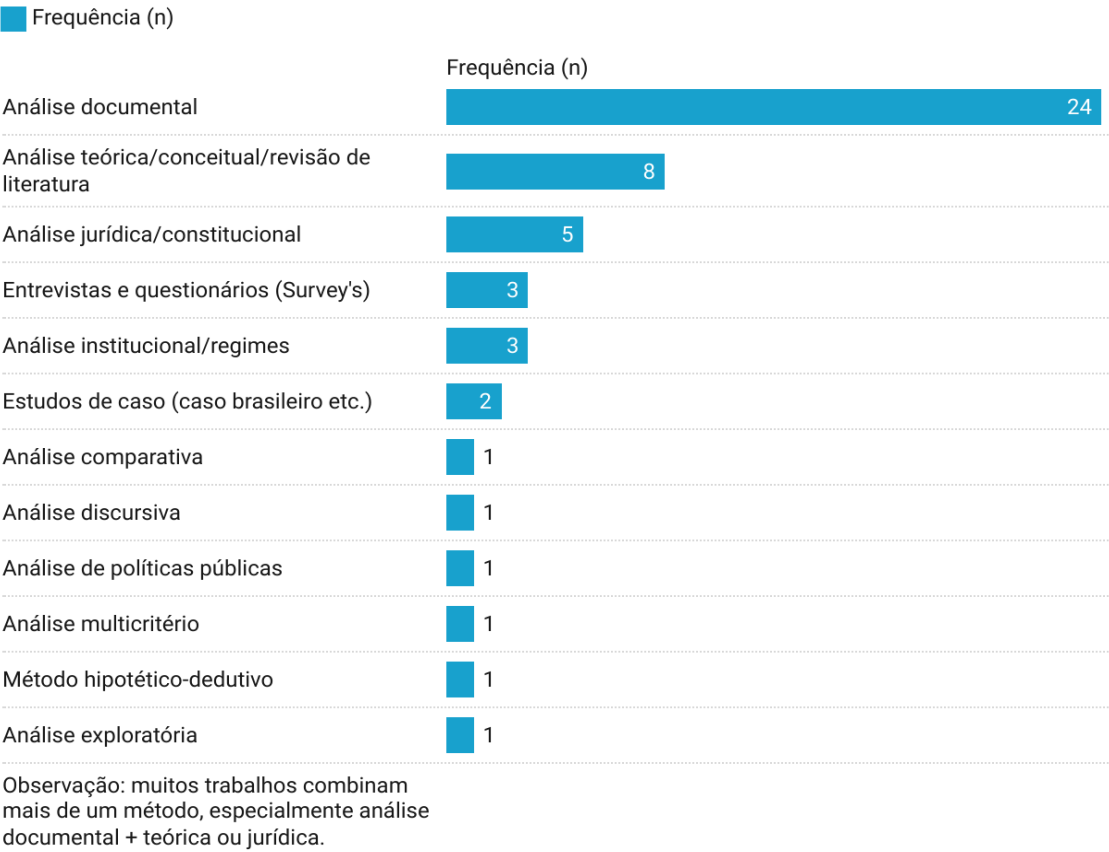


Gráfico: Criado pelo autor. • Fonte: Elaboração própria (2025) • Criado com Datawrapper

Fonte: Elaboração própria do autor (2025)

A análise das metodologias revela que a maioria dos trabalhos se apoia fortemente na análise documental, o que já era esperado, considerando que muitos desses estudos se debruçam sobre legislações, diretrizes estatais e documentos oficiais.

Ademais, chama atenção a presença significativa de revisões teóricas e análises conceituais, utilizadas principalmente em pesquisas que buscam compreender os fundamentos normativos e políticos da regulação do ciberespaço. Alguns trabalhos também apostam em entrevistas, questionários e estudos de caso, embora em número menor, o que sugere um esforço ainda inicial de trazer evidências empíricas para o debate. Há, ainda, metodologias mais específicas, como análises jurídicas, institucionais e discursivas, que aparecem de forma

complementar em certas pesquisas. Em geral, nota-se que o campo ainda privilegia abordagens mais normativas e qualitativas, com espaço para maior diversificação metodológica no futuro.

Tabela 2 - Impactos das áreas temáticas e relevância dos autores em determinados estudos.

Especifica quais autores e áreas temáticas de estudo estão moldando o campo.

