UDC 341.1:004
DOI: https://doi.org/10.31861/jiel.2026.2.18-31

Svitlana Karvatska,
Doctor of Law, Professor,
Acting Head of the Department of
International Law and Comparative Law,
Yuriy Fedkovych Chernivtsi National University,
Ukraine
e-mail : s.karvatska@chnu.edu.ua
ORCID: https://orcid.org/0000-0001-9948-4866

Aurora Ciuca,
Professor, PhD,
Ștefan cel Mare University
Faculty of Law and Administrative Sciences, Romania
E-mail: aurora_ciuca_2000@yahoo.com

DIGITALIZATION OF THE INTERNATIONAL LEGAL SPHERE: SYSTEMIC CHALLENGES AND PROSPECTS FOR THE EVOLUTION OF INTERNATIONAL LAW

This article examines the digital transformation of international law as a multidimensional process of rethinking traditional mechanisms of international interaction. It is argued that the penetration of digital technologies into the sphere of international legal regulation leads not only to the emergence of new objects of legal protection but also to the transformation of established approaches to determining state jurisdiction, enforcing international responsibility, and ensuring compliance with international obligations.

The paper identifies the key challenges of the digital age for international law, including the fragmentation of international regulation of the digital environment, the asymmetry of states' technological capabilities, the complexity of establishing liability for cross-border digital offenses, and the need to harmonize cybersecurity requirements with international human rights standards. The study emphasizes that the effectiveness of international legal regulation increasingly depends on the ability of international institutions and states to ensure the interaction of universal legal principles with flexible mechanisms for responding to technological risks without undermining guarantees of human rights, state sovereignty, and international security.

Promising directions for legal development are outlined, including the improvement of international standards for digital governance, the formation of coordinated approaches to international legal liability for the use of digital technologies, the strengthening of international cooperation in the field of cybersecurity, and the development of regulatory mechanisms to oversee the use of artificial intelligence. The paper demonstrates the advisability of transitioning from a piecemeal response to individual technological threats to a systematic model of international legal regulation based on the principles of coherence and respect for fundamental human rights. It is concluded that the digital transformation of international law represents not only a technology-driven challenge but also an opportunity to renew its normative potential, institutional capacity, and instruments for ensuring the international legal order in the context of global digital interdependence.

Keywords: *digital transformation of international law, human rights, international legal order, international legal responsibility, digital rights, artificial intelligence, international cooperation in the field of cybersecurity.*

ISSN 3083-7979

Карвацька Світлана, Чука Аурора. Цифровізація міжнародно-правового простору: системні виклики та перспективи еволюції міжнародного права.

У статті досліджено цифрову трансформацію міжнародного права як багатовимірний процес переосмислення традиційних механізмів міжнародної взаємодії. Обґрунтовано, що проникнення цифрових технологій у сферу міжнародно-правового регулювання зумовлює не лише появу нових об'єктів правового захисту, а й трансформацію усталених підходів до визначення юрисдикції держав, реалізації міжнародної відповідальності та забезпечення дотримання міжнародних зобов'язань.

Визначено ключові виклики цифрової епохи для міжнародного права, серед яких фрагментарність міжнародного регулювання цифрового середовища, асиметрія технологічних можливостей держав, складність встановлення відповідальності за транскордонні цифрові правопорушення, а також необхідність узгодження вимог кібербезпеки із міжнародними стандартами захисту прав людини. Акцентовано на тому, що ефективність міжнародно-правового регулювання дедалі більше залежить від здатності міжнародних інституцій і держав забезпечувати взаємодію універсальних правових принципів із гнучкими механізмами реагування на технологічні ризики без послаблення гарантій прав людини, державного суверенітету та міжнародної безпеки.

Сформульовано перспективні напрями правового розвитку, що передбачають удосконалення міжнародних стандартів цифрового врядування, формування узгоджених підходів до міжнародно-правової відповідальності за використання цифрових технологій, посилення міжнародного співробітництва у сфері кібербезпеки та розроблення нормативних механізмів контролю за застосуванням штучного інтелекту. Доведено доцільність переходу від фрагментарного реагування на окремі технологічні загрози до системної моделі міжнародно-правового регулювання, заснованої на принципах узгодженості та поваги до фундаментальних прав людини. Зроблено висновок, що цифрова трансформація міжнародного права становить не лише технологічно зумовлений виклик, а й можливість оновлення його нормативного потенціалу, інституційної спроможності та інструментів забезпечення міжнародного правопорядку в умовах глобальної цифрової взаємозалежності.

Ключові слова: *цифрова трансформація міжнародного права, права людини, міжнародний правопорядок, міжнародно-правова відповідальність, цифрові права, штучний інтелект, міжнародне співробітництво у сфері кібербезпеки.*

Introduction. The digital transformation of the international legal sphere is generating conditions for a fundamental reconsideration of the nature of international law and the mechanisms through which it operates. Its implications extend beyond the implementation of existing legal provisions, affecting the processes through which legal norms are formulated, interpreted, and applied in practice. In doing so, digitalisation is reshaping established conceptions of the role and function of law within the system of international relations. The magnitude of these changes calls for comprehensive theoretical inquiry aimed at identifying structural developments within the international legal order and elucidating the patterns emerging from the integration of digital technologies into the legal domain.

