UDC 321.011+327.8(73)EC

DIVERGENT PATHS IN DIGITAL SOVEREIGNTY: A COMPARATIVE ANALYSIS OF EU AND US REGULATORY AND STRATEGIC FRAMEWORKS

D. A. BUKONKIN[a]

[a]*Belarusian State University, 4 Niezaliezhnasci Avenue, Minsk 220030, Belarus*

Abstract. This study compares how the EU and the US pursue digital sovereignty as a component of national digital security policy. The analysis examines the normative and legal frameworks of each actor, as well as their engagement on international platforms. It also explores the EU's multilateralist orientation alongside the US' alliance-building and leadership-focused paradigm. Through case studies, it identifies the challenges and risks each faces in implementing information sovereignty strategies and evaluates the diplomatic and legal ramifications of their respective approaches. The analysis also tracks shifts in US perspectives on collaboration with traditional partners. The conclusion assesses prospects for reconciling US and EU approaches within transatlantic relations.

Keywords: digital sovereignty; legal frameworks; global governance; data policy; geopolitical strategy.

РАЗНЫЕ ПУТИ К ЦИФРОВОМУ СУВЕРЕНИТЕТУ: СРАВНИТЕЛЬНЫЙ АНАЛИЗ НОРМАТИВНО-ПРАВОВОЙ БАЗЫ И СТРАТЕГИИ ЕС И США

Д. А. БУКОНКИН[1)]

[1)]*Белорусский государственный университет, пр. Независимости, 4, 220030, г. Минск, Беларусь*

Аннотация. Проводится сравнительный анализ подходов ЕС и США к реализации информационного суверенитета как интегральной политики информационной безопасности на государственном уровне. В рамках компаративистского подхода изучены сходства и различия в нормативной и правовой базах указанных акторов, их активность на международных площадках. Рассмотрены особенности мультилатералистской ориентации ЕС и ее отличия от стремящейся к созданию альянсов и лидерству ориентации США. Кроме того, на примере кейс-метода показаны различные вызовы и риски, с которыми сталкивается каждая из сторон в процессе реализации стратегии информационного суверенитета, дипломатические и правовые последствия, возникающие при реализации каждого из подходов. Прослеживается определенная эволюция взглядов американской администрации на сотрудничество со своими традиционными партнерами. Делается вывод о том, что указанные подходы каждой из сторон достаточно сложно совмещать в процессе выстраивания союзнических отношений по линии ЕС–США.

Ключевые слова: информационный суверенитет; правовое регулирование; международное сотрудничество; глобальное влияние; управление данными.

Образец цитирования:
Буконкин ДА. Разные пути к цифровому суверенитету: сравнительный анализ нормативно-правовой базы и стратегии ЕС и США. *Журнал Белорусского государственного университета. Международные отношения*. 2025; 1:26–34 (на англ.).
EDN: WGEBQK

For citation:
Bukonkin DA. Divergent paths in digital sovereignty: a comparative analysis of EU and US regulatory and strategic frameworks. *Journal of the Belarusian State University. International Relations*. 2025;1:26–34.
EDN: WGEBQK

Автор:
Денис Алексеевич Буконкин – соискатель кафедры политологии юридического факультета. Научный руководитель – доктор политических наук, профессор Н. А. Антанович.

Author:
Dzianis A. Bukonkin, competitor at the department of political science, faculty of law.
bukonkin@mail.ru

Introduction

Digital sovereignty, defined as a state's ability to govern data flows, digital infrastructure, and cyber norms, has emerged as a defining feature of 21st-century geopolitics [1, p. 12]. Accelerating digitalisation has heightened the strategic stakes of data flows, cybersecurity, and technological autonomy, creating new arenas for geopolitical competition. The EU and the US, as leading digital powers, adopt notably different approaches. The EU champions regulatory leadership founded on normative values such as privacy and fundamental rights, while the US favours security-centred pragmatism grounded in strategic alliances and proactive cyber capabilities [2, p. 220–223; 3, p. 2–6].

This paper compares these differing strategies, examining their underlying rationales, policy instruments, and implications for the global digital order [1, p. 25; 2, p. 224]. It investigates how these distinct strategies reveal deeper ideological differences between the EU's normative approach to digital governance and the US' security-driven pragmatism. As cyber threats intensify (evident in attacks on critical infrastructure and incidents of cyber-espionage) the contrasting strategies of the EU and the US reflect their distinct geopolitical priorities: regulation versus alliance-building.

The EU seeks digital sovereignty partly to address historical technological shortcomings and to safeguard individual privacy, even when this conflicts with commercial interests. Conversely, the US adopts a more market-driven strategy, emphasising technological leadership, international competitiveness, and a comparatively liberal approach to data flows. This divergence has created considerable friction in transatlantic data exchange.

Both actors have established legal frameworks to assert digital sovereignty. However, the EU has embraced a more regulatory approach, most notably through the General data protection regulation (GDPR), whereas the US leans towards industry-led self-regulation and voluntary standards. The EU has further advanced its ambitions by developing an alternative data infrastructure through projects such as «Gaia-X». This initiative aims to establish a federated data infrastructure consistent with European values and standards.