Área Temática	Descrição	Autores Principais
Regulação e Direito Internacional	Estuda a construção de normas, estruturas legais e regimes internacionais voltados ao ciberespaço, incluindo soberania digital, jurisdição e proteção de dados.	Lino Santos, Gonçalo Nuno Baptista de Sousa, Zulmar Fachin, Fernanda Marques Alves, Rafael Padilha dos Santos Vaz, Carmille Leal do Amaral
Cibersegurança como Política Pública	Enfoca a formulação de políticas estatais para a proteção do ciberespaço, estratégias de segurança nacional e estruturas administrativas.	Schwether & Oliveira, Rafael de Souza & Cinthia Freitas, Maria Luís Barbosa, Rodrigo Eurico Fidalgo Pombo, Bruno José de Sá Vaz, Eduardo de Rê, LUANA C. C. Borges
Geopolítica e Relações Internacionais	Analisa o impacto da tecnologia e da cibersegurança nas dinâmicas de poder global, com foco em disputas entre grandes potências e reconfiguração do sistema.	Pecequillo & Marzinotto Jr., BRUNO MOSER NUNES et al., Gabriel Coutinho, Márcio Jorge Ferreira Guimarães, Arthur Martini Bronzatti
União Europeia como Ator Regulatório	Estuda a atuação da UE como promotora de normas e modelos de cibersegurança, especialmente em proteção de dados, segurança digital e direitos fundamentais.	Sofia Martins Gerales, Graça Enes et al., Maria Luís Barbosa, Inês Isabel Baião Serrano, Márcio Jorge Ferreira Guimarães
Governança Global e Multilateralismo	Reflete sobre a arquitetura internacional da governança do ciberespaço, envolvendo múltiplos atores e modelos concorrentes de regulação.	Tiago Mallmann Guterres Lopes, Rafael Oliveira Brotherhood, Jaqueline Trevisan Pigatto, Rafael Padilha dos Santos Vaz, Fernanda Marques Alves, Louise Marie Hurel

Tabela: Criado pelo autor • Fonte: Elaboração própria (2025) • Criado com Datawrapper

Fonte: Elaboração própria do autor (2025)

A análise desses estudos permite a identificação de cinco grandes áreas temáticas que refletem as principais linhas de pesquisa sobre o ciberespaço nas Relações Internacionais. A categorização apresentada a seguir evidencia como os pesquisadores têm abordado esse fenômeno multifacetado, revelando tanto a diversidade teórica quanto a centralidade do tema na agenda internacional contemporânea.

1. Regulação e Direito Internacional no Ciberespaço³⁶

A área de maior incidência nos trabalhos analisados diz respeito à interseção entre o Direito Internacional e a regulação do ciberespaço. As contribuições concentram-se na adaptação de normas tradicionais a um ambiente digital transnacional, destacando temas como soberania, jurisdição, ciberguerra, direitos fundamentais e governança normativa.

Autores como Fachin (2020), Barbosa (2022), Pombo (2021) e Enes et al. (2023) abordam as implicações jurídicas da crescente digitalização das relações sociais e políticas, enfatizando a urgência de respostas regulatórias eficazes e multiescalares. Esses trabalhos reforçam que a ausência de marcos jurídicos claros no ciberespaço compromete a estabilidade normativa global, tornando-o um espaço de disputa entre modelos regulatórios concorrentes.

2. Cibersegurança como Política Pública e Estratégia Nacional/Regional³⁷

Nesta categoria, observa-se um conjunto de estudos que examina a cibersegurança como um problema de política pública, com ênfase em estratégias nacionais e regionais. Schwether e Oliveira (2021), Sá Vaz (2023) e Guterres Lopes (2021) oferecem análises comparativas sobre planos de segurança digital, destacando tanto os desafios da coordenação institucional quanto às diferenças entre os modelos adotados por países e blocos regionais.

Os textos mostram que a cibersegurança ultrapassa o domínio técnico, consolidando-se como um eixo estratégico para a soberania estatal e a proteção de infraestruturas críticas. Em muitos casos, como destacam Geraldles (2020) e Sousa (2022), essas políticas são moldadas por influências externas, como os padrões da União Europeia e os posicionamentos das grandes potências tecnológicas.

3. Geopolítica e Disputa Internacional no Ciberespaço³⁸

Outro eixo central diz respeito à geopolítica da internet e à competição interestatal pelo controle das infra estruturas e fluxos digitais. Autores como Pecequillo e Marzinotto Jr. (2020), Guimarães (2021) e Dumit (2022) destacam o ciberespaço como campo de disputa estratégica entre Estados Unidos, China, União Europeia e outros atores, seja por meio do desenvolvimento de tecnologias críticas, seja pela imposição de padrões regulatórios. A abordagem evidencia que o poder cibernético tornou-se uma dimensão central das relações internacionais

³⁶ Ver KASPERSEN, Anja. "International law in cyberspace: old rules, new battles." *Sur - International Journal on Human Rights*, v. 14, n. 26, 2017.