An examination of this subject requires a systemic analytical framework capable of revealing overarching patterns in the digital evolution of international law beyond the confines of individual legal regimes. This approach involves synthesising findings from specialised academic studies, critically comparing their conclusions, and identifying

interrelationships among the various ways in which technological developments affect international legal regulation. Its methodological significance lies in facilitating a transition from the examination of discrete technological challenges towards a broader explanation of the systemic transformation of international law as an integrated normative framework.

The objective of the article is to develop a comprehensive understanding of the transformation of international law under the influence of digital technologies by examining the evolving nature of international legal regulation, identifying the principal normative and institutional challenges arising from the digitalization of international relations, and determining prospective avenues for adapting international legal frameworks to emerging technological realities. Particular emphasis is placed on reassessing established legal approaches to state sovereignty, jurisdiction, international responsibility, cybersecurity, and the protection of fundamental human rights, with a view to substantiating the need for a coherent, adaptive, and internationally coordinated regulatory framework capable of safeguarding the stability of the international legal order amid accelerating technological change.

Literature Review. The digitalization of international relations has stimulated a growing body of legal scholarship concerned with the capacity of international law to respond to technological change while preserving its foundational principles and regulatory coherence. A central question within this debate is whether digital technologies merely expand the subject matter of existing legal norms or fundamentally alter the structures through which international law operates. Burchardt (2023) addresses this issue by investigating the structural implications of digitalization for the international legal order, while the edited volume Digital Transformations in Public International Law, by Golia, Kettemann, and Kunz, examines the broader consequences of technological developments for international legal institutions, normative processes, and governance arrangements. In addition, Osula, Kasper, and Kajander (2022) analyse the European Union's position on the applicability of international law in cyberspace. Collectively, these works demonstrate that digital transformation raises questions extending beyond the adoption of new technologies, particularly concerning the interpretation of established legal principles, the coordination of regulatory approaches, and the maintenance of international legal stability in an increasingly interconnected environment.

A further body of research investigates the legal consequences of digitalization within particular regulatory fields, including artificial intelligence, cybersecurity, financial technologies, human rights protection, and international criminal justice. Hughes (2020) analyses approaches to the regulation of blockchain-based currencies in the United States, highlighting the challenges involved in establishing appropriate legal responses to emerging financial technologies. Casarosa (2022) examines the relationship between AI regulation and cybersecurity certification in the European Union, emphasizing the importance of coordination between legal instruments addressing technological risks. Burchardt's (2022) conceptual analysis of legal space provides an additional theoretical perspective on the interaction between overlapping normative frameworks and multiple forms of legal authority. Within Ukrainian legal scholarship, A. Labyk (2025) and I. Zakharchuk (2025) explore the implications of digitalization for international human rights law and the development of emerging categories of rights, while S. Karvatska, A. Manyk, and M. Stroich (2025) investigate contemporary cybersecurity challenges and international legal approaches to data protection. S. Karvatska and M. Hrushko (2026) extend this discussion to the evidentiary dimension of international criminal proceedings by examining the legal foundations and practical challenges associated with digital evidence in the

ISSN 3083-7979

prosecution of war crimes. Although these studies provide valuable insights into distinct aspects of digital transformation, the interaction between technological innovation, international legal responsibility, regulatory fragmentation, and institutional adaptation warrants further integrated examination. Against this background, the present article seeks to establish a comprehensive analytical perspective on the principal challenges confronting international law in the digital era and to identify regulatory and institutional pathways capable of strengthening the coherence, adaptability, and effectiveness of the international legal framework.

Results and Discussion. To assess the nature and scope of these developments, an analytical framework may be employed that encompasses three interrelated dimensions: the subjects of international law, the body of applicable legal norms, and the underlying values of the international legal order. The subject-related dimension makes it possible to examine changes in the composition of participants in international relations, their capacity to influence law-making processes, and the evolving patterns of interaction among states, international organisations, and other actors operating in digital environments. The normative dimension focuses on changes in the processes through which international legal rules are formulated, interpreted, and implemented. The value-based dimension, in turn, enables an assessment of how digitalisation reshapes the priorities of international legal regulation, the balance between competing legal interests, and the fundamental principles guiding the further development of international law.

The systematic application of this analytical framework involves several successive stages. The first entails establishing the theoretical and methodological foundations of the inquiry, clarifying its principal concepts, and defining the criteria for assessing the structural implications of digitalisation for international law. The second stage consists of organising the identified transformations into distinct analytical categories on the basis of the conceptual framework developed, followed by an examination of the relationships between them. This methodological sequence makes it possible not only to classify the consequences of digitalisation but also to explain their significance for the internal structure of international law, the mechanisms governing its operation, and the prospects for its future evolution.

Accordingly, an examination of the structural implications of digitalisation for international law requires an integrated approach that brings together the analysis of changes affecting legal subjects, the evolution of normative mechanisms, and the reconfiguration of underlying value orientations. The interaction between these dimensions provides a comprehensive basis for understanding how digital technologies are transforming not merely individual instruments of legal regulation but also the broader conditions under which international law operates as a system designed to govern international relations and uphold shared legal values [1].