Academic discourse on digital sovereignty has grown substantially. A. Bradford's concept of the Brussels effect illustrates how EU regulations like the GDPR exert global normative influence [4]. Some scientists contend that European policies prioritise fundamental rights over economic imperatives [5]. Conversely, C. Kavanagh and J. B. Sheldon characterise US cybersecurity strategy as more pragmatic, emphasising national security and strategic alliances [6]. J. Goldsmith argues that US cyber policy aligns with wider geopolitical objectives, often sidelining normative frameworks in favour of security interests [7]. Recent comparative studies highlight tensions between EU regulatory frameworks and US pragmatism, particularly concerning transatlantic data flows in the wake of the Schrems II judgment, which invalidated the Privacy shield arrangement on transatlantic data transfers[1].

Russian-speaking scholars have contributed to this discourse. Ya. N. Shevchenko, A. Yu. Olimpiev, I. A. Strelnikova, P. Sharikov, N. Stepanova have addressed EU and US divergent policies relating to digital sovereignty through the lenses of global governance, digital security, and international law [8–10]. This analysis delineates the ideological and structural distinctions between EU and US approaches to digital sovereignty, situating them within wider geopolitical dynamics.

While existing scholarship extensively explores individual strategies, thorough comparative examinations remain scarce. This article bridges that gap through a systematic evaluation of EU and US digital sovereignty strategies, elucidating their ramifications for global governance.

Materials and methods

Employing qualitative thematic content analysis, this study scrutinises primary policy documents including the EU Digital sovereignty agenda, GDPR, Schrems II judgment, US Cyber Command doctrines, and the Clarifying lawful overseas use of data (CLOUD) act. The analysis is further informed by relevant academic scholarship. Empirical case studies, such as the Schrems II judgment, responses to the «SolarWinds» cyberattack, «Meta's» GDPR penalty, «Huawei» sanctions, and US Cyber Command's «hunt-forward» operations, demonstrate the real-world consequences of each strategy. This triangulated methodology illuminates the divergent models of digital sovereignty pursued by the EU and the US.

Comparative strategy analysis

EU strategy: regulatory hegemony and normative influence. The EU's strategy relies on comprehensive regulatory frameworks designed to project its normative power globally, a phenomenon often termed the Brussels effect [4, p. 10–16]. Central to it is the GDPR, which establishes stringent privacy standards with

[1]The Court of Justice invalidates decision 2016/1250 on the adequacy of the protection provided by the EU – US Data protection shield [Electronic resource]. URL: https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091en.pdf (date of access: 24.03.2025) ; *Burwell F.* Looking ahead to the next chapter of US – EU digital collaboration [Electronic resource]. URL: https://www.atlanticcouncil.org/in-depth-research-reports/report/looking-ahead-to-the-next-chapter-of-us-eu-digital-collaboration/ (date of access: 24.03.2025) ; EU – US relations on Internet governance [Electronic resource]. URL: https://www.chathamhouse.org/2019/11/eu-us-relations-internet-governance (date of access: 24.03.2025).

extraterritorial reach. By mandating compliance under threat of substantial fines (exemplified by «Meta's» 1.2 bln euro penalty in 2023)[2] the regulation has recalibrated international data governance norms.

The Schrems II judgment reinforced the EU's regulatory authority by invalidating the Privacy shield framework, citing insufficient safeguards against US surveillance. Initiatives such as «Gaia-X» seek to lessen European reliance on non-European cloud providers by developing sovereign cloud infrastructure. Similarly, the Articial intelligence (AI) act establishes risk-based regulations to ensure ethical AI deployment consistent with European values[3].

US strategy: security-centric pragmatism and alliance-building. In contrast, the United States prioritises security-oriented pragmatism, pursued through proactive cyber operations and strategic alliances. US Cyber Command's «defend forward» doctrine exemplifies this stance, deploying «hunt-forward» missions on allied networks to detect threats pre-emptively [6, p. 14–15].

The CLOUD act demonstrates pragmatic principles by granting law enforcement agencies extraterritorial data access, placing national security above privacy concerns [11, p. 397–398]. Similarly, export controls outlined in the Creating helpful incentives to produce Semiconductors (CHIPS) and science act deploy strategic economic leverage to constrain adversaries' technological advancements, notably targeting China's semiconductor industry[4].

Alliance-building also forms a key component of US strategy. Quadrilateral security dialogue (Quad) and AUKUS (Australia, UK, US) explicitly aim to counterbalance China's growing technological influence. The sanctions against «Huawei» further illustrate how diplomatic alliances can be utilised to isolate Chinese technology firms from global markets.

The comparative table highlights that while both the EU and the USA recognise the critical importance of digital sovereignty, their strategies diverge significantly due to underlying following ideological differences:

- the EU's normative-regulatory model, exemplified by GDPR and Schrems II judgment seeks to influence global standards through stringent compliance requirements rooted in fundamental rights protection;
- the US' pragmatic-security model, characterised by proactive cyber operations («defend forward»), export controls via CHIPS and science act, and alliance-building initiatives like Quad or AUKUS, prioritises national security interests over normative considerations.