³⁷ Cf. CARR, Madeline. "Public-private partnerships in national cyber-security strategies." *International Affairs*, v. 92, n. 1, 2016.

³⁸ Ver NYE, Joseph S. "Cyberpower." *Harvard Belfer Center Paper*, 2010.

contemporâneas, em que o domínio sobre dados, redes e plataformas digitais é diretamente associado à capacidade de influência global.

4. Governança Global da Internet e Ciberdiplomacia

A governança da internet e os esforços diplomáticos para criar normas multilaterais formam o núcleo desta área temática. Brotherhood (2022), Marques Alves (2021) e Padilha dos Santos Vaz (2020) analisam a atuação de instituições internacionais e blocos regionais, com ênfase na construção de consensos e na formação de regimes voltados à segurança digital. A ciberdiplomacia aparece como ferramenta de mitigação de conflitos cibernéticos, sendo particularmente relevante para países do Sul Global, como o Brasil, que buscam equilibrar sua atuação entre diferentes pólos de influência (Amaral, 2021). A literatura também aponta para a fragmentação da governança global, na medida em que se intensificam os desacordos sobre princípios como neutralidade da rede, proteção de dados e jurisdição digital.

5. Teoria das Relações Internacionais e Poder no Ciberespaço

Por fim, os estudos mais teóricos da amostra trazem importantes contribuições ao aplicar conceitos clássicos das Relações Internacionais à análise do ciberespaço. Bronzatti (2021), Santos (2020) e Hurel (2022) examinam, por exemplo, a securitização da ameaça digital, a transformação da soberania estatal e o surgimento de novos vetores de poder, como o chamado “Software Power”³⁹. Tais abordagens ampliam o escopo analítico do campo ao integrar discussões sobre tecnologia, segurança e construção social de ameaças, revelando como o ciberespaço desestabiliza categorias analíticas tradicionais.

Basicamente, essa categorização temática permite visualizar a complexidade e a interdisciplinaridade que caracterizam o debate sobre o ciberespaço nas Relações Internacionais. A regulação jurídica e a formulação de políticas públicas de segurança digital aparecem como eixos dominantes, mas os trabalhos também apontam para uma crescente preocupação com os impactos geopolíticos da digitalização e com os desafios teóricos impostos pela emergência do ciberespaço como arena autônoma.

³⁹ Ver MAZZUCATO, Mariana. *The Value of Everything*. Penguin Books, 2018.

Tabela 3 – Gaps e Oportunidades de Pesquisa

Identificação de temas pouco explorados ou regiões pouco analisadas.

Tema/Região	Observação
Mercosul / América do Sul	Praticamente ausente. Nenhuma análise focada em integração regional sul-americana
CPLP (Comunidade dos Países de Língua Portuguesa)	Ausente. Não há referência à articulação lusófona sobre cibersegurança ou regulação digital
África / Países Africanos	Ausente. Nenhum estudo voltado para contextos africanos ou a atuação continental sobre o tema
Sudeste Asiático / ASEAN	Não identificado. Nenhuma menção aos países asiáticos do bloco regional (exceto China)
América Latina (exceto Brasil)	Pouco abordada. Apenas o Brasil aparece isoladamente; vizinhos regionais são ignorados
Temas relacionados à juventude e educação digital	Inexistentes nas amostras analisadas
Setor privado e Big Techs	Pouco abordado. Não há objetivos que investiguem empresas privadas ou regulação de plataformas

Tabela: Criado pelo autor • Fonte: Elaboração própria (2025) • Criado com Datawrapper

Fonte: Elaboração própria do autor (2025)

A escassez de trabalhos que abordem integrações regionais fora do eixo Europa-EUA, como o Mercosul ou a CPLP⁴⁰, evidencia uma lacuna importante no mapeamento das respostas políticas e normativas à cibersegurança no Sul Global. Do mesmo modo, a ausência de perspectivas africanas e latino-americanas (exceto Brasil) indica a necessidade de descolonizar o debate sobre regulação digital e incorporar outros contextos regionais ao centro da discussão acadêmica.