The fundamental values underpinning international law constitute the third analytical dimension necessary for understanding the systemic implications of digital transformation. The integration of digital technologies may not only bring renewed attention to the compatibility of established international legal values with emerging social realities but also contribute to the emergence of new normative priorities. Against this background, it is essential to examine how the value orientations of subjects of international law are evolving, under what circumstances such changes occur, and which values acquire particular significance for different participants in international relations.

A distinct strand of inquiry concerns the identification of the underlying value commitments reflected in international and domestic legal instruments governing the

ISSN 3083-7979

digital environment. This involves examining the principles and priorities embedded in the relevant regulatory frameworks, while also identifying established foundations of international law whose implementation is being reconsidered or challenged by technological developments. Such an approach makes it possible to determine whether the regulation of digitalisation continues to reproduce the established system of international legal values or instead creates conditions conducive to its gradual transformation. However, the value dimension of digitalisation cannot be adequately explored through an examination of legal provisions alone. It also requires critical reflection on the purpose and function of international law in an environment characterised by technological change. Digital developments may prompt a reassessment of the objectives pursued by international legal regulation, the priorities it establishes, and the means through which its intended outcomes are achieved. Consequently, changing perceptions of the proper role of international law may influence the evolution of regulatory mechanisms, the definition of matters falling within the scope of legal regulation, and the development of new approaches to addressing international challenges.

In this regard, values should be examined through two interrelated perspectives: first, as factors shaping the formulation, interpretation, and evolution of international legal rules; and second, as an integral element of the broader discourse of international law within which the legality, legitimacy, and acceptability of particular decisions are assessed. From this perspective, the concept of values encompasses normatively significant reference points to which relevant actors attach particular importance and which they invoke to justify the substance and orientation of legal regulation. This understanding extends beyond purely ethical or moral considerations, treating values more broadly as determinants of normative priorities and factors influencing the development of legal institutions.

To facilitate a systematic examination of these processes, an analytical framework is employed that centres on the interrelationship between three fundamental structural dimensions of international law. The first concerns the composition of the actors involved in legal interactions and the changing characteristics of those participants. The second addresses the essential attributes of international legal norms, including the processes through which they are established, their substantive content, and the ways in which they operate. The third focuses on changes in the fundamental values that shape normative priorities and determine the overall orientation of international legal regulation. Considered collectively, these dimensions provide a basis for assessing how digitalisation affects the structural foundations of international law and whether it creates conditions for a more comprehensive reassessment of its underlying principles and systemic organisation [2].

The values underpinning international law do not necessarily require explicit incorporation into every individual legal rule. Their significance may instead be reflected in general principles, conceptual foundations, and shared normative reference points that provide a common basis for different branches of international law. It is precisely the cross-cutting nature of these values that makes it possible to assess the impact of digitalisation not merely on individual legal regimes but also on the coherence of the international legal order as a whole, particularly with regard to the relationship between established legal principles and the emerging demands of the digital age [1]. This study places particular emphasis on the implications of digitalisation for the structural organisation of the international legal system. Such an approach makes it possible to distinguish technology-driven transformations affecting international law in general from more limited developments confined to particular branches of law or specific legal institutions. Although adaptability and change are inherent features of law, the intensity, depth, and scope of these processes

may vary considerably. Some transformations affect only discrete elements of legal regulation, whereas others have the potential to reshape its fundamental attributes and alter the broader principles governing the operation of the legal system. Within this framework, the structural impact of digitalisation is understood as a set of developments affecting the core characteristics of international law that are essential to its overall functioning, irrespective of the particularities of individual legal branches. These characteristics pertain to the meta-level of the legal system, encompassing its general organisational, normative, and value-based parameters. Accordingly, the focus is placed less on the emergence of individual digital legal instruments than on the possibility that digitalisation may alter the underlying foundations that determine the nature of international law, the mechanisms through which it evolves, and the ways in which international relations are organised and regulated.

Structural transformations should not, however, be understood as instantaneous or necessarily completed developments. They may unfold incrementally, affect different components of the international legal system to varying degrees, and assume diverse forms. In some instances, digitalisation prompts a reassessment of a single structural feature; in others, it generates interconnected changes across several components simultaneously. Furthermore, the direction of these developments is not predetermined. Technological progress may reinforce established principles of international law, modify their substantive meaning, or create conditions for the emergence of new normative reference points. This calls for structural change to be examined as a multidimensional and evolving process rather than a linear trajectory leading to a predetermined outcome.

The complexity and multilayered nature of digital regulation are particularly evident in the European Union's regulatory framework governing data management, digital platforms, and cybersecurity. The EU's established and continuously evolving body of legislation encompasses a range of interconnected legal instruments, including the Digital Services Act (DSA), the Digital Markets Act (DMA), the Data Act, the Artificial Intelligence Act (AI Act), the General Data Protection Regulation (GDPR), and the Cybersecurity Act. Taken together, these instruments illustrate the EU's commitment to a comprehensive regulatory approach to the digital environment, in which personal data protection, digital platform accountability, the use of artificial intelligence, and the resilience of information infrastructure are closely interrelated and require a coherent legal framework [3].