Both approaches have distinct advantages and limitations:

- the EU's rigorous regulations provide strong protections but risk stifling innovation among smaller firms;
- the US' flexible, alliance-based strategy allows rapid response to threats but raises diplomatic tensions and internal ideological conflicts regarding Internet openness.

Despite these differences, shared geopolitical threats particularly from authoritarian states like China and Russia may drive future convergence toward hybrid strategies integrating regulatory norms with strategic alliances.

Comparative analysis of digital sovereignty: EU and US approaches

Criterions	EU	US	Comparative implications
Strategic orientation	• Normative or regulatory-driven (Brussels effect) character • Emphasis on privacy, fundamental rights, consumer protection	• Security-driven pragmatic character • Emphasis on national security, strategic alliances, proactive cyber defence	EU prioritises rights-based governance. US emphasises security interests
Data regulation	• GDPR • Schrems II judgment (Privacy shield invalidation) • Digital markets act (DMA) • Digital services act (DSA)	• CLOUD act • Sector-specific regulations (California consumer prifacy act (CCPA), Health insurance portability and accountability act (HIPPA), etc.) • State-level privacy laws (varying by state)	GDPR has global normative influence but creates friction in transatlantic data flows, CLOUD act raises sovereignty concerns abroad
Cybersecurity approach	• Network and information systems directive • European Union Agency for Cybersecurity • Computer emergency response team – EU coordination • Cyber resilience act	• US Cyber Command («defend forward» doctrine) • National Security Agency cyber operations • Cybersecurity and Infrastructure Security Agency (CISA) coordination	EU emphasises resilience and regulatory frameworks. US emphasises proactive cyber operations and deterrence

[2]Antitrust: commission fines Meta 1.2 billion euro for breaching EU data protection rules [Electronic resource]. URL: https://ec.europa.eu/commission/presscorner/detail/en/ip_23_2778 (date of access: 24.03.2025).

[3]Proposal for a regulation laying down harmonised rules on artificial intelligence (Artificial intelligence act) [Electronic resource]. URL: https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence (date of access: 24.03.2025).

[4]Public law 117–167. Aug. 9, 2022 [Electronic resource]. URL: https://www.congress.gov/117/plaws/publ167/PLAW-117publ167.pdf (date of access: 24.03.2025).

Ending of the table

Criterions	EU	US	Comparative implications
Technological autonomy initiatives	• «Gaia-X» federated cloud initiative • European CHIPS act • AI act risk-based regulation • Horizon Europe funding programmes for tech innovation	• CHIPS and science act • Export controls on advanced technologies • Significant public-private investment in AI and quantum computing research	Both seek tech autonomy but through different methods: EU through regulation and public infrastructure, US through strategic investments and export controls
International engagement and diplomacy	• Multilateralism via UN digital compact, G7/G20 frameworks • Promotion of global digital norms aligned with human rights and democracy • Bilateral digital partnerships emphasising normative alignment	• Alliance-centric approach via Quad, AUKUS • Clean network initiative • Bilateral agreements prioritising security cooperation	EU promotes universal norms multilaterally. US builds targeted coalitions based on strategic alignment against geopolitical rivals like China or Russia
Key case studies and examples	• GDPR enforcement («Meta's» 1.2 bln euro fine in 2023) • Schrems II judgment disrupting data flows (1.3 bln euro economic impact in 2022) • «Gaia-X» implementation challenges due to reliance on non-EU tech providers	• «SolarWinds» cyberattack response (NATO collaboration and unilateral sanctions on Russian actors); • «Huawei» sanctions and global 5G coalition-building efforts isolating Chinese technology providers • *TikTok* bans, highlighting ideological tensions between openness and security	Case studies illustrate practical impacts: EU's regulatory rigour versus US' pragmatic security measures. Both strategies have economic and diplomatic implications
Challenges and limitations	• Regulatory burden potentially stifling innovation among startups • Persistent reliance (near 75 %) on non-European technology providers despite sovereignty initiatives • Difficulty balancing stringent regulations with rapid technological innovation needs	• Creation of internal ideological tradeoffs by balancing open Internet ideals with national security imperatives • Diplomatic risks associated with unilateral cyber operations («defend forward») • Fragmented domestic regulatory landscape complicates coherent national policy formulation	Both face internal tensions: EU struggles with innovation versus regulation balance. US faces ideological conflicts between openness and security interests
Future trajectories and emerging issues	• Quantum computing regulation frameworks under development • Internet of things (IoT) cybersecurity standards emerging via Cyber resilience act • Potential harmonisation with US under common threats from authoritarian regimes' cyber espionage activities	• Quantum computing investment prioritised for strategic advantage over China or Russia • IoT cybersecurity addressed through sector-specific standards rather than comprehensive federal legislation • Possible convergence with EU approaches under shared geopolitical threats	Emerging technologies will test existing frameworks, potential convergence toward hybrid models combining regulatory norms with strategic alliances is likely under shared geopolitical threats

International cooperation: alignment or discord?

