Stepanenko, N., & Perepadin, K. (2025). Ensuring human rights in the context of digital technologies during an armed conflict. *Legal Horizons, 26*(3), 77-87. All authors declare that they have no conflicts of interest.

ENSURING HUMAN RIGHTS IN THE CONTEXT OF DIGITAL TECHNOLOGIES DURING AN ARMED CONFLICT

Nataliia Stepanenko
Department of Theory and History of the State and Law
«KROK» University
03113, 30-32 Tabirna St., Kyiv, Ukraine
e-mail: nataliasv@krok.edu.ua
https://orcid.org/0000-0001-6216-2206

Kostiantyn Perepadin
«KROK» University
03113, 30-32 Tabirna St., Kyiv, Ukraine
e-mail: perepadinkv@krok.edu.ua
https://orcid.org/0009-0009-5205-5824

Abstract

In the context of the full-scale armed conflict caused by the russian federation's aggression against Ukraine, digital technologies have become an integral part of both hostilities and the daily lives of the civilian population. This poses unprecedented challenges for ensuring and protecting human rights. The article analyzes the key issues arising at the intersection of digital technologies, human rights, and armed conflict in the Ukrainian context. It examines the use of digital platforms for spreading disinformation and propaganda, which violates the right to receive reliable information, as well as countermeasures against these phenomena and the associated risks of restricting freedom of speech. Threats to the right to privacy and personal data protection, stemming from increased state surveillance and data collection under martial law, are analyzed, emphasizing the importance of adhering to the principles of legality and data minimization. The impact of cyberattacks on critical infrastructure as a factor violating the socio-economic rights of the civilian population and the complexity of legally qualifying such actions are highlighted. Simultaneously, the positive potential of digital technologies as a tool for documenting war crimes and human rights violations using open-source intelligence (OSINT), photo, and video evidence is demonstrated, underscoring the importance of adhering to standards for handling digital evidence (e.g., the Berkeley Protocol). The article is based on the analysis of current research by Ukrainian academic institutions, human rights, and expert organizations. It concludes that a comprehensive approach is necessary, including improving national legislation and international legal norms, strengthening cybersecurity, developing standards for working with digital evidence, and ensuring a balance between national security needs and the protection of fundamental human rights and freedoms in wartime.

Keywords: human rights, digital technologies, martial law, armed conflict, disinformation.

1. Introduction

Contemporary armed conflicts increasingly demonstrate the profound integration of digital technologies into all spheres of social life. Whereas in the twentieth century the information domain largely played an auxiliary role in supporting defence and communications, it has today evolved into an autonomous arena of confrontation. Cyber operations, disinformation campaigns, the blocking of online resources, and the use of digital platforms to shape public opinion have become as decisive for the course of hostilities as traditional military operations. The full-scale aggression of the Russian

DOI: https://doi.org/10.54477/LH.25192353.2025.3.pp.77-87

Federation against Ukraine, which began in 2022, has vividly confirmed this trend, rendering digitalisation an inalienable element of wartime reality (Mazepa, 2024).