Another significant consequence of the digital transformation of international law is the emergence of hybrid legal norms and regulatory spaces. This phenomenon arises where particular legal provisions, regulatory mechanisms, or normative approaches simultaneously belong to different legal systems or operate at the intersection of multiple regulatory frameworks. As a result, the traditional boundaries separating distinct legal regimes become less clearly defined, while the relationships between them grow increasingly complex. Hybridisation reflects a broader tendency towards the convergence and mutual penetration of different normative layers, whereby rules of international law, domestic legislation, and transnational regulatory mechanisms may jointly shape the legal conditions governing the operation of the digital environment [4].

The convergence of legal norms and regulatory frameworks represents another systemic consequence of the digital transformation of international law, contributing to the emergence of hybrid models of legal governance. These models are distinguished by the fact that particular normative provisions and regulatory mechanisms extend beyond the boundaries of a single legal system, incorporating elements that differ in origin and functional purpose. This interaction gradually weakens the traditional distinctions between

ISSN 3083-7979

separate legal regimes and increases the interdependence of different levels of normative regulation. Within the digital environment, this phenomenon is reflected in the interplay between principles of international law, domestic legislative provisions, and transnational regulatory practices, which collectively shape the rules governing the conduct of participants in digital relations. Hybridisation therefore illustrates the growing complexity of contemporary legal regulation and brings to the fore questions concerning normative consistency, the delimitation of competences, and the legal consequences arising from the concurrent application of different regulatory frameworks [1].

Under these circumstances, established approaches to documenting international wrongful acts, verifying the authenticity of digital information, and determining the criteria for attributing responsibility to subjects of international law are undergoing significant change. The rapid advancement of digital technologies is fundamentally reshaping the nature of international relations by introducing new mechanisms of interaction among states, international organisations, private entities, and individuals. As digital technologies become increasingly embedded in the activities of states, international organisations, judicial institutions, and other subjects of international law, conventional approaches to establishing legally relevant facts, exercising international oversight, assessing evidentiary material, and ensuring international accountability are being progressively reconfigured.

The digital transformation of international law has long since moved beyond the mere technological modernisation of international relations. It is increasingly emerging as a distinct trajectory in the evolution of the international legal order, influencing not only the implementation of international legal norms but also the reconsideration of their substantive content, underlying principles, and mechanisms of application. The integration of artificial intelligence, algorithmic analytical models, big data processing technologies, and digital information resources is giving rise to a new architecture for establishing legally relevant facts, evaluating evidence, and making decisions under international law. At the same time, digitalisation generates a range of new legal challenges concerning the status of digital information and the requirements governing its authenticity, provenance, integrity, admissibility, and evidentiary weight. Traditional categories of international law, developed primarily in contexts where physical or documentary evidence predominated, no longer fully accommodate the specific characteristics of digital environments, in which information may be generated, altered, disseminated, or processed by automated systems. Moreover, the widespread adoption of artificial intelligence underscores the need to develop contemporary international legal approaches to its regulation, including standards of transparency, accountability, and responsibility for the outcomes produced by intelligent digital systems.

These issues are particularly sensitive from a legal perspective in the context of international human rights protection. The deployment of algorithmic models may reproduce existing societal biases, intensify discriminatory practices, result in disproportionate interference with private life, and restrict individuals' ability to seek effective remedies for violations of their rights. Such risks arise not only from potential technological shortcomings but also from the characteristics of training datasets, the criteria underpinning algorithmic assessments, and the institutional circumstances in which these systems are deployed. Further challenges stem from the development of technologies capable of manipulating or generating digital content, thereby increasing the risk of fabricated evidence. The use of artificial intelligence tools and advanced image and video manipulation technologies consequently necessitates new approaches to the expert verification of digital information [5, с. 87-95].

ISSN 3083-7979

One of the most rapidly evolving areas of contemporary international law is the development of new standards governing the use of digital evidence by international judicial and quasi-judicial bodies. Armed conflicts, cyber operations, transnational criminal activity, and the widespread circulation of digital information have substantially expanded the range of electronic evidentiary sources. These include satellite imagery, open-source materials, social media content, digital databases, recordings generated by unmanned systems, and other forms of electronically stored information. In this context, particular importance attaches to the recognition of digital evidence under international law and to the establishment of safeguards ensuring its authenticity, reliability, integrity, and admissibility. Equally significant is the development of consistent approaches to the assessment of such evidence in international criminal proceedings, human rights protection mechanisms, and procedures concerning the international responsibility of states. Taken together, these developments point towards the emergence of a new paradigm in international legal scholarship, in which digital technologies serve not merely as an object of legal regulation but also as a driving force behind the further evolution of international law itself [6].

