УДК 004.056:34

Ван Синьюй

Магистр

Белорусский государственный университет

Минск, Беларусь

ПРАВО КИБЕРБЕЗОПАСНОСТИ В КОНТЕКСТЕ ГЛОБАЛЬНОЙ ЦИФРОВИЗАЦИИ: ОТ ПРЕВЕНТИВНОГО РЕГУЛИРОВАНИЯ К ПРАВОВОЙ ЗАЩИТЕ ЦИФРОВЫХ ПРАВ

Аннотация: В статье исследуется эволюция правовых подходов к кибербезопасности в условиях глобальной цифровизации, фокусируясь на переходе от превентивного регулирования к защите цифровых прав. Автор анализирует противоречия между необходимостью обеспечения коллективной безопасности и защитой индивидуальных свобод, подчеркивая недостаточность традиционных механизмов, ориентированных на постфактум-реагирование. Особое внимание уделяется теоретическим основам кибербезопасности, включая защиту данных, критической инфраструктуры и борьбу с киберпреступностью, а также интеграции цифровых прав в правовые рамки. Исследование выделяет вызовы гармонизации превентивных мер с правами человека, такие как риск усиления государственного контроля и фрагментации интернета. Предлагается дуалистический подход: на национальном уровне — внедрение принципов пропорциональности и необходимости, на международном — развитие консенсусных норм через мягкое право . В контексте России подчеркивается баланс между цифровым суверенитетом и глобальным взаимодействием. Статья аргументирует, что устойчивая кибербезопасность требует синтеза технических, этических и правовых аспектов, трансформируя закон в инструмент социальной справедливости.

Ключевые слова: Кибербезопасность, Глобальная Цифровизация, Превентивное Регулирование, Цифровые Права, Правовая Защита,

Wang Xinyu
Master
Belarusian State University
Minsk, Belarus

Cybersecurity Law in the Context of Global Digitalization: From Preventive Regulation to Legal Protection of Digital Rights

Abstract: The article examines the evolution of legal approaches to cybersecurity in the context of global digitalization, focusing on the transition from preventive regulation to the protection of digital rights. The author analyzes the contradictions between the need to ensure collective security and the protection of individual freedoms, emphasizing the inadequacy of traditional mechanisms focused on post-factum response. Particular attention is paid to the theoretical foundations of cybersecurity, including the protection of data, critical infrastructure and the fight against cybercrime, as well as the integration of digital rights into the legal framework. The study highlights the challenges of harmonizing preventive measures with human rights, such as the risk of increasing state control and fragmentation of the Internet. A dualistic approach is proposed: at the national level the implementation of the principles of proportionality and necessity, at the international level the development of consensus norms through soft law. In the context of Russia, a balance is emphasized between digital sovereignty and global interaction. The article argues that sustainable cybersecurity requires a synthesis of technical, ethical and legal aspects, transforming the law into an instrument of social justice.

Keywords: Cybersecurity, Global Digitalization, Preventive Regulation, Digital Rights, Legal Protection, International Harmonization.

Introduction

The rapid advancement of global digitalization has fundamentally transformed socio economic structures, governance models, and individual interactions,

necessitating a parallel evolution in legal frameworks to address emerging challenges. This shift has elevated cybersecurity law from a niche regulatory concern to a cornerstone of transnational legal discourse, particularly as digital infrastructures become increasingly interdependent. The escalating frequency and sophistication of cyber threat sranging from data breaches to state sponsored attack sunderscore the inadequacy of traditional legal mechanisms in safeguarding both collective security and individual rights.[1] Consequently, the field now demands a critical reassessment of its foundational principles, moving beyond reactive measures toward a more dynamic integration of preventive regulation and digital rights protection.

A significant gap persists in current legal scholarship, which often treats cybersecurity law and digital rights as distinct domains rather than interconnected elements of a unified framework. While preventive regulation remains essential in mitigating systemic risks, its predominant focus on compliance and punitive measures frequently neglects the broader imperative of embedding fundamental rights within digital governance. This oversight becomes increasingly untenable as technologies such as artificial intelligence and the Internet of Things blur the boundaries between public security and private autonomy. The present study seeks to bridge this divide by interrogating how legal systems can reconcile the imperative of cybersecurity with the protection of digital rights, thereby fostering a more equitable and sustainable digital ecosystem.