Além disso, há uma notável carência de investigações sobre o papel de atores não estatais, especialmente empresas de tecnologia, sociedade civil e usuários em geral, bem como

⁴⁰ A Comunidade dos Países de Língua Portuguesa (CPLP) é uma organização internacional criada em 1996, composta por Estados que têm o português como idioma oficial. Seus membros são Angola, Brasil, Cabo Verde, Guiné-Bissau, Moçambique, Portugal, São Tomé e Príncipe, Timor-Leste e Guiné Equatorial. A CPLP tem como objetivos principais o fortalecimento da cooperação política e diplomática, a promoção da língua portuguesa e o desenvolvimento de projetos conjuntos nas áreas da educação, cultura, segurança, saúde e tecnologia.

temas transversais como educação digital, juventude, gênero e privacidade. Isso pode limitar a compreensão mais ampla do impacto social das estruturas de ciber governança.

Gráfico 6 – Nível de regulação

Predominância e amplitude da regulação proposta nas pesquisas.

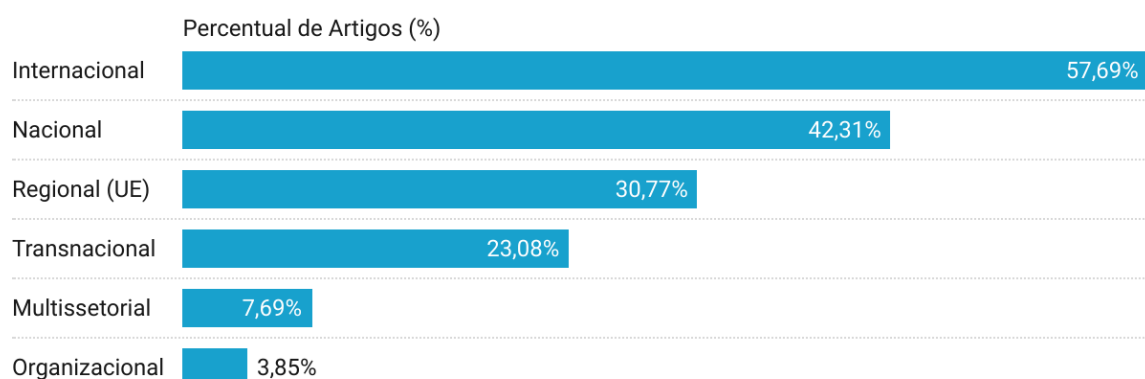


Gráfico: Criado pelo autor • Fonte: Elaboração própria (2025) • Criado com Datawrapper

Fonte: Elaboração própria do autor (2025)

O nível de regulação abordada nos artigos é predominantemente Internacional e Nacional, com uma forte presença Regional (UE) e uma relevante consideração do nível Transnacional. A amplitude é notável, com muitos estudos analisando a interação entre múltiplos níveis de regulação. Vale ressaltar que a soma das porcentagens será maior que 100%, pois um mesmo artigo frequentemente aborda múltiplos níveis de regulação. Cada porcentagem representa a proporção dos 26 artigos que incluem aquele nível específico.

Limitações

Ainda que tenha respondido à pergunta de pesquisa, a principal limitação faz referência à própria metodologia. Pois normalmente, uma revisão sistemática necessita de um grupo maior de pesquisadores e de profissionais especializados em diversas áreas de estudo e da ciência. Necessariamente dois para fazer a codificação e correção das partes codificadas e analisadas. Para suprir essa limitação, fez-se necessário o próprio autor elaborar todas as fases do processo literário e metodológico da pesquisa.

Ainda houve limitações acerca dos softwares utilizados, no qual o *Harzing's Publish or Perish 8.8* não se mostrou tão intuitivo nas pesquisas então apesar de ter sido utilizado no início, por necessidade e urgência na conclusão da pesquisa, toda a busca e armazenagem dos artigos foi migrada para o Zotero que se pareceu muito mais intuitivo, onde através de sua ferramenta

no próprio navegador, permite ao pesquisador baixar rapidamente quantidades massivas de artigos de qualquer base de dados e bibliotecas digitais artigos científicos e periódicos.

Outra limitação foi com relação à quantidade de artigos selecionados para a pesquisa, já que os critérios de seleção e a urgência com relação à publicação da pesquisa acabaram por limitar a sua robustez. Por fim, o principal limitador foi o tempo, pois fez a pesquisa se voltar à maior parte dos artigos para os de língua portuguesa, idioma nativo do autor, agilizando o processo de revisão, ainda de deixando de lado boa parte da literatura em língua inglesa que por ser mais rica em quantidade e qualidade, poderia agregar significativamente à pesquisa.

As planilhas e os dados usados nesta pesquisa serão disponibilizados de forma pública no repositório OSF, seguindo os princípios de transparência científica e as boas práticas acadêmicas. Para não só permitir que outros pesquisadores possam reproduzir a análise realizada, mas também contribuir com informações que ajudem a ampliar a base de dados e aprofundar o estudo da literatura sobre a regulação do ciberespaço.