The EU's multilateral approach: universal standards and human rights. The EU approach to cyber sovereignty rests on its normative governance model, prioritising human rights, privacy, and democratic values. Initiatives such as the UN Digital compact and the Cyber solidarity act advance a global cybersecurity framework that aligns with international human rights law[5]. Regulatory instruments like the GDPR and the DMA reinforce these objectives by promoting fair competition and protecting individual freedoms in digital environments[6].

This multilateral strategy facilitates broad coalitions with states, civil society, and private sector actors. Key mechanisms include the following positions:

• Cyber solidarity act, which provides for a European cybersecurity reserve and a cross-border threat-alert system to enhance collective defence against cyber-threats. These structures encourage resource-sharing and regional resilience;

• UN Digital compact, positioning the EU as a key architect of global cybersecurity norms by advocating inclusive, cooperative solutions to common challenges.

[5]European Union contribution to the Global digital compact [Electronic resource]. URL: https://www.un.org/digital-emerging-technologies/sites/www.un.org.techenvoy/files/GDC-submission_European-Union.pdf (date of access: 24.03.2025).

[6]European declaration on digital rights and principles [Electronic resource]. URL: https://digital-strategy.ec.europa.eu/en/library/european-declaration-digital-rights-and-principles (date of access: 24.03.2025).

Such efforts demonstrate the EU's ambition to embed human rights into digital governance while promoting interoperability and technological neutrality[7]. Despite its merits, the EU's multilateral approach encounters several obstacles:

1. Fragmentation. Divergent cybersecurity policies across member states complicate implementation. While the GDPR sets global benchmarks for data protection, enforcement remains inconsistent throughout the EU.

2. Technological dependence. The EU continues to rely on external technology providers for critical infrastructure, including cloud computing and semiconductors. Projects such as «Gaia-X» aim to enhance autonomy in these areas, but have struggled to achieve broad adoption[8].

3. Geopolitical vulnerabilities. The Schrems II judgment struck down the EU – US Privacy shield agreement with the US over concerns about American surveillance practices. This decision disrupted transatlantic data transfers and exposed tensions between European data protection standards and US security-driven policies[9].

Diverging sharply from European multilateralism, the US pursues a strategy centred on national security and strategic alliances. Frameworks like the Trade and Technology Council (TTC) and partnerships such as Quad and AUKUS enable Washington to align interests against common adversaries like China and Russia[10]. These arrangements allow the US to respond rapidly to emerging threats while sustaining technological superiority.

The pragmatic US approach draws on cooperation with both allies and private-sector actors. For example, the CISA international strategic plan promotes cross-border information-sharing and coordinated critical infrastructure protection[11], reflecting a commitment to building trust and addressing systemic vulnerabilities.

Similarly, the «defend forward» doctrine authorises targeting adversaries' networks with pre-emptive operations before threats materialise. This approach was credited with deterring malicious activity by increasing its costs, as demonstrated during incidents such as the «SolarWinds» breach[12].

Yet this coalition-centric model carries its own challenges, including the following:

• diplomatic risks (unilateral measures, such as sanctions or offensive cyber operations, risk straining alliances). NATO members, for example, raised concerns over collateral impacts during US countermeasures against Russian cyber actors in the «SolarWinds» case;

• fragmented regulation. Unlike the EU's GDPR, US policy remains divided between sector-specific laws, for example, HIPAA in healthcare, and state-level mandates like CCPA. This lack of uniformity undermines Washington's ability to advocate for a coherent global governance model [12, p. 1085–1086];

• ideological tensions. US policymaking grapples with an inherent trade-off between upholding open Internet ideals and addressing national security imperatives. Measures such as bans on *TikTok* illustrate this tension, pitting Internet freedom against mitigating perceived risks linked to foreign-operated platforms[13].

Despite differing policy approaches, shared challenges are prompting strategic alignment between the EU and US in critical domains.

Both actors confront escalating cyber threats, particularly state-sponsored attacks on vital infrastructure including energy, transport, and water systems. Enhanced cooperation through multilateral frameworks like NATO or the G7 could bolster joint defences and deepen trust among allies[14].

The transatlantic tensions in digital policies, as exemplified by the Schrems II judgment, could be alleviated by creating a more sustainable data privacy framework aligning GDPR safeguards with US security objectives. Such an approach would support uninterrupted cross-border data transfers essential for global commerce.

Collaborative ventures in quantum computing and AI safety protocols could establish both regions as standard-setters in digital governance. Ongoing TTC dialogues on quantum technologies, for example, highlight opportunities to co-design post-quantum encryption standards that address shared vulnerabilities.

[7]*Latici T.* Understanding the EU's approach to cyber diplomacy and cyber defence [Electronic resource]. URL: https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651937/EPRS_BRI(2020)651937_EN.pdf (date of access: 24.03.2025).