Methodologically, this analysis adopts a doctrinal and comparative approach, examining normative developments across key jurisdictions to identify convergent principles and persistent contradictions. By synthesizing theoretical insights from legal philosophy, international law, and digital governance, the study aims to construct a coherent paradigm that transcends conventional binaries between security and liberty. The analysis deliberately avoids empirical case studies to prioritize conceptual clarity, aligning with the Russian academic tradition of emphasizing theoretical rigor in legal scholarship. In doing so, it contributes to a growing body of

research that redefines cybersecurity law not merely as a technical discipline but as a vital instrument of social justice in the digital age.

This introduction sets the stage for a systematic exploration of the transition from preventive regulation to rights-based governance, arguing that the future of cybersecurity law lies in its ability to harmonize these ostensibly competing imperatives. The subsequent sections will elaborate on this thesis through a structured examination of legal doctrines, regulatory mechanisms, and emerging rights frameworks, ultimately proposing a recalibrated approach for policymakers and scholars alike.

Theoretical Foundations of Cybersecurity Law

The conceptualization of cybersecurity law necessitates a precise delineation of its scope, which encompasses three principal dimensions: data protection, critical infrastructure security, and the legal response to cybercrime. Data protection frameworks establish safeguards for personal and sensitive information, balancing individual privacy against state and corporate interests. Critical infrastructure regulation addresses vulnerabilities in essential services energy, finance, and telecommunications where breaches could precipitate systemic disruptions. Cybercrime legislation, meanwhile, defines punitive measures for malicious activities, though jurisdictional ambiguities often complicate enforcement in transnational contexts.[2] These interconnected domains collectively form the structural basis of cybersecurity law, reflecting its dual role as both a protective mechanism and a facilitator of digital governance.

The evolution of cybersecurity law mirrors the broader trajectory of digital transformation, marked by a gradual shift from reactive legal measures to anticipatory regulatory paradigms. Early approaches prioritized post incident remediation, but the escalating scale and complexity of cyber threats have rendered such models insufficient. Contemporary legal theory increasingly emphasizes proactive governance, integrating risk assessment, mandatory compliance standards,

and public private cooperation into regulatory frameworks. This transition underscores the field's growing alignment with principles of preventive jurisprudence, wherein legal norms are designed not merely to punish violations but to preempt them.[3] Yet, this paradigm remains contested, as critics argue that an overreliance on preventive measures risks marginalizing fundamental rights in favor of security imperatives a tension that subsequent sections will examine in depth.

Preventive Regulation: Mechanisms and Challenges

The architecture of preventive regulation in cybersecurity law is predicated on a suite of mechanisms designed to anticipate and neutralize digital risks before they materialize. Central to this framework are risk assessment mandates, which compel organizations to systematically identify vulnerabilities and implement preemptive safeguards. These obligations are reinforced by compliance requirements modeled after influential regimes such as the EU's General Data Protection Regulation (GDPR), which institutionalize accountability through stringent data handling protocols and breach notification procedures. Such tools reflect a growing consensus that cybersecurity cannot rely solely on post hoc remedies but must instead embed resilience into the design of digital systems.[4] By prioritizing proactive governance, these mechanisms aim to align legal norms with the dynamic nature of cyber threats, fostering a culture of continuous risk management across public and private sectors.Yet the preventive paradigm is not without inherent contradictions. Its operationalization often privileges the interests of states and corporations, framing security as a technical challenge to be resolved through centralized control rather than a sociopolitical issue requiring democratic deliberation. For instance, compliance frameworks, while ostensibly universal, frequently impose disproportionate burdens on smaller entities, exacerbating market consolidation under large technology firms. Moreover, the emphasis on preemptive measures risks legitimizing expansive surveillance and data collection practices, ostensibly justified as necessary for threat detection but functionally eroding individual privacy and autonomy. This tension is

exacerbated by the lack of robust safeguards to ensure that preventive powers are exercised proportionally, leaving room for arbitrariness in enforcement.