5. CONCLUSÃO

O presente trabalho focou em analisar o estado da literatura voltada à regulação do ciberespaço onde se encontram os principais conflitos e debates acerca da cibersegurança entre os anos de 2015 e 2025. Para isso, o estudo abordou o método de revisão sistemática da literatura, tratando desde a coleta dos dados, a sua codificação e análise de 26 artigos a partir de critérios de inclusão e exclusão pré-determinados.

A princípio, foram utilizados diferentes tipos de softwares para determinadas fases. Onde inicialmente buscou-se através do Zotero, extrair e armazenar a maior quantidade de artigos e publicações científicas de diferentes buscadores acerca do tema, para filtrar com os critérios de seleção. Posteriormente, foi feita a codificação dos elementos nas seguintes variáveis: "Identificador", "Título do Artigo", "Autor(es)", "Ano de Publicação", "Fonte ou Revista Científica", "Tipo de Publicação", "Afiliação Institucional do(s) Autor(es)", "Enfoque Principal do Estudo", "Perspectiva Teórica Utilizada", "Âmbito Geográfico de Análise", entre outras variáveis. Através da análise desses dados obtidos nas pesquisas, pôde-se chegar à resposta para a pergunta base.

Os primeiros resultados das análises sobre o tipo de documento predominante, revelaram que a produção acadêmica no campo da cibersegurança e da regulação do ciberespaço está majoritariamente concentrada em artigos científicos publicados em periódicos especializados, seguidos por dissertações de mestrado. Essa predominância de artigos indica que os resultados das pesquisas na área são amplamente difundidos por meio de publicações em revistas acadêmicas, o que contribui para a rápida circulação e o debate entre pares.

Seguido pelas análises de escopo geográfico, onde revelou uma concentração significativa de estudos voltados para a União Europeia, bem como para questões de caráter global e internacional. Essa predominância sugere que as pesquisas acadêmicas têm direcionado atenção especial à estrutura normativa e institucional europeia, reconhecida por sua liderança em iniciativas regulatórias no campo digital.

Ao mesmo tempo, o enfoque global demonstrou a relevância das dinâmicas transnacionais da cibersegurança, que ultrapassam fronteiras estatais e exigem abordagens cooperativas e multilaterais. Ressalta-se, ainda, a presença do Brasil como objeto de investigação, especialmente no que se refere à construção de políticas públicas, estratégias nacionais de segurança cibernética e inserção em fóruns.

Acerca dos números de publicações por ano, pôde-se inferir que nos últimos anos, tem-se observado um crescimento considerável na produção acadêmica voltada para a cibersegurança e a regulação do ciberespaço. Esse movimento se intensificou especialmente após eventos marcantes, como o ataque NotPetya, em 2017, e o início da guerra na Ucrânia, em 2022. Tais acontecimentos evidenciaram a centralidade do ciberespaço nas disputas internacionais contemporâneas, ao expor a vulnerabilidade de infraestruturas críticas e ao destacar o uso estratégico de ferramentas digitais em conflitos geopolíticos.

A partir disso, questões como segurança digital, soberania tecnológica e governança multilateral passaram a ganhar maior espaço nos debates acadêmicos. Como observa Deibert (2021), o crescente uso do ciberespaço como instrumento de poder e influência tem exigido novas formas de regulação e cooperação internacional.

Em seguida foi analisada a literatura acerca dos temas mais frequentes e concentrou-se principalmente em três áreas: Relações Internacionais (23%), Estudos de Segurança (21%) e Direito Internacional (21%), abordando temas como soberania, poder, cibersegurança e a criação de normas jurídicas no ambiente digital. Além disso, questões como governança global (11%), regulação comparada e disputas por modelos de controle (9%) são frequentemente discutidas, refletindo as dinâmicas geopolíticas e os interesses de diferentes países e blocos regionais. Embora áreas como Filosofia da Tecnologia, Sociologia e Gestão da Informação

contribuam para o debate, sua presença na literatura ainda é menos significativa, evidenciando a predominância das abordagens mais convencionais na análise da regulação do ciberespaço.

Ainda, elaborou-se uma tabela para categorizar e especificar os setores com mais aparições em foco nas publicações, agrupados entre atores, quantidade de vezes que foi foco e suas categorias, em ordem crescente de classificação dos principais atores envolvidos aos menos.

Dando continuidade aos resultados, também foi feita uma análise dos setores e atores mais envolvidos na literatura, revelando os Estados nacionais e a União Europeia como os principais atores nas discussões sobre a regulação do ciberespaço. Sob um claro foco nas estruturas de poder bem como na formulação de políticas públicas. Seguido por organizações internacionais, atores não estatais, refletindo preocupações com a dimensão democrática da regulação digital e o setor privado, que apesar de sua influência, é menos abordado, enquanto o setor militar apareceu em contextos estratégicos específicos.