The influence of artificial intelligence on international law extends beyond the emergence of new objects of legal regulation to encompass the transformation of the mechanisms through which international legal norms are implemented and applied. The integration of algorithmic technologies into national and international security, intelligence operations, digital surveillance, personal identification, and the analytical processing of information raises important questions concerning the compatibility of automated procedures with the fundamental requirements of due process. These concerns become particularly significant where algorithmically generated assessments directly or indirectly shape decisions made by public authorities or international institutions. In such circumstances, there is a pressing need to establish clear limits on the use of technology-based recommendations, identify the actors responsible for the consequences of their application, and ensure that individuals have a genuine opportunity to challenge decisions made with the assistance of artificial intelligence systems.

From an international legal perspective, the delegation of certain analytical or procedural functions to automated systems does not, in itself, absolve states of their obligations to respect and protect human rights. The increasing virtualisation of social interactions, advances in artificial intelligence and biotechnology, the widespread use of big data, and the proliferation of online platforms are creating new challenges for the protection of human rights [7, c. 354]. On the contrary, the deployment of artificial intelligence requires appropriate risk assessments, transparency within the limits established by law, independent oversight, opportunities for human review, and access to effective remedies.

The expanding use of artificial intelligence is therefore driving structural changes in international law, raising questions not only about the adequacy of existing legal frameworks in addressing emerging technologies but also about the continued effectiveness of established legal safeguards in environments increasingly shaped by algorithmic decision-making. The use of statistical models, machine learning, and automated data processing calls for a reassessment of the relationship between technological efficiency, legal accountability, and procedural guarantees afforded to individuals. Against this background, contemporary international and regional regulatory initiatives are increasingly embracing risk-based approaches, appropriate human oversight of high-risk systems, and mechanisms designed to prevent human rights violations. The decisive criterion for determining the lawfulness of these technologies should not be their technical capabilities

ISSN 3083-7979

alone, but rather whether their deployment complies with the requirements of legality, necessity, proportionality, accountability, and effective legal protection. International cooperation in cybersecurity is progressively becoming an essential prerequisite for maintaining the stability of the global digital environment. The United Nations and the International Telecommunication Union recognise the importance of coordinating international efforts to counter cyber threats. Nevertheless, establishing a coherent global framework for cyberspace governance remains a complex and protracted undertaking. The work of the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UNGGE) has contributed to the development of normative guidance on responsible state behaviour in the use of information and communication technologies [8, c. 52].

The transnational character of cyber threats creates an inherent need for multilateral cooperation, as their prevention, detection, and mitigation frequently extend beyond the jurisdiction of any single state. International coordination is particularly important for the timely exchange of information concerning vulnerabilities and cyber incidents, the harmonisation of response mechanisms, the enhancement of technical interoperability between security systems, and the development of common approaches to risk assessment [9]. Nevertheless, the practical necessity of such cooperation does not automatically lead to the establishment of a unified regulatory framework. Reaching an international consensus remains difficult because states differ in their views on the permissible extent of governmental control over digital infrastructure, the protection of information sovereignty, the preservation of an open Internet, and the relationship between cybersecurity and human rights [10, c. 85].

A critical examination of existing mechanisms for global cybersecurity governance suggests that the challenges of international coordination cannot be attributed solely to institutional inertia or insufficient political trust. More fundamental tensions arise from structural limitations within the current system of international legal regulation. These include varying degrees of specificity in the rules governing responsible state behaviour, difficulties in establishing the factual circumstances surrounding cyber operations, and the absence of a universal mechanism for monitoring compliance with all agreed standards. Under these conditions, broader political endorsement of common principles, although significant, cannot by itself serve as a sufficient measure of the effectiveness of international regulation unless accompanied by an assessment of the practical capacity to ensure compliance with the relevant rules. Against this background, the development of coordinated international legal mechanisms has become particularly important, especially those designed to ensure the reliability of digital evidence while safeguarding fundamental human rights [5, c. 87].

Particular attention should be paid to the risk that states possessing substantial technological, economic, or military resources may use international cyber norms to advance their strategic objectives. In the absence of adequate oversight and accountability mechanisms, normative provisions may be interpreted selectively, invoked to legitimise particular political interests, or applied unevenly to different participants in international relations. Such practices risk turning global cybersecurity governance into an instrument of geopolitical influence rather than a framework designed to promote predictable and responsible state conduct. Consequently, the effectiveness of international cooperation depends not merely on the number of principles agreed upon, but also on the equitable application of those principles, the transparency of procedures for assessing violations, and the availability of effective mechanisms for establishing international responsibility.

ISSN 3083-7979

Addressing international challenges related to cybersecurity and data protection therefore requires a multidimensional approach that combines intergovernmental cooperation, the strengthening of technical and legal capacities, and the development of a global culture of cybersecurity [11, c. 255].

Concluding a universal legally binding treaty on cybersecurity remains a formidable challenge in the face of fundamental disagreements concerning digital sovereignty, the scope of state jurisdiction, and the permissible forms of control over cyberspace. Nevertheless, these difficulties do not preclude the gradual advancement of international legal regulation through the combined application of existing rules of international law, specialised treaty-based mechanisms, agreed standards of responsible conduct, and institutional frameworks for cooperation. A promising approach would involve a regulatory model in which technical coordination is complemented by more clearly defined legal obligations, transparent procedures for responding to violations, and safeguards ensuring respect for human rights. Such an approach avoids both the overly optimistic assumption that political consensus necessarily translates into effective regulation and the pessimistic conclusion that international legal agreement on cybersecurity is fundamentally unattainable. In light of these considerations, an appropriate response at the international level is required to facilitate the harmonisation of standards for the promotion and protection of human rights and to ensure a secure digital environment for everyone [12, c. 433].