[8]*Körbächer M.* Is Gaia-X failing? [Electronic resource]. URL: https://www.linkedin.com/posts/maxkoerbaecher_gaia-x-failed-it-failed-already-years-ago-activity-7294417905893441536-DWih/ (date of access: 31.03.2025).

[9]Schrems II impact survey report [Electronic resource]. URL: https://www.digitaleurope.org/resources/schrems-ii-impact-survey-report/ (date of access: 24.03.2025).

[10]Fact sheet: Biden–Harris administration releases version 2 of the National cybersecurity strategy implementation plan [Electronic resource]. URL: https://bidenwhitehouse.archives.gov/oncd/briefing-room/2024/05/07/fact-sheet-ncsip-version-2/ (date of access: 24.03.2025).

[11]CISA Strategic plan 2023–2025 [Electronic resource]. URL: https://www.cisa.gov/sites/default/files/2025-01/StrategicPlan%2023-25%20508.pdf (date of access: 24.03.2025).

[12]Homeland threat assessment-2025 [Electronic resource]. URL: https://www.dhs.gov/sites/default/files/2024-10/24_0930_ia_24-320-ia-publication-2025-hta-final-30sep24-508.pdf (date of access: 24.03.2025).

[13]Fact sheet: Biden–Harris administration releases version 2 of the National cybersecurity strategy implementation plan [Electronic resource]. URL: https://bidenwhitehouse.archives.gov/oncd/briefing-room/2024/05/07/fact-sheet-ncsip-version-2/ (date of access: 24.03.2025).

[14]*Schroeder E., Scott S., Herr T.* Victory reimagined: toward a more cohesive US cyber strategy [Electronic resource]. URL: https://www.atlanticcouncil.org/wp-content/uploads/2022/06/Victory-reimagined-Toward-a-more-cohesive-US-cyber-strategy.pdf (date of access: 24.03.2025).

Key challenges

European Union. ***Regulatory burden inhibiting innovation.*** While the GDPR has pioneered global data protection and privacy benchmarks, its stringent provisions impose substantial compliance costs, particularly on startups and small and medium-sized enterprises. As Ya. N. Shevchenko observes, smaller firms often lack the administrative capacity to meet these demands, entrenching advantages for resource-rich multinationals and potentially stifling domestic technological advancement among smaller players [8, p. 257].

The EU's fragmented digital market exacerbates these challenges. The lack of regulatory harmonisation across member states hinders startups from scaling operations efficiently within the single market, diminishing their competitiveness against US and Chinese rivals [9, p. 76]. Critiques of the EU cybersecurity certification scheme further reveal gaps in addressing external threats, underscoring the necessity for integrated governance mechanisms [10, p. 80–81].

Persistent dependence on external technology providers. Europe continues to depend heavily on foreign providers for essential technologies, including cloud computing and semiconductors, despite initiatives such as «Gaia-X» and the European CHIPS act aimed at technological autonomy. Over 90 % of European data resides in US-based clouds, creating strategic vulnerabilities for the bloc[15]. This reliance compromises Europe's capacity to assert digital sovereignty while exposing its infrastructure to external security risks.

As A. Yu. Olimpiev notes, this dependence extends to Chinese corporations, notably «Huawei», which maintain dominant positions in critical sectors like 5G networks. Apprehensions regarding surveillance and cybersecurity have led to tighter restrictions on Chinese infrastructure, yet Europe still lacks competitive domestic alternatives in several domains[16]. Inability of the initiative «Gaia-X» to exclude foreign hyperscale cloud providers illustrates the difficulty of cultivating homegrown technological ecosystems[17].

Reconciling regulatory rigour with innovation demands. A central challenge for the EU lies in harmonising its stringent regulatory frameworks with the imperative to accelerate technological innovation. While instruments such as the AI act prioritise ethical AI development consistent with European values, they can impede swift technological adoption due to bureaucratic complexities and inconsistent implementation across member states[18].

As Ya. N. Shevchenko contends, such regulatory complexity risks stifling Europe's competitiveness in fields like artificial intelligence and quantum computing, where rivals such as the US and China advance with fewer constraints. Regulatory delays can deter private sector investment in high-risk, high-reward technologies, thereby constraining Europe's capacity for large-scale innovation [8, p. 257].

United States. ***Ideological tensions: open Internet versus national security.*** The US has long positioned an open Internet as integral to democratic principles, yet escalating geopolitical tensions have prompted measures prioritising national security, such as *TikTok* bans and semiconductor export controls under the CHIPS and science act. This reflects an unresolved tension between promoting Internet openness and addressing security threats from adversaries such as China[19].

P. A. Sharikov and N. V. Stepanova [10] critique this ambivalence, arguing that security-centric policies, while addressing immediate risks, erode trust in multilateral governance frameworks[20] and alienate international partners. The Trump administration's focus on economic protectionism further exemplifies a shift towards digital sovereignty policies that prioritise national security at the expense of broader international cooperation[21].