The deployment of digital technologies in wartime generates complex and often contradictory consequences for the protection of human rights. On the one hand, digital tools provide unprecedented opportunities to record war crimes, document violations of international humanitarian law, and rapidly disseminate truthful information. Smartphones, social networks, satellite imagery and open-source intelligence (OSINT) technologies enable the collection of evidence of crimes on a scale previously unimaginable. This enhances transparency and strengthens the work of international judicial institutions such as the International Criminal Court (Shevchuk et al., 2022). On the other hand, the digital environment itself has become an instrument of large-scale human rights violations. Disinformation campaigns and propaganda undermine the right to access reliable information, provoke panic, create a fertile ground for manipulation, and even incite violence. Cyberattacks on critical infrastructure directly affect the enjoyment of the socio-economic rights of civilians by depriving them of access to electricity, water supply, and essential medical and public services. In parallel, state surveillance has expanded significantly, which under martial law may assume excessive dimensions and jeopardise the right to privacy (Zarembo et al., 2024). Thus, digitalisation simultaneously emerges as both a means of protection and an instrument of restriction of human rights. The relevance of this problem is heightened by the fact that existing international legal norms only partially address these novel challenges. While the Universal Declaration of Human Rights and the European Convention on Human Rights guarantee freedom of expression, the right to privacy, and access to information, the specific issues of the qualification of cyberattacks, the admissibility of digital evidence, and the permissible scope of digital monitoring during armed conflict remain unresolved. Additional complications arise from the transboundary nature of cybercrime: disinformation and hacking campaigns are often launched from the territory of the aggressor state, which significantly hinders accountability. Ukraine has found itself in a unique situation where the war coincides with rapid processes of digital transformation. The introduction of e-government services such as Diia, the development of state cyber-defence infrastructure, and partnerships with international technology companies illustrate the high level of digital resilience demonstrated by the state. At the same time, the accelerated proliferation of digital practices in crisis conditions produces legal and ethical dilemmas. For instance, the storage and processing of personal data concerning internally displaced persons and other war-affected groups require special protection, as data breaches may lead to discrimination, fraud, or even direct physical threats (Kravchuk et al., 2024). The academic study of these issues demands the combination of several research perspectives. On the one hand, a formal legal analysis of national legislation and international instruments that define standards in the field of digital rights is indispensable. On the other hand, it is essential to take into account the experience of human rights organisations, analytical reports, the work of international expert communities, and practical case studies from Ukraine. Such an approach makes it possible to view digital rights not merely as abstract legal categories, but as concrete mechanisms of protecting the individual under the exceptional circumstances of war. The topic of safeguarding human rights in conditions of armed conflict and digitalisation has been actively addressed in the recent academic literature. Several thematic strands allow for a comprehensive understanding of the multifaceted nature of the challenges involved. Firstly, a number of authors, including Bochkova and Baadzhi (2024), Belov, Peresh, and Pokorba (2024), focus on the conceptualisation of “digital human rights”. Their works consider digital rights both as an extension of traditional rights in the online sphere (freedom of expression, right to privacy) and as novel legal categories such as the right to Internet access, digital identity, and protection against content manipulation. These contributions provide a valuable

theoretical foundation, while simultaneously highlighting the insufficient elaboration of mechanisms for implementing digital rights within national legal systems. Secondly, studies on information security and disinformation campaigns (Mazurenko, 2022) show that the digital environment has become a crucial channel of hybrid warfare. Scholars emphasise that the large-scale spread of disinformation undermines the right to reliable information and threatens democratic processes. At the same time, these works point to the difficulty of striking a balance between countering disinformation and safeguarding freedom of expression, which necessitates clear criteria and procedural safeguards for state intervention. Thirdly, a significant strand of literature focuses on cyber security and the classification of cyberattacks. Authors such as Petryshyn and Hilyaka (2021) draw attention to the vulnerability of critical infrastructure and social systems to cyber threats. Although the technical dimension of the problem is extensively described, the legal qualification of such actions as war crimes remains controversial. The absence of unified international legal criteria of attribution and harm assessment leaves a gap in mechanisms of accountability. Fourthly, scholars such as Shevchuk and Haiduk (2022) examine the protection of personal data under martial law. They identify risks related to data leaks concerning internally displaced persons and other vulnerable groups, underscoring the necessity of data minimisation principles and independent supervisory mechanisms, as well as the adaptation of GDPR standards to the Ukrainian context. Fifthly, a distinct body of research addresses the use of digital evidence in judicial proceedings. Tikhomirov (2022), together with Denysenko, Borko and Kosov (2023), highlight the potential of digital materials in documenting war crimes, while also identifying problems of verification, preservation, and compliance with procedural safeguards. The lack of harmonised international norms on the admissibility of digital evidence reduces their effectiveness in judicial practice.

Overall, the literature review demonstrates considerable scholarly interest in the issue of digital rights during wartime, yet reveals several important gaps: the lack of clear international criteria for the classification of cyberattacks as war crimes, the absence of unified standards for the admissibility of digital evidence, insufficient systemic proposals for harmonising Ukrainian law with EU standards, and a shortage of interdisciplinary approaches that combine legal, technical, and sociological perspectives.

Despite the substantial body of existing scholarship, a number of fundamental questions remain unresolved. Firstly, there is no consistent international practice recognising cyberattacks against civilian infrastructure as war crimes, despite their often greater destructive consequences compared to conventional attacks. Secondly, there are no harmonised standards for the admissibility of digital evidence in international and national courts. Thirdly, the balance between national security requirements and the protection of fundamental rights—particularly the right to privacy and freedom of expression—remains unsettled.