To respond effectively to the challenges of digital transformation and realise its potential at both international and national levels, it is essential to strengthen mechanisms for digital interoperability among states. This requires the alignment of legal approaches, technical standards, and principles governing interaction within the digital environment to ensure the effective functioning of cross-border digital processes. A key priority in this regard is the development of a coherent set of global normative guidelines that takes into account differences in states' levels of economic development, political systems, and cultural traditions. Such an approach should reconcile the pursuit of universal standards for international digital regulation with respect for national particularities, thereby creating favourable conditions for more effective international cooperation, mutual recognition of legal frameworks, and the reduction of fragmentation within the digital space. As M. Khaustova emphasises, "a core set of rules entails the development of a global instrument that establishes principles and priorities for the dissemination of digital technologies, grounded in established international practice, with a view to ensuring their interoperability, preventing the fragmentation of the global digital space, and avoiding the emergence of digital «islands» [13, c. 14].

A comprehensive examination of the impact of strategic litigation on the evolution of public international law warrants separate scholarly investigation, as it extends beyond the scope of the present article. Despite growing academic interest in strategic litigation concerning human rights protection and other matters of significant public interest, its role in shaping international legal approaches to Internet governance and the protection of digital rights remains insufficiently systematised. This gap in the existing body of scholarship points to a promising avenue for further research, particularly with regard to determining how strategic litigation influences the interpretation of international legal norms, the development of human rights protection standards in digital environments, and the evolution of mechanisms governing international legal responsibility. At the same time, new human rights are emerging, while established rights are acquiring broader substantive dimensions. Both national and international legal frameworks increasingly address such

ISSN 3083-7979

rights and protections as access to the Internet, the protection of personal data online, the right to be forgotten, the right to a secure digital environment, protection against digital discrimination, and the right to digital identity, among others [7, с. 355].

An interdisciplinary examination of the interaction between law, digital technologies, and social processes, drawing in particular on research in the field of Internet and society studies, may provide a methodological foundation for further inquiry. This approach would make it possible to conceptualise strategic litigation not merely as a means of protecting individual or collective rights, but also as an instrument for developing legal standards capable of influencing the conduct of states, international organisations, and private digital platforms. Particular attention should be directed towards the ways in which judicial decisions contribute to clarifying the scope and substance of digital rights, defining the limits of permissible state interference, and strengthening safeguards for freedom of expression, privacy, and access to information in the digital environment. The dynamic nature of technological development continually reshapes both the subject matter and the methods of strategic litigation. The emergence of new digital services, algorithmic systems, and forms of cross-border interaction generates novel legal disputes while simultaneously expanding the opportunities to use judicial mechanisms in the pursuit of public interests. Under these circumstances, further research into strategic litigation concerning the Internet and digital rights offers considerable potential for advancing our understanding of the ongoing transformation of public international law and identifying prospects for its adaptation to the challenges of the digital age [14].

Conclusions. The digital transformation of the international legal order represents a systemic process involving changes in the ways international relations are normatively structured. This process extends beyond the mere adaptation of existing legal rules to technological innovations. Its defining characteristic lies in the emergence of new interdependencies between the fundamental principles of international law, digital technologies, and mechanisms of cross-border governance. The analysis demonstrates that the proliferation of artificial intelligence, algorithmic systems, digital communication infrastructures, and data-processing technologies necessitates a critical reassessment of established approaches to state sovereignty, jurisdiction, international responsibility, and the protection of human rights. Under these circumstances, the capacity of international law to maintain its regulatory effectiveness will depend not only on the comprehensiveness of the legal frameworks governing emerging social relations but also on the ability of its institutional mechanisms to respond to technological change while preserving fundamental legal principles and safeguards.

The principal challenge posed by digital transformation has been identified as the growing disparity between the global reach of technological processes and the fragmented nature of their regulation under international law. Divergent national approaches to digital governance, unequal access to technological resources, difficulties in identifying the parties responsible for cross-border violations, and the complexity of establishing causal relationships within digital environments all impede the development of coherent international standards of conduct. At the same time, regulatory adaptation must not be equated with the unrestricted expansion of state control over digital spaces, as such an approach may result in disproportionate interference with privacy, freedom of expression, and other fundamental rights. Accordingly, a forward-looking framework for international legal regulation should integrate technological adaptability with legal certainty, procedural transparency, the accountability of relevant actors, and effective safeguards for the protection of individuals.