Logo após, analisou-se quais os tipos de metodologias mais empregadas nos trabalhos e concluiu-se que a maioria dos estudos sobre regulação do ciberespaço utiliza análise documental, especialmente por lidarem com legislações e diretrizes oficiais. Revisões teóricas e análises conceituais também são frequentes, enquanto métodos empíricos, como entrevistas e estudos de caso, aparecem com menos destaque. Abordagens jurídicas, institucionais e discursivas surgem de forma complementar, revelando um campo ainda dominado por metodologias normativas e qualitativas.

Por fim, houveram três grandes análises, a primeira com relação aos impactos das áreas temáticas e relevância dos autores em determinados estudos. Onde foi possível identificar cinco grandes áreas temáticas que estruturam o debate sobre o ciberespaço nas Relações Internacionais: (I) a regulação jurídica e o Direito Internacional, com destaque para a adaptação de normas tradicionais ao ambiente digital; (II) a cibersegurança como política pública e estratégia nacional, marcada por planos estatais e modelos regionais de proteção digital; (III) a geopolítica do ciberespaço, centrada na disputa entre grandes potências pelo controle das infra estruturas e fluxos de dados; (IV) a governança global da internet e a ciber diplomacia, com foco na atuação multilateral e na fragmentação dos regimes normativos; e (V) as abordagens teóricas que aplicam conceitos das Relações Internacionais à compreensão dos novos vetores de poder e ameaça no espaço digital.

Essa categorização evidenciou tanto a diversidade das abordagens quanto a centralidade do ciberespaço na agenda internacional contemporânea, demonstrando a complexidade e o caráter interdisciplinar do tema.

A segunda foi com relação aos “gaps” e onde se dá oportunidades de pesquisas futuras. Evidenciou uma lacuna significativa na literatura sobre cibersegurança no que diz respeito às integrações regionais fora do eixo Europa-EUA, como o Mercosul e a CPLP, bem como à escassa presença de perspectivas africanas e latino-americanas (com exceção do Brasil).

Essa ausência reforça a necessidade de descolonizar o debate e ampliar a inclusão de contextos do Sul Global. Também se observou uma carência de estudos voltados ao papel de atores não estatais, como empresas de tecnologia, sociedade civil e usuários. Em temas transversais, como educação digital, juventude, gênero e privacidade, o que pode restringir uma compreensão mais ampla e socialmente sensível das dinâmicas da ciber governança.

Finalmente, a última análise de revisão dos artigos, referente aos níveis de regulação, revelou que os níveis internacional e nacional são os mais recorrentes nas discussões sobre regulação do ciberespaço, seguidos de uma presença significativa do nível regional, especialmente no contexto da União Europeia, e de um interesse crescente pelo nível transnacional. Cabe destacar que muitos trabalhos abordam mais de um nível simultaneamente, o que justifica a sobreposição nas proporções analisadas.

6. REFERÊNCIAS

ALVES, Fernanda Marques. Espaço cibernético: desafios para a sua regulamentação e seu impacto sobre a relação de poder entre Estados soberanos. 2025. Disponível em: <https://repositorio.uniceub.br/jspui/handle/prefix/15671>. Acesso em: 12 abr. 2025.

AMARAL, Carmille Leal do. Regulação do ciberespaço: o enfrentamento do regime jurídico constitucional de proteção dos direitos fundamentais perante o alcance das novas tecnologias. 2021. Dissertação (Mestrado) – Universidade de Lisboa, Lisboa, 2021. Disponível em: <https://search.proquest.com/openview/b4140f5f383b392a8aca9117a79e6e94/1?pq-origsite=gscholar&cbl=2026366&diss=y>. Acesso em: 12 abr. 2025.

BARBOSA, Maria Luís. As ameaças ao ciberespaço e a estratégia de cibersegurança na UE e em Portugal. *Revista de Direito*, p. 161, 5 abr. 2025.

BORGES, Luana Chystyna Carneiro. Teorias ciberregulatórias e o caso brasileiro: entre regulação e governança. 2019.

BRONZATTI, Arthur Martini. Os atores não-estatais e estatais no mundo cibernético e sua influência no sistema internacional. 2021. Disponível em: <http://repositorio.jesuita.org.br/bitstream/handle/UNISINOS/11772/Arthur%20Martini%20Bronzatti.pdf?sequence=1>. Acesso em: 12 abr. 2025.