Accordingly, this study aims to conduct a comprehensive analysis of the main challenges and problems in the field of human rights protection associated with the use of digital technologies under wartime conditions in Ukraine. The objective is not only to identify existing threats but also to propose potential solutions, drawing upon contemporary academic approaches, international standards, and human rights practices. Particular emphasis is placed on finding a balance between legitimate security measures and the guarantees of individual rights, as well as on exploring the possibilities for harmonising Ukrainian legislation with European Union law in the domain of digital rights.

The purpose of this article is to identify and classify the principal threats to digital human rights during armed conflict, to analyse the legal regulation of this field, and to develop recommendations for its improvement. The specific objectives include: clarifying the legal nature of digital human rights; assessing the impact of disinformation, cyberattacks and digital surveillance on individual rights; analysing international and

DOI: https://doi.org/10.54477/LH.25192353.2025.3.pp.77-87

national standards in the sphere of digital rights; and formulating proposals for aligning Ukrainian regulations with the European legal framework.

The novelty of this study lies in combining legal, information-security, and human rights approaches to the issue of digital rights in wartime. For the first time in Ukrainian scholarship, a systematic analysis is offered of the justification and excessiveness of restrictions on digital rights during armed conflict; the specific features of documenting war crimes through digital technologies are explored; and pathways for adapting Ukrainian legislation to EU standards are proposed.

2. Materials and Methods

The methodology of this study is grounded in a combination of general scientific and specialised legal methods, which enabled a comprehensive analysis of the impact of digital technologies on the protection of human rights during the armed conflict in Ukraine. Addressing the research problem required both theoretical reflection and the consideration of practical data derived from an examination of current legislation, international legal instruments, the practice of human rights organisations, and scholarly research.

A dialectical method of inquiry was employed, which made it possible to view the interaction between digital technologies and human rights as a dynamic process that evolves under the influence of wartime conditions. This method facilitated an examination of how traditional human rights acquire new forms in the digital environment and how their realisation changes during armed conflict. In addition, a systemic approach was applied, allowing human rights, digital technologies, and legal regulation to be regarded as an interconnected whole. Within this framework, individual phenomena such as disinformation, cyberattacks, and digital surveillance were analysed alongside their cumulative impact on the overall state of rights protection in Ukraine.

A comparative legal method played a particularly significant role, providing the basis for analysing the compliance of Ukrainian legislation with international and European standards in the field of digital rights. This entailed a comparison of the provisions of the Constitution of Ukraine, the Law “On Information”, and the Law “On Personal Data Protection” with the norms of the European Convention on Human Rights, the Universal Declaration of Human Rights, as well as European Union standards, in particular the General Data Protection Regulation (GDPR). This comparison made it possible to identify shortcomings and to outline avenues for harmonisation. The formal legal method was also applied to analyse the substance of legal norms regulating the digital sphere in Ukraine and at the international level. This method made it possible to define the permissible limits of restrictions on human rights in wartime and to assess their compliance with the criteria of legitimacy, proportionality, and necessity.

A historical-legal method was used to trace the evolution of approaches to information security and digital human rights since 2014, when Russia’s hybrid aggression against Ukraine commenced. This facilitated an understanding of both the continuity and transformation of threats and countermeasures. Equally important was the method of content analysis, which enabled the examination of publications by Ukrainian and foreign scholars, reports by human rights organisations (such as the Human Rights Platform, Access Now, and the Expert Centre for Human Rights), as well as materials produced by international organisations including the United Nations, the OSCE, and the Council of Europe. The use of this method allowed for the identification of key themes, challenges, and approaches in the field of digital rights in wartime. Finally, a prognostic method was employed, which provided the means to formulate recommendations for the further development of national legislation and international standards in the sphere of digital rights, taking into account prospective challenges associated with the use of artificial intelligence, deepfakes, and other innovative technologies in armed conflicts.

The empirical foundation of the study consisted of: national legal acts of Ukraine,

including the Constitution of Ukraine, the Law "On Information", the Law "On Personal Data Protection", and other acts regulating martial law and digital activity; international instruments such as the Universal Declaration of Human Rights, the European Convention on Human Rights, international standards for the collection and use of digital evidence (the Berkeley Protocol), and the Tallinn Manual on the International Law Applicable to Cyber Operations; reports and analytical materials by human rights organisations (Human Rights Platform, Access Now, Expert Centre for Human Rights) documenting practical cases of violations of digital rights during the war; scholarly publications by Ukrainian and foreign researchers (Bochkova, Baadzhi, Petryshyn, Hilyaka, Mazurenko, Rusakevych, among others) exploring doctrinal and practical aspects of digital rights; and the practice of international and national judicial institutions illustrating approaches to the assessment of digital evidence and the limitation of rights during armed conflict.