ISSN 3083-7979

The principal priorities for the further evolution of international law include strengthening international cooperation in cybersecurity, refining mechanisms for establishing international legal responsibility for wrongful conduct in digital environments, developing harmonised standards for the use of artificial intelligence, and reinforcing the institutional foundations for the protection of digital rights. Particular importance should be attached to the development of a multilevel regulatory framework in which international treaties, general principles of law, institutional mechanisms for cooperation, and established practices of digital governance operate as complementary instruments. The value of this approach lies in its potential to reconcile the normative stability of international law with its capacity to address emerging technological challenges. Digital transformation should therefore be understood not as a force undermining the established international legal order, but as an impetus for its substantive renewal. Such renewal should ensure that technological progress is accompanied by stronger legal safeguards, enhanced international accountability, and a fair balance between the interests of states, society, and individuals.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Burchardt D. Does Digitalization Change International Law Structurally? German Law Journal. 2023; 24(3):438-460. URL: https://doi.org/10.1017/glj.2023.31(date of access: 13.10.2026).
2. Krieger Heike & Liese Andrea eds. Tracing Value Change in the International Legal Order – Perspectives from Legal and Political Science. 2023. Krieger, Heike, and Andrea Liese (eds), Tracing Value Change in the International Legal Order: Perspectives from Legal and Political Science (Oxford, 2023; online edn, Oxford Academic, 22 June 2023). DOI: https://doi.org/10.1093/oso/9780192855831.001.0001(date of access: 13.10.2026).
3. Casarosa Federica. Cybersecurity Certification of Artificial Intelligence: A Missed Opportunity to Coordinate Between the Artificial Intelligence Act and the Cybersecurity Act. International Cybersecurity Law Review. June 2022. 3(1). Pp. 1-16. DOI: 10.1365/s43439-021-00043-6 (date of access: 13.10.2026).
4. Burchardt Dana. The Concept of Legal Space: A Topological Approach for Addressing Multiple Legalities. Global Constitutionalism. Volume 11, Issue 3: Populist Challenges to Global Governance: Feminist Perspectives. November 2022. Pp. 518 – 547. DOI: https://doi.org/10.1017/S2045381722000041(date of access: 13.10.2026).
5. Карвацька С. Б., Грушко М.В. Міжнародно-правові засади та виклики використання цифрових доказів у процесі притягнення до відповідальності за воєнні злочини. Правничий часопис Донецького національного університету імені Василя Стуса. 2026. №1 Ч. 1. С. 86-95. DOI: https://doi.org/10.31558/2786-5835.2026.1.1.9 (дата звернення: 14.10.2026).
6. Keyfacts UNESCO's Recommendation on the Ethicsof ArtificialIntelligence URL: https://unesdoc.unesco.org/ark:/48223/pf0000385082(date of access: 13.10.2026).
7. Захарчук І. Міжнародне право в умовах цифровізації: становлення четвертого покоління прав людини. Аналітично-порівняльне правознавство. 2025. No 3 (5). С. 353–359. DOI: https://doi.org/10.24144/2788-6018.2025.05.3.52 (дата звернення: 14.10. 2026).
8. UN GGE Report: Major Players Recommending Norms of Behaviour, Highlighting Aspects of International Law. 2015. URL: https://ccdcoe.org/incyder-articles/2015-un-gge-report-major-players-recommending-norms-of-behaviour-highlighting-aspects-of-international-law/ (date of access: 13.10.2026).
9. Osula Anna-Maria, Kasper Agnes & Kajander Aleksi. EU Common Position on International Law and Cyberspace, 2022. Vol. 16. No. 1 URL: https://doi.org/10.5817/MUJL2022-1-4(date of access: 13.10.2026).
10. Hughes S. U. S. Regulation of Blockchain Curr chain Currencies: A P encies: A Policy

ISSN 3083-7979

Overview. American University Washington College of Law. 2020. 1. 1. URL: https://digitalcommons.wcl.american.edu/facsch_lawrev/1883(date of access: 13.10.2026).
11. Карвацька С. Б., Маник А. З., Строїч М. І. Кібербезпека: сучасні виклики та міжнародно-правові рамки щодо захисту даних. Науковий вісник Ужгородського Національного Університету. Серія Право. 2025. Випуск 87: частина 4. С. 251-256. DOI: https://doi.org/10.24144/2307-3322.2025.87.4.39 (дата звернення: 14.10.2026).
12. Лабик А. Р. Міжнародне право прав людини в умовах цифровізації: аналіз ключових понять. Аналітично-порівняльне правознавство. 2025. № 6. Ч. 3. С. 429-433. DOI: https://doi.org/10.24144/2788-6018.2025.06.3.65 (дата звернення: 14.10.2026).
13. Хаустова М. Г. Поняття цифровізації: національні та міжнародні підходи. Право та інновації. 2022. № 2 (38). С. 7–18. DOI: https://doi.org/10.37772/2518-1718-2022-2(38)-1 (дата звернення: 14.10.2026).
14. Golia Angelo Jr., Kettemann Matthias C., Kunz Raffaela [Eds.]. Digital Transformations in Public International Law. URL: https://pure.mpg.de/rest/items/item_3560540_1/component/file_3560541/content (date of access: 13.10.2026).