The limitations of prevention-centric models thus reveal a fundamental misalignment between regulatory objectives and the protection of digital rights. While preventive mechanisms address systemic vulnerabilities, they often subordinate individual freedoms to collective security imperatives, neglecting the ethical dimensions of digital governance. This critique underscores the necessity of reorienting cybersecurity law toward a more inclusive paradigm one that integrates preventive rigor with enforceable rights guarantees, ensuring that security measures do not become instruments of control but rather enablers of equitable digital participation. Such a recalibration demands not only doctrinal innovation but also a reevaluation of the philosophical foundations underpinning contemporary regulatory practices.

Digital Rights as a Legal Paradigm

The recognition of digital rights as a distinct legal paradigm marks a pivotal shift in contemporary jurisprudence, reflecting the need to address the asymmetries of power inherent in digital ecosystems. At its core, this paradigm encompasses four interrelated principles: privacy, data sovereignty, algorithmic transparency, and access equity. Privacy, traditionally rooted in the protection of personal autonomy, now extends to safeguarding digital identities against unauthorized surveillance and data exploitation. Data sovereignty, a concept gaining prominence in an era of cross border data flows, asserts jurisdictional control over data generated within national boundaries, challenging the hegemony of transnational corporations and foreign states. Algorithmic transparency demands accountability in automated decision making systems, ensuring that their operations align with ethical norms and legal standards. Access equity, meanwhile, seeks to eliminate digital divides by guaranteeing universal availability of essential services, thereby framing connectivity as a precondition for exercising citizenship in the 21st century.Integrating these rights

into cybersecurity frameworks requires a deliberate reorientation of legislative priorities toward human-centric design. The European Union's Digital Rights Principles exemplify this approach, embedding fundamental freedoms into the architecture of digital governance rather than treating them as ancillary considerations. Such frameworks recognize that cybersecurity cannot be divorced from the broader sociopolitical context in which technologies operate; securing digital infrastructures must simultaneously empower individuals and constrain arbitrary exercises of power.[5] For instance, privacy-preserving technologies like end-to-end encryption are increasingly framed not merely as tools for data protection but as enablers of democratic participation. Similarly, data localization laws, while contentious, underscore the imperative of aligning data governance with national legal and cultural values a principle resonant with Russia's emphasis on digital sovereignty in its strategic policymaking.

The challenge lies in reconciling these rights with the functional demands of cybersecurity. Algorithmic transparency, while vital for mitigating biases in AI-driven systems, may conflict with proprietary interests and trade secrecy protections. Likewise, stringent data sovereignty measures risk fragmenting the global internet, complicating international cooperation against cyber threats. These tensions reveal a deeper philosophical dilemma: whether digital rights should be construed as absolute entitlements or balanced against collective security imperatives. Legal systems adopting a human-centric approach increasingly favor the former, positing that rights protections constitute the foundation of legitimate governance rather than a constraint on efficiency. This perspective aligns with Russia's evolving discourse on digital law, which emphasizes state sovereignty and cultural specificity while cautiously engaging with global norms.

Critically, the digital rights paradigm compels a reevaluation of the role of law in mediating technological progress. By embedding ethical considerations into regulatory frameworks, it transcends instrumentalist views of cybersecurity as a

technical discipline, repositioning it as a vehicle for social justice. This necessitates not only doctrinal innovation but also institutional reforms, such as establishing independent oversight bodies to audit compliance with transparency mandates and adjudicate disputes over data misuse. The paradigm's ultimate strength lies in its capacity to harmonize individual agency with systemic resilience, ensuring that cybersecurity law evolves from a reactive shield against threats into a proactive guarantor of digital dignity. As states navigate the complexities of global digitalization, this rights-based approach offers a coherent blueprint for aligning legal norms with the transformative potential and risks of the digital age.

Synthesizing Prevention and Rights Protection

The harmonization of preventive cybersecurity measures with digital rights protection demands a principled equilibrium between collective security imperatives and individual liberties. Central to this balance is the legal doctrine of proportionality, which requires that regulatory interventions minimally infringe upon fundamental rights while achieving legitimate security objectives. Necessity tests further constrain overreach by mandating that measures adopted are the least intrusive means available. These juridical tools, rooted in constitutional traditions, have gained traction in cybersecurity law as states grapple with dilemmas such as encryption backdoors or mass data retention. However, their application remains uneven, reflecting divergent cultural and political valuations of privacy versus security. In jurisdictions prioritizing state sovereignty, proportionality assessments often tilt toward security rationales, whereas rights centric frameworks, such as those emerging in the EU, impose stricter scrutiny on surveillance powers.[6] This disparity underscores the absence of universal standards for reconciling these competing values, leaving the equilibrium vulnerable to geopolitical and ideological influences.