Diplomatic risks of unilateral cyber operations. The Pentagon's «defend forward» doctrine employs pre-emptive cyber operations against adversaries' networks before threats reach US systems. Although designed to deter malicious actors by raising their costs, this strategy presents significant diplomatic risks. A. Yu. Olimpiev and I. A. Strelnikova [9] caution that unilateral measures may escalate tensions with rivals such as Russia and China while undermining trust among traditional allies, who often perceive such operations as destabilising or disproportionate[22].

[15]Digital sovereignty: Europe's bold response to tech challenges [Electronic resource]. URL: https://europeanbusinessmagazine.com/business/digital-sovereignty-europes-bold-response-to-tech-challenges/ (date of access: 24.03.2025).

[16]Homeland threat assessment-2025 [Electronic resource]. URL: https://www.dhs.gov/sites/default/files/2024-10/24_0930_ia_24-320-ia-publication-2025-hta-final-30sep24-508.pdf (date of access: 24.03.2025).

[17]The top-10 digital risks for organisations in 2025 [Electronic resource]. URL: https://www.controlrisks.com/our-thinking/insights/the-top-10-digital-risks-for-organisations-in-2025 (date of access: 24.03.2025).

[18]What is digital sovereignty and how are countries approaching it? [Electronic resource]. URL: https://www.weforum.org/stories/2025/01/europe-digital-sovereignty/ (date of access: 24.03.2025).

[19]*Marcos H.* The US – China mirror: TikTok, national security, and techno-nationalism [Electronic resource]. URL: https://opiniojuris.org/2025/05/02/the-us-china-mirror-tiktok-national-security-and-techno-nationalism/ (date of access: 24.03.2025).

[20]European tech industry coalition calls for «radical action» on digital sovereignty, starting with buying local [Electronic resource]. URL: https://techcrunch.com/2025/03/16/european-tech-industry-coalition-calls-for-radical-action-on-digital-sovereignty-starting-with-buying-local/ (date of access: 24.03.2025).

[21]Trump's impact on global data sovereignty [Electronic resource]. URL: https://incountry.com/blog/trumps-impact-on-global-data-sovereignty/ (date of access: 24.03.2025).

[22]Homeland threat assessment-2025 [Electronic resource]. URL: https://www.dhs.gov/sites/default/files/2024-10/24_0930_ia_24-320-ia-publication-2025-hta-final-30sep24-508.pdf (date of access: 24.03.2025).

For example, NATO members raised concerns during US-led cyber campaigns against supposedly Russian-linked actors in incidents such as «SolarWinds» case. Such tensions underline the need for more coordinated cybersecurity approaches within multilateral frameworks[23].

Fragmented domestic regulatory landscape. US data governance lacks the harmonised structure of the EU's GDPR, instead comprising a patchwork of federal and state statutes. Regulatory dissonance not only diminishes the US's capacity to advocate a coherent model for global data governance but also imposes disproportionate compliance burdens on businesses operating across multiple jurisdictions[24].

A. Yu. Olimpiev and I. A. Strelnikova [9] observe that this disjointed regime impedes international collaboration on data protection standards. The absence of a unified federal privacy law stands in marked contrast to Europe's centralised approach, placing US enterprises at a disadvantage within the global regulatory environment [12, p. 1079–1080].

Empirical case studies

Information sovereignty (the capacity of states to regulate data flows, digital infrastructure, and cyber norms) has become a defining feature of contemporary global governance. The EU and the US exemplify contrasting strategies, shaped by diverging ideological frameworks and geopolitical imperatives. This section analyses three case studies: 1) the EU AI act; 2) the US response to the «SolarWinds» cyberattack; 3) the Schrems II judgment, examining their implications for sovereignty, innovation, and global governance.

The EU's AI act represents one of the world's most comprehensive regulatory frameworks for AI, though its implementation has revealed substantial challenges for smaller firms and start-ups. The act categorises AI systems into three risk levels: 1) unacceptable risk (banned outright); 2) high risk (stringent oversight); 3) minimal risk (lightly regulated).

High-risk systems must comply with rigorous requirements concerning algorithmic transparency, human oversight, and risk management. Compliance imposes significant challenges for developers.

Ya. N. Shevchenko notes that while the legislation advances Europe's ethics-driven governance framework, it disproportionately burdens small and medium-sized enterprises, which often lack sufficient financial or technical capacity for compliance [8, p. 261–265]. Start-ups, which depend on rapid innovation cycles, encounter delays in product launches due to exhaustive documentation processes and mandatory audits. This dynamic may stifle innovation among smaller firms, potentially advantaging established corporations with greater resources [9, p. 81–82].

The AI act's regulatory demands could further disadvantage European firms relative to competitors in less-regulated jurisdictions, such as the US or China. T. Schmalfeld contends that protracted time-to-market timelines for high-risk AI systems risk diminishing Europe's competitive position in rapidly evolving fields, including machine learning[25]. Such tensions exemplify the potential conflict between the EU's regulatory ambitions and its strategic goal of technological leadership [13, p. 23–24].