REFERENCES:

1. Burchardt D. Does Digitalization Change International Law Structurally? German Law Journal. 2023; 24(3):438-460. URL: https://doi.org/10.1017/glj.2023.31(date of access: 13.10.2026).
2. Krieger Heike & Liese Andrea eds. Tracing Value Change in the International Legal Order – Perspectives from Legal and Political Science. 2023. Krieger, Heike, and Andrea Liese (eds), Tracing Value Change in the International Legal Order: Perspectives from Legal and Political Science (Oxford, 2023; online edn, Oxford Academic, 22 June 2023). DOI: https://doi.org/10.1093/oso/9780192855831.001.0001(date of access: 13.10.2026).
3. Casarosa Federica. Cybersecurity Certification of Artificial Intelligence: A Missed Opportunity to Coordinate Between the Artificial Intelligence Act and the Cybersecurity Act. International Cybersecurity Law Review. June 2022. 3(1). Pp. 1-16. DOI: 10.1365/s43439-021-00043-6 (date of access: 13.10.2026).
4. Burchardt Dana. The Concept of Legal Space: A Topological Approach for Addressing Multiple Legalities. Global Constitutionalism. Volume 11, Issue 3: Populist Challenges to Global Governance: Feminist Perspectives. November 2022. Pp. 518 – 547. DOI: https://doi.org/10.1017/S2045381722000041(date of access: 13.10.2026).
5. Karvatska, S. B., & Hrushko, M. V. (2026). Mizhnarodno-pravovi zasady ta vyklyky vykorystannia tsyfrovykh dokaziv u protsesi prytiahnennia do vidpovidalnosti za voienni zlochyny [International legal principles and challenges of using digital evidence in proceedings concerning accountability for war crimes]. Pravnychyi chasopys Donetskoho natsionalnoho universytetu imeni Vasylia Stusa, (1, Pt. 1), 86–95. https://doi.org/10.31558/2786-5835.2026.1.1.9 (дата звернення: 14.10.2026).
6. Keyfacts UNESCO's Recommendation on the Ethicsof ArtificialIntelligence URL: https://unesdoc.unesco.org/ark:/48223/pf0000385082(date of access: 13.10.2026).
7. Zakharchuk, I. (2025). Mizhnarodne pravo v umovakh tsyfrovizatsii: stanovlennia chetvertoho pokolinnia prav liudyny [International law in the context of digitalization: The emergence of the fourth generation of human rights]. Analitychno-porivnialne pravoznavstvo, (3[5]), 353–359. https://doi.org/10.24144/2788-6018.2025.05.3.52(дата звернення: 14.10.2026).
8. UN GGE Report: Major Players Recommending Norms of Behaviour, Highlighting Aspects of International Law. 2015. URL: https://ccdcoe.org/incyder-articles/2015-un-gge-report-major-players-recommending-norms-of-behaviour-highlighting-aspects-of-international-law/ (date of access: 13.10.2026).

ISSN 3083-7979

9. Osula Anna-Maria, Kasper Agnes & Kajander Aleksi. EU Common Position on International Law and Cyberspace, 2022. Vol. 16. No. 1 URL: https://doi.org/10.5817/MUJL2022-1-4(date of access: 13.10.2026).
10. Hughes S. U. S. Regulation of Blockchain Curr chain Currencies: A P encies: A Policy Overview. American University Washington College of Law. 2020. 1. 1. URL: https://digitalcommons.wcl.american.edu/facsch_lawrev/1883(date of access: 13.10.2026).
11. Karvatska, S. B., Manyk, A. Z., & Stroich, M. I. (2025). Kiberbezpeka: suchasni vyklyky ta mizhnarodno-pravovi ramky shchodo zakhystu danykh [Cybersecurity: Contemporary challenges and international legal frameworks for data protection]. Naukovyi visnyk Uzhhorodskoho natsionalnoho universytetu. Seriia Pravo, (87, Pt. 4), 251–256. https://doi.org/10.24144/2307-3322.2025.87.4.39 (дата звернення: 14.10.2026).
12. Labik, A. R. (2025). Mizhnarodne pravo prav liudyny v umovakh tsyfrovizatsii: analiz kliuchovykh poniat [International human rights law in the context of digitalization: An analysis of key concepts]. Analitychno-porivnialne pravoznavstvo, (6, Pt. 3), 429–433. https://doi.org/10.24144/2788-6018.2025.06.3.65(дата звернення: 14.10.2026).
13. Khaustova, M. H. (2022). Poniattia tsyfrovizatsii: natsionalni ta mizhnarodni pidkhody [The concept of digitalization: National and international approaches]. Pravo ta innovatsii, (2[38]), 7–18. https://doi.org/10.37772/2518-1718-2022-2(38)-1(дата звернення: 14.10.2026).
14. Golia Angelo Jr., Kettemann Matthias C., Kunz Raffaela [Eds.]. Digital Transformations in Public International Law. URL: https://pure.mpg.de/rest/items/item_3560540_1/component/file_3560541/content (date of access: 13.10.2026).

Дата першого надходження/Date of first submission: 15.08.2026
Прийнято до друку/Accepted: 25.09.2026
Опубліковано/Published: 01.11.2026

ISSN 3083-7979