BROTHERHOOD, Rafael Oliveira. Cibersegurança e cyberdiplomacy: o papel da diplomacia brasileira nas Nações Unidas para a normatização do ciberespaço. 2024. Dissertação (Mestrado) – Universidade de Lisboa, Lisboa, 2024. Disponível em: <https://search.proquest.com/openview/0d784eb89c5d471174cfa17c469f9028/1?pq-origsite=gscholar&cbl=2026366&diss=y>. Acesso em: 12 abr. 2025.

CAVELTY, Myriam Dunn. Cyber Security Politics: Socio-Technological Transformations and Political Fragmentation. London: Routledge, 2022.

COUNCIL ON FOREIGN RELATIONS. Increasing International Cooperation in Cybersecurity and Adapting Cyber Norms. 2021. Disponível em: <https://www.cfr.org>. Acesso em: 05 abr. 2025.

COUTINHO, Gabriel. Militarização da inteligência artificial: sistemas de armas autônomas, governança internacional e a campanha Stop Killer Robots. 2024. Disponível em: <https://repositorio.ufsc.br/handle/123456789/262041>. Acesso em: 12 abr. 2025.

DE NARDIS, Laura. The Global War for Internet Governance. New Haven: Yale University Press, 2014.

DINIZ SCHWETHER, Natália; OLIVEIRA, Marcos Aurélio Guedes de. A cibernética na grande estratégia: um estudo comparado de Reino Unido, França e Portugal. *Relações Internacionais*, n. 82, 2024. Disponível em: https://ipri.unl.pt/images/publicacoes/revista_ri/pdf/ri82/RI_82_NET_NataliaSchwether_MarcosdeOliveira.pdf. Acesso em: 12 abr. 2025.

DUMIT, Patryck Lino. A realidade da cibersegurança nas organizações portuguesas. 2023. Dissertação (Mestrado) – ISCTE-Instituto Universitário de Lisboa, Lisboa, 2023. Disponível em: <https://search.proquest.com/openview/6afclala8d02d76c25e148ca8a179073/1?pq-origsite=gscholar&cbl=2026366&diss=y>. Acesso em: 12 abr. 2025.

ENES, Graça; MONTEIRO, Augusto Batalha; OLIVEIRA, Flávia. A reforma da cibersegurança na União Europeia: o regime jurídico de cibersegurança instituído pela Diretiva (UE). *Western Journal of Communication*, v. 63, n. 3, p. 382–412, 7 abr. 2025.

FACHIN, Zulmar. Desafios da regulação do ciberespaço e a proteção dos direitos da personalidade. *Revista Jurídica (FURB)*, v. 25, n. 56, p. e10081–e10081, 2021.

GERALDES, Sofia Martins. A estratégia de cibersegurança da União Europeia: catastrofista, realista e/ou otimista? *Nação e Defesa*, n. 154, p. 91–108, 2019.

GREENLEAF, Graham. Global Data Privacy Laws 2017: 120 National Data Privacy Laws, Including Indonesia and Turkey. *Privacy Laws & Business International Report*, n. 145, 2018.

GUIMARÃES, Márcio Jorge Ferreira. O contributo da União Europeia para a segurança da informação: a proteção da identidade digital dos cidadãos e a posição soberana dos Estados aplicada aos conflitos no ciberespaço. 2020. Dissertação (Mestrado) – Universidade de Lisboa, Lisboa, 2020. Disponível em:

<https://search.proquest.com/openview/dc66b6a594cb433b203d548ce91bb52a/1?pq-origsite=gscholar&cbl=2026366&diss=y>. Acesso em: 12 abr. 2025.

HUREL, Louise Marie. Securitização e a governança da segurança cibernética no Brasil. *Horizonte Presente: Tecnologia e Sociedade em Debate*, p. 320–342, 2019.

KITTICHAISAREE, Kriangsak. Public International Law of Cyberspace. Cham: Springer, 2017.

LOPES, João Francisco Adriano Silva. A governação do ciberespaço: uma análise das dinâmicas de poder de um novo meio. 2021. Dissertação (Mestrado) – Universidade NOVA de Lisboa, Lisboa, 2021. Disponível em: <https://search.proquest.com/openview/0fc3a1a3d9e269b5bdc2d3dfde4094e1/1?pq-origsite=gscholar&cbl=2026366&diss=y>. Acesso em: 12 abr. 2025.

NUNES, Bruno Moser; OLIVEIRA, Thays Felipe David de; BRITO, Renato Victor Lira. Ciberdefesa e software power: uma análise exploratória da China. *Revista Brasileira de Estudos de Defesa*, v. 11, n. 1, 2024. Disponível em: <https://rbed.emnuvens.com.br/rbed/article/view/75323>. Acesso em: 12 abr. 2025.