Though emblematic of Europe's normative governance ethos, the AI act raises critical questions about whether it effectively balances regulatory objectives with innovation incentives. A. Yu. Olimpiev and I. A. Strelnikova argues that excessive rigidity in compliance frameworks could hinder Europe's global competitiveness and constrain exploration in emerging fields such as generative AI or quantum computing [9].

Discovered in December 2020, the «SolarWinds» breach epitomises the scale of modern cyber espionage. Believed to be linked to Russia hackers exploited security flaws in platform «Orion» of «SolarWinds», a widely used IT management tool, to infiltrate US federal agencies and private entities. The incident exposed systemic vulnerabilities within supply chains, catalysing a comprehensive US response.

The Biden administration adopted a dual strategy: imposing unilateral sanctions on suspect Russian-linked entities, while simultaneously pursuing multilateral coordination through NATO. Sanctions specifically targeted Russia's Foreign intelligence service, in a move to establish accountability and a deterrent posture against future cyber threats. Concurrently, NATO partners were engaged to enhance collective cyber defences, reflecting a pragmatic balance between unilateral action and alliance-based cooperation.

A. Yu. Olimpiev and I. A. Strelnikova [9] caution that unilateral sanctions risk heightening confrontations with adversarial states, particularly Russia, while alienating allies who may view such measures as destabilising. Examples include NATO members' apprehensions regarding unintended consequences from US cyber campaigns against Russian entities during the «SolarWinds» incident. These diplomatic frictions highlight the necessity for multilateral coordination in cybersecurity governance [10].

[23] *Schroeder E., Scott S., Herr T.* Victory reimagined…

[24] Proposal for a regulation laying down harmonised rules on artificial intelligence (Artificial intelligence act) [Electronic resource]. URL: https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence (date of access: 24.03.2025).

[25] *Schmalfeld T.* Is the EU AI act unfair to smaller companies and startups? [Electronic resource]. URL: https://www.linkedin.com/pulse/eu-ai-act-unfair-smaller-companies-startups-thomas-schmalfeld-spn7f/ (date of access: 24.03.2025).

The «SolarWinds» breach exposed critical weaknesses in supply chains, compromising national sovereignty by leaving infrastructure vulnerable to external threats. As P. A. Sharikov and N. V. Stepanova contend, resolving such vulnerabilities demands not merely technical interventions but also structured international collaboration to address cross-border risks [10, p. 77–82].

In 2020, the Court of Justice of the European Union revoked the EU–US Privacy shield framework through its Schrems II judgment, citing inadequate protections against US surveillance programmes under legislation such as the Foreign intelligence surveillance act. This landmark judgment accentuated tensions between GDPR's stringent privacy requirements and transatlantic data flows crucial for global commerce [14, p. 194–195].

The ruling precipitated substantial economic repercussions: association «DigitalEurope» reported 1.3 bln euro in losses during 2022 alone, attributing these to ambiguities surrounding Standard contractual clauses and GDPR-compliant transfer mechanisms[26]. Smaller firms faced heightened burdens, struggling to evaluate extraterritorial legal regimes and implement safeguards, thereby intensifying economic pressures.

N. A. Molchanov and E. K. Matevosova critique Schrems II judgment for exacerbating regulatory uncertainty by dismantling Privacy shield without proposing viable substitutes. Businesses now face the arduous task of evaluating data protection standards in recipient countries on an individual basis a process both legally ambiguous and prohibitively costly [15, p. 100–101]. Such fragmentation hinders the formulation of coherent international data governance norms.

The Trump administration's suspension of the Privacy and Civil Liberties Oversight Board, which oversees adherence to data agreements, further endangered the EU–US data transfer framework. This policy shift heightened prospects of the agreement's annulment[27], prompting European states to pursue strategic autonomy initiatives aimed at reducing reliance on US technology and data infrastructure.

These developments prompted the EU to establish autonomous data storage standards and infrastructure, reducing reliance on American technology firms. The Trump administration's stance amplified the trend towards data localisation, with EU member states enacting stricter legislation mandating that sensitive data be held within national jurisdictions. This legislative push responded to anxieties over US government access to information via mechanisms embedded in instruments such as the Foreign intelligence surveillance act.

A. Yu. Olimpiev and I. A. Strelnikova [9] argue that the Schrems II judgment epitomises the clash between Europe's normative approach to data governance and the US' security-oriented pragmatism. Though the judgment underscores the EU's prioritisation of privacy, it risks weakening transatlantic collaborative mechanisms essential to countering shared cyber threats [10, p. 79–81].

Conclusions

Despite enduring policy divides (protective regulation versus security-focused pragmatism) the EU and the US may find common ground as geopolitical challenges mount. Hybrid models combining regulatory frameworks with strategic alliances could emerge as pragmatic solutions bridging ideological divides.

Advancements in disruptive technologies like quantum computing and IoT will strain existing notions of digital sovereignty, demanding policies that reconcile technological innovation with cybersecurity imperatives. The ability of these technologies to reshape the digital landscape and upend established power structures further exacerbates the need for such policies.