The research was conducted in several stages. At the initial stage, the relevance of the topic was established, and the main directions of inquiry were defined, including disinformation, digital surveillance, cyberattacks, and digital evidence. Scholarly publications, reports, and international documents concerning digital rights in armed conflicts were systematised. A formal legal analysis of the Constitution of Ukraine, relevant laws, and international instruments was conducted to assess their compliance with international standards. Ukrainian norms were compared with European and international standards, particularly the GDPR and the jurisprudence of the European Court of Human Rights. Empirical cases of digital rights restrictions, cyberattacks, disinformation campaigns, and the documentation of war crimes through digital technologies were studied. On the basis of these findings, conclusions were drawn regarding the dual impact of digitalisation on human rights in wartime, and directions for improving both national and international law were identified.

The choice of methods was determined by the interdisciplinary nature of the subject, which lies at the intersection of law, information security, technology, and human rights practice. Reliance solely on a formal legal approach would have been insufficient, as the realities of war create new challenges that transcend the boundaries of classical legal scholarship. Accordingly, the combination of systemic, comparative, content-analytical, and prognostic methods ensured a multidimensional understanding of the problem.

In sum, the methodology of the study rests upon a combination of theoretical and applied approaches, which enabled a comprehensive result. The application of a broad range of methods and sources ensured both the objectivity and depth of the analysis and allowed for the formulation of well-founded conclusions and recommendations.

3. Results and Discussion

The armed conflict in Ukraine is unfolding in an era of profound societal digitalisation, which generates specific and multifaceted challenges for the protection of human rights, while simultaneously opening new avenues for their assertion and the documentation of violations. The concept of "digital human rights" has emerged to address the unique challenges and opportunities arising in the digital age. These rights encompass traditional human rights as they apply to online environments, as well as novel rights specific to the digital sphere, such as the right to internet access, data protection, and digital identity. According to V.A. Bochkovaya and N.A. Baadji (2024), digital human rights constitute a set of rights and freedoms safeguarding individuals in digital environments, including the right to communication, freedom of content, digital identity, and the acquisition of digital skills.

We concur with scholars who emphasise that digital human rights are becoming an integral component of contemporary society, where technology is rapidly transforming lifestyles and modes of interaction (Belov et al., 2024). O.V. Petryshyn and O.S. Hilyaka note that the digital technology era offers entirely new and qualitatively

DOI: https://doi.org/10.54477/LH.25192353.2025.3.pp.77-87

distinct opportunities for the realisation of human rights, while simultaneously creating novel challenges and threats to their protection (Petryshyn & Hilyaka, 2021).

International human rights law, in particular the Universal Declaration of Human Rights and the European Convention on Human Rights (ECHR), provides a foundation for the protection of digital rights. Article 10 of the ECHR guarantees the right to freedom of expression, which extends to all individuals without exception, including users in online environments (Freedom of Speech on the Internet. Human Rights Platform NGO. International and National Standards of Freedom of Speech on the Internet, 2025).

Ukrainian national legislation, including the Constitution (Article 34), the Law on Information, and the Law on Personal Data Protection, also regulates aspects of digital rights (Data Protection Legislation in Ukraine, 2025). Article 34 of the Constitution guarantees every person the right to freedom of thought and expression, the free articulation of views and convictions, and the right to freely collect, store, utilise, and disseminate information orally, in writing, or by other means. The right to privacy is enshrined in international instruments and the constitutions of most countries, including Ukraine.

In the context of martial law in Ukraine, the issue of temporarily restricting fundamental human rights, including digital rights, arises in the interest of national security. However, according to international human rights standards, such restrictions must be legitimate, justified by pressing social needs, and proportionate to the pursued objectives. Limitations on informational rights during armed conflict may be necessitated by the objective requirement to preserve national viability, aligning with the state's right to undertake measures that restrict certain individual rights to ensure security and operational effectiveness.