NYE, Joseph S. Cyber Power. Cambridge, MA: Harvard University, Belfer Center for Science and International Affairs, 2010.

PAPAIANO, Theo; TINATI, Ramine; GLOVER, Matthew; LEAVEY, Gerard. *How to research social science: an introduction*. London: SAGE Publications, 2016.

PECEQUILO, Cristina Soreanu; MARZINOTTO JR., Francisco Luiz. A geopolítica da economia digital e os Estados Unidos: pressões internas e externas sobre a Meta Platforms e o TikTok (2018–2023). *Revista de Geopolítica*, v. 14, n. 4, p. 1–19, 2023.

PETTICREW, Mark; ROBERTS, Helen. *Systematic reviews in the social sciences: a practical guide*. Oxford: Blackwell Publishing, 2006.

PIGATTO, Jaqueline Trevisan. Governança global da internet: regimes e transnacionalidade no período pós-Snowden. 2024. Disponível em: <https://repositorio.unesp.br/entities/publication/75c5186c-0fdc-4aeb-ba2e-2e69f6d3aa95>. Acesso em: 12 abr. 2025.

POMBO, Rodrigo. Política europeia de segurança no ciberespaço. 2019. Tese (Doutorado) – Academia da Força Aérea, Lisboa, 2019. Disponível em: <https://comum.rcaap.pt/handle/10400.26/39771>. Acesso em: 12 abr. 2025.

RIORDAN, Shaun. Cyberdiplomacy: Managing Security and Governance Online. Cambridge: Polity Press, 2019.

SAMPAIO, Rafael; LYCARIÃO, Dyego. Revisão sistemática e metanálise em ciência política: práticas, desafios e oportunidades. *Revista Brasileira de Ciência Política*, n. 41, p. 1–38, 2023. Disponível em: <https://doi.org/10.1590/0103-3352.2023.41.266097>. Acesso em: 12 abr. 2025.

SANTOS, Lino. Cyberspace regulation: cesurist and traditionalists. 2015. Disponível em: <https://repositorio.ual.pt/bitstreams/56fa937d-aacd-416b-8cee-d40d3da742f8/download>. Acesso em: 12 abr. 2025.

SCHMIDT, Eric; COHEN, Jared. The New Digital Age: Reshaping the Future of People, Nations and Business. New York: Knopf, 2013.

SERRANO, Inês Isabel Baião. Cibersegurança na União Europeia: a ciberdiplomacia como ferramenta política de gestão e prevenção de conflitos. 2022. Dissertação (Mestrado) – Universidade de Évora, Évora, 2022. Disponível em: <https://search.proquest.com/openview/38eabcafd3d74df70e5a2268da3e4280/1?pq-origsite=gscholar&cbl=2026366&diss=y>. Acesso em: 12 abr. 2025.

SHANY, Yuval; MIMRAN, Tal. International Regulation of Cyber Operations. *Hebrew University of Jerusalem Legal Research Paper*, n. 22-2, 2021.

SOUSA, Gonçalo. Direito e ciberespaço: percursos institucionais numa perspetiva transdisciplinar. 2024. Disponível em: <https://repositorio.ulisboa.pt/handle/10400.5/98707>. Acesso em: 12 abr. 2025.

SOUZA, Leonardo Rafael de; FREITAS, Cinthia Obladen de Almendra. A construção da cibersoberania na União Europeia: a cibersegurança e a integração do ciberespaço europeu. *Revista de Direito Internacional*, v. 19, n. 3, 2022. Disponível em: <https://search.ebscohost.com/login.aspx?direct=true&profile=ehost&scope=site&authtype=crawler&jrnl=2236997X&AN=163033613>. Acesso em: 12 abr. 2025.

VALERIANO, Brandon; MANESS, Ryan C. International Relations Theory and Cyber Security. In: *Oxford Handbook of International Political Theory*, 2015.

VAZ, Bruno. A aplicabilidade do Direito dos Conflitos Armados à ciberguerra: o posicionamento da OTAN no Manual de Talin. 2017. Disponível em: <https://comum.rcaap.pt/handle/10400.26/21312>. Acesso em: 12 abr. 2025.

VAZ, Rafael Medeiros Popini. A proteção dos dados pessoais no direito do comércio internacional: a prevalência do modelo da União Europeia. 2023. Disponível em: <https://repositorio.ufsc.br/handle/123456789/251833>. Acesso em: 12 abr. 2025.