Global harmonization efforts face profound challenges due to the tension between soft law instruments and binding legal regimes. Initiatives led by the United Nations and OECD, such as voluntary guidelines on responsible state behavior in cyberspace,

promote shared norms without enforcing compliance. While such instruments foster dialogue among states with divergent legal traditions, their non-binding nature limits their efficacy in resolving disputes over extraterritorial data access or cyber-espionage. Conversely, hard law frameworks, including regional agreements like the Budapest Convention, struggle to achieve consensus among major powers, particularly where digital sovereignty claims clash with transnational governance models. Russia's advocacy for multilateral internet governance under UN auspices exemplifies this tension, emphasizing state control over digital infrastructures as a counterweight to Western-dominated regulatory paradigms.

The synthesis of prevention and rights protection thus necessitates a dual-track approach: domestically, embedding proportionality into legislative design to prevent security measures from devolving into tools of oppression; internationally, cultivating interoperable norms through incremental consensus-building. This requires acknowledging that cybersecurity is not a zero sum contest between states and individuals but a layered governance challenge. Legal frameworks must evolve to address emerging technologies like quantum computing and AI-driven cyberweapons, which will exacerbate existing asymmetries. Crucially, the legitimacy of cybersecurity law hinges on its capacity to demonstrate that preventive mechanisms enhance, rather than erode, the social contract in digital spaces. For Russia, this entails navigating its unique position as both a proponent of digital sovereignty and a participant in global cyber diplomacy a balance that will test its ability to reconcile national security priorities with the cross-border nature of digital rights. Ultimately, the path forward lies in reimagining cybersecurity not as a domain of conflict between prevention and rights but as a dynamic field where both are mutually constitutive elements of sustainable digital order.

Conclusion

The transition from preventive regulation to rights-based approaches in cybersecurity law reflects a paradigm shift necessitated by the evolving

sociotechnical realities of global digitalization. Traditional models, anchored in risk mitigation and compliance, have proven inadequate in addressing the dual imperatives of safeguarding collective security and upholding individual freedoms. The ascendancy of digital rights encompassing privacy, algorithmic accountability, and equitable access signals a recognition that legal frameworks must transcend technical governance to embody ethical and democratic principles. This reorientation challenges the primacy of state and corporate interests, positing that cybersecurity's legitimacy hinges on its capacity to protect, rather than restrict, digital citizenship.

Future legal developments must prioritize adaptive frameworks capable of anticipating disruptions wrought by emerging technologies such as artificial intelligence and the Internet of Things. These technologies amplify both vulnerabilities and asymmetries of power, demanding regulations that are both agile and principled. For instance, AI-driven surveillance systems necessitate strict adherence to proportionality tests to prevent rights erosion under the guise of security. Similarly, IoT ecosystems require interoperability standards that harmonize innovation with data sovereignty protections. Such efforts must be underpinned by a dynamic understanding of law as an evolving dialogue between technological possibilities and societal values.

References

1. Fuster G G, Jasmontaite L. Cybersecurity regulation in the European union: the digital, the critical and fundamental rights // The ethics of cybersecurity. 2020. Pp. 97–115.

2. Yesimov S, Borovikova V. Methodological foundations of information security research // Social and Legal Studios. 2023. T. 6. № 1. Pp. 49–55.

3. Dion M.Cybersecurity policy and theory // Theoretical Foundations of Homeland Security. Routledge, 2020. Pp. 257–284.

4. Bechara F R, Schuch S B.Cybersecurity and global regulatory challenges // Journal of Financial Crime. 2021. T. 28. № 2. Pp. 359–374.

5. Ruiz J M G. The Paradigma of legal science in a global digital society // Revista de Direitos e Garantias Fundamentais. 2021. T. 22. № 2. Pp. 9–40.

6. Pashentsev D A. Legal behavior under the technological paradigm change and modern social transformations // Vestnik Saint Petersburg UL. 2022. Pp. 810.