Analysis of Ukrainian practice indicates a partial deviation from obligations under Article 10 of the ECHR regarding freedom of expression and access to information due to the imposition of martial law. The concept of digital rights remains in a dynamic phase of development, and its implementation during armed conflict is particularly complex. In this context, the challenge of balancing national security interests with individual rights becomes especially salient. Although the fundamental principles of human rights are universal and applicable in online environments, the precise boundaries and permissible limitations of digital rights remain subjects of scholarly debate and legal determination.

Martial law constitutes an exceptional circumstance that may justify deviations from peacetime standards. Nonetheless, such deviations require stringent oversight to prevent abuse and ensure their genuine necessity and proportionality. The interplay between international human rights law and national legislation in regulating digital rights during armed conflict is decisive. National legislation must demonstrate alignment with international standards to ensure adequate protection, while simultaneously accounting for specific domestic needs and challenges faced by the state.

Ukraine's legal framework for digital rights is shaped by both international conventions and domestic constitutional and statutory provisions. Analysing the coherence and consistency across different levels of legal regulation is key to understanding the overall degree of protection afforded to individuals in the digital space during wartime.

The use of digital technologies during the war in Ukraine has posed numerous human rights challenges, including cyberattacks targeting critical infrastructure and civilians (What They Did in the Shadows: Internet Shutdowns and Atrocities in Ukraine, 2025). Disinformation campaigns aimed at manipulating public opinion and undermining trust have become prevalent. Concerns have been raised regarding privacy violations due to data breaches and surveillance. False information has been disseminated since 2014 to destabilise Ukraine. Disinformation distorts public opinion both within and outside Ukraine, indicating that false narratives can induce panic and damage the government’s reputation, including interference by Russian hackers with

Ukrainian broadcasting and media websites.

Ukrainian scholars have actively investigated the impact of these digital threats on human rights during the war. L.I. Mazurenko (2022) examines challenges and threats to information security amid the Russia–Ukraine conflict, including the dissemination of disinformation via social networks and the importance of countering false information. A.I. Rusakevych (2024) analyses information security under martial law in the context of citizens' informational rights, highlighting legal, political, and technical dimensions. Legal aspects of safeguarding information security during full-scale invasion are also explored, emphasising the protection of political rights and freedoms in the information space. Violations of the right to publish content in digital media constitute breaches of digital rights and fundamental principles of freedom of expression enshrined in Article 19 of the Universal Declaration of Human Rights (Denysenko et al., 2023).

In the context of armed conflict, information assumes strategic significance, transforming into a tool of influence, with digital spaces becoming a primary arena of confrontation. This necessitates a comprehensive approach encompassing cybersecurity measures to protect information systems and informational-psychological security aimed at countering destructive informational influences and manipulation. Research indicates that contemporary armed conflicts possess not only kinetic but also pronounced informational dimensions. Digital platforms significantly extend the reach and intensity of both verified and misleading information, highlighting the critical need to understand the impact of information flows on human rights, individuals' psychological states, and national security.

Persistent emphasis on the threats of disinformation and cyberattacks in the literature suggests deliberate, coordinated efforts to destabilise Ukraine using digital tools. This directly affects a broad spectrum of human rights, including the right to receive objective and reliable information, freedom of expression (potentially limited through censorship or manipulation), and the right to privacy (compromised by unauthorised access to personal data). The consistency of identified threats across different information sources and over time points to the strategic nature of the aggressor's actions. Analysing tactical methods, strategic objectives, and operational impacts of these digital operations is critical for devising effective countermeasures and ensuring human rights protection in digital environments.

Ukrainian scholars emphasise the need for a multi-faceted approach, incorporating legal and technical mechanisms alongside initiatives to enhance media literacy and critical thinking skills among the population. Combating disinformation and mitigating cyberattack consequences require fostering societal resilience to manipulative influences and raising awareness of potential digital risks. Educational and informational campaigns play a pivotal role in empowering citizens to protect their rights and strengthen national informational security.

Limited internet access in conflict zones and occupied territories constitutes a significant human rights challenge, restricting access to information, communication, and essential services (Tikhomirov, 2022). Reports highlight censorship and blocking of online resources, particularly those perceived as pro-Russian. Concerns exist regarding unlawful surveillance and potential misuse of personal data collected via digital platforms (Internet in Wartime: Are Restrictions Necessary in Ukraine, 2025). The dissemination of hostile propaganda and disinformation remains a serious issue, influencing public opinion and potentially inciting violence (Lytvyn & Yarosh, 2024). Russia's deliberate internet shutdowns in occupied territories coincided with human rights violations. Ukrainian scholars have documented specific challenges and their human rights consequences, including internet restrictions, censorship of pro-Russian resources, IT sector regulation, and violations of digital and informational rights due to cyberattacks and disinformation. The right to access information may be limited under martial law in Ukraine for national security reasons.