Although ideological rifts over privacy-security trade-offs persist, the EU and the US may develop fragmented but interoperable governance systems to address mutual geopolitical risks. As digital interdependence grows, collaborative frameworks will prove vital to safeguarding ecosystem stability. Successfully addressing this intricate and evolving environment demands a careful reconciliation of national priorities with international cooperation.

Recent US policy shifts under the Trump administration have deepened transatlantic tensions regarding information sovereignty. The EU's drive to decouple from American technological infrastructure could hinder future cooperation, potentially fragmenting digital ecosystems and raising barriers for enterprises operating across the Atlantic. As the digital environment continues to evolve, the need for cooperative and adaptive governance will become ever more critical for safeguarding the stability and resilience of the transatlantic digital ecosystem.

The analysis of EU and the US digital sovereignty strategies demonstrates fundamental differences in approaches to data regulation and cybersecurity. For Belarus, facing the consequences of a liberal personal data protection regime and the rise of cyber fraud, this experience offers valuable lessons. Balanced borrowing of elements of the European regulatory model and American pragmatism can become the basis for building an effective information security system.

EU and US experience demonstrates that an effective digital sovereignty policy requires a combination of

[26]Schrems II impact survey report [Electronic resource]. URL: https://www.digitaleurope.org/resources/schrems-ii-impact-survey-report/ (date of access: 24.03.2025).

[27]Trump takes aim at «overseas extortion» of American tech companies [Electronic resource]. URL: https://www.iss.europa.eu/publications/commentary/trump-takes-aim-overseas-extortion-american-tech-companies-eu-us-rift (date of access: 24.03.2025).

regulatory rigor and technological flexibility. The following action are critical for Belarus:

• to avoid the extremes of over-regulation (as in GDPR) and market anarchism (as in the early US model);

• to invest in national technological competencies, reducing dependence on foreign software;

• to establish an interagency cyber-reserve system for rapid incident response.

The key lesson for Belarus is that digital sovereignty is not achieved through isolation, but through a strategic balance of openness and protection of national interests.

References

1. Dobner P, Loughlin M, editors. *The twilight of constitutionalism?* Oxford: Oxford University Press; 2018. 352 p. DOI: 10.1093/acprof:oso/9780199585007.001.0001.

2. Metakides G. A crucial decade for European digital sovereignty. In: Werner H, Prem E, Lee EA, Ghezzi C, editors. *Perspectives on digital humanism*. Berlin: Springer; 2022. p. 219–225. DOI: 10.1007/978-3-030-86144-5.

3. Benyusz A, Hulko G, editors. *Digital sovereignty in Central & Eastern Europe*. Budapest: Hungarian Academy of Sciences; 2021. 286 p.

4. Bradford A. *The Brussels effect: how the European Union rules the world*. Oxford: Oxford University Press; 2020. 404 p. DOI: 10.1093/oso/9780190088583.001.0001.

5. Roberts H, Cowls J, Morley J, Taddeo M, Wang V, Floridi L. Safeguarding European values with digital sovereignty: an analysis of statements and policies. *Internet Policy Review.* 2021;10(3):1575. DOI: 10.14763/2021.3.1575.

6. Kavanagh C, Sheldon JB, editors. *Cybersecurity sovereignty and US foreign policy*. New York: National Committee on American Foreign Policy Report; 2014. 23 p.

7. Goldsmith JL. Against cyberanarchy. *University Chicago Law Review.* 1998;65(4):1199–1250. DOI: 10.2307/1600262.

8. Шевченко ЯН. Цифровой суверенитет Европы в контексте политики глобального управления данными. *Политическая наука*. 2021;3:251–270. DOI: 10.31249/poln/2021.03.11.

9. Олимпиев АЮ, Стрельникова ИА. Проблемы международного права в области киберпространства и цифрового суверенитета на европейском и азиатском пространстве. *Информационное общество.* 2021;2:74–87.

10. Шариков ПА, Степанова НВ. Подходы США, ЕС и России к проблеме информационной политики. *Современная Европа*. 2019;2:73–84.

11. Huang MJ, Tsou YL, Lee SC. Integrating fuzzy data mining and fuzzy artificial neural networks for discovering implicit knowledge. *Knowledge-based Systems*. 2006;19(6):396–403. DOI: 10.1016/j.knosys.2006.04.003.

12. Fahey E. The evolution of EU–US cybersecurity law and policy: on drivers of convergence. *Journal of European Integration*. 2024;46(7):1073–1088. DOI: 10.1080/07036337.2024.2411240.

13. Mercer ST. The limitations of European data protection as a model for Global privacy regulation. *AJIL Unbound*. 2020;114:20–25. DOI: 10.1017/aju.2019.83.

14. Steinke G. Data privacy approaches from US and EU perspectives. *Telematics and Informatics*. 2002:19(2)193–199. DOI: 10.1016/S0736-5853(01)00013-2.

15. Молчанов НА, Матевосова ЕК. Информационный терроризм в международно-правовом контексте. *Вестник Университета имени О. Е. Кутафина*. 2018;5:94–103. DOI: 10.17803/2311-5998.2018.45.5.094-103.

Received by editorial board 01.04.2025.