DOI: https://doi.org/10.54477/LH.25192353.2025.3.pp.77-87

Targeting internet infrastructure and enforcing shutdowns in occupied territories indicates a strategy to control information flows and isolate populations, potentially facilitating human rights violations and obstructing accountability. By restricting external access and limiting internal communication, occupying forces promote population isolation, creating an environment of impunity. This complicates victims' ability to report abuses and hinders international observers' collection of objective data and monitoring of human rights violations. Striking the right balance is crucial to avoid undermining democratic values in the name of security. Overly broad or opaque restrictions on internet access and content may produce unintended consequences, including suppression of lawful dissent, obstruction of journalists' and human rights defenders' work, and opportunities for spreading unverified rumours and disinformation.

The vulnerability of personal data during wartime is a significant concern, as data breaches can expose individuals to increased risk of harm, particularly displaced persons or conflict-affected populations. Electronic registries containing confidential information about internally displaced persons, victims of war, and social assistance recipients are potential cyberattack targets. Compromise of such data may result in identity theft, fraud, discrimination, or even physical harm.

Although Ukraine possesses a robust legal framework, legislation requires improvement in line with international standards. There is a need to harmonise digital practices with international human rights norms and ensure cybersecurity. The Ukrainian government has actively leveraged digital technologies to support governance, service provision, and citizen engagement during the war, demonstrating a high degree of digital resilience. Rapid deployment and expansion of platforms such as "Diia" for essential services, coupled with efforts to maintain internet connectivity despite infrastructure damage, underscore the strategic importance of digital transformation in crisis conditions. Engagement with international partners, including technology companies and foreign governments, has been crucial in sustaining digital infrastructure and cybersecurity efforts, highlighting the transnational nature of digital security and the significance of international cooperation in addressing wartime digital challenges.

Provision of services such as Starlink, transfer of confidential data abroad for protection, and sharing of expertise and resources demonstrate collective efforts to strengthen Ukraine's digital defence and maintain critical online functions. Ukrainian experts recognise the need for continual refinement of the legal framework and practical measures to protect digital rights during wartime. This includes adapting legislation to specific armed conflict challenges, enhancing cybersecurity capabilities, and promoting digital literacy among the population. The dynamic nature of both digital technologies and the conflict itself necessitates ongoing assessment and improvement of strategies for human rights protection in the digital sphere, requiring commitment to learning from experience and adapting to emerging threats and challenges.

The right to freedom of expression faces challenges due to censorship, content restrictions, and criminalisation of statements deemed to undermine national security. Access to information is hindered by infrastructure damage, government restrictions on certain data for security reasons, and digital inequality. Privacy is threatened by surveillance, data breaches, and potential misuse of personal information collected online. Data security is paramount given the risk of cyberattacks targeting confidential information and critical infrastructure.

Ukrainian scholars stress the importance of aligning national laws with international human rights principles in the digital sphere, advocate strengthening the international legal framework for regulating digital rights during armed conflicts, and acknowledge that national legislation alone may be insufficient to address transnational threats and ensure accountability. Calls for a new international convention on digital and informational human rights reflect recognition that existing international law may inadequately address digital technology-specific challenges in conflict contexts, highlighting the need

for a more comprehensive, globally adaptive approach. The emphasis on harmonising Ukrainian legislation with EU standards reflects broader aspirations toward European integration and recognition of the EU's advanced legal frameworks in areas such as data protection and cybersecurity. Adoption of EU norms could enhance Ukraine's protection of digital rights and facilitate greater compatibility and cooperation with European partners in countering digital threats. The study underscores the dynamic nature of digital environments and the necessity for continual adaptation of legal norms and enforcement mechanisms to keep pace with technological progress and evolving threats. Rapid development of digital technologies, including artificial intelligence and deepfakes, presents new challenges for human rights protection. Legal frameworks must be flexible and adaptive to effectively address these emerging issues.

At the same time, despite these challenges, digital technologies have become a powerful instrument for protecting human rights and documenting the aggressor's atrocities. The capacity to record events via smartphones and other mobile devices, analyse high-resolution satellite imagery, and collect and verify open-source intelligence (OSINT) allows for the documentation of war crimes, crimes against humanity, and other serious human rights violations on an unprecedented scale (NGO Human Rights Platform, 2023). Such digital evidence has the potential to play a pivotal role in national and international investigations and judicial proceedings (International Criminal Court, International Court of Justice). However, to ensure legal validity and admissibility, the collection, storage, analysis, and presentation of such evidence in court must adhere to rigorous internationally recognised procedures and standards, such as the Berkeley Protocol on the Use of Digital Open Source Information in Investigations (Expert Center for Human Rights, 2023).

Thus, digitalisation exerts a profound and dual impact on the human rights situation in Ukraine during armed conflict, generating both significant threats and unique opportunities.

Conclusion

The study demonstrates that digitalisation in the context of the armed conflict in Ukraine exerts a dual impact: on the one hand, it presents significant challenges to the protection of human rights, while on the other, it provides tools for safeguarding them and documenting violations.

Firstly, the analysis of practice confirms that restrictions on rights during wartime are heterogeneous in terms of their justification. Temporary restrictions on access to specific resources directly used for coordinating the aggressor or disseminating harmful propaganda, as well as the reinforcement of cybersecurity measures to prevent attacks on critical infrastructure, may be considered justified. Such measures meet the criteria of legitimacy, urgent societal need, and proportionality. By contrast, excessively broad or opaque blocking of websites and social media platforms encompassing lawful content, as well as the unwarranted expansion of state digital monitoring without adequate oversight safeguards, are disproportionate. These practices risk transforming wartime exceptions into instruments for long-term curtailment of freedom of expression and the right to privacy.

Secondly, particular attention should be given to the harmonisation of Ukrainian norms with EU law. In light of Ukraine's European trajectory, the most appropriate steps include:

the implementation of GDPR provisions concerning transparency in personal data processing and the strengthening of the independence of supervisory authorities;

- the adaptation of practices for the collection and use of digital evidence in accordance with the standards set out in the Berkeley Protocol and the recommendations of the Council of Europe;
- the development of a dedicated law on digital rights during a state of martial

DOI: https://doi.org/10.54477/LH.25192353.2025.3.pp.77-87

law, clearly defining the limits of permissible restrictions and mechanisms for ensuring their proportionality;

- the enhancement of media literacy among the population and the integration of European approaches to countering disinformation, including mechanisms under the EU Code of Practice on Disinformation.

Thirdly, the findings underscore the need for a balanced strategy: the state must ensure security and counter hostile digital attacks while guaranteeing that restrictions on rights remain temporary, transparent, and accountable. Otherwise, the risks of authoritarian tendencies under the guise of wartime circumstances may undermine public trust in institutions.

The scientific novelty of this study lies in the fact that, for the first time in domestic scholarship, a comprehensive analysis has been conducted of the justification and excessiveness of restrictions on digital rights during martial law in Ukraine, accompanied by proposals for harmonising Ukrainian legislation with European standards. A promising avenue for further research is the development of international legal mechanisms for classifying cyberattacks on civilian infrastructure as war crimes and the establishment of a global convention on digital human rights.

References

Access Now. (n.d.). What they did in the shadows: Internet shutdowns and atrocities in Ukraine. Retrieved June 30, 2025, from https://www.accessnow.org/internet-shutdowns-and-atrocities-in-ukraine

Belov, D. M., Peresh, I. Ye., & Pokorba, I. (2024). Digital human rights: Doctrinal foundations. *Analytical and Comparative Jurisprudence*, 110–115.

Bochkova, V. A., & Baadzhi, N. A. (2024). Digital human rights and their limitations in the context of modern legal challenges. *Scientific Bulletin of Uzhhorod National University,* 228–233.

Denysenko, K. V., Borko, I. S., & Kosov, O. M. (2023). Implementation of digital and information human rights in the conditions of martial law. *Scientific Bulletin of Uzhhorod National University. Law Series, 77*(1), 90–94.

DLA Piper. (n.d.). Data protection legislation in Ukraine. Retrieved June 30, 2025, from https://www.dlapiperdataprotection.com/index.html?t=law&c=UA

Expert Center for Human Rights. (2023, February 2). Documenting war crimes: How does the Berkeley Protocol work? Retrieved June 30, 2025, from https://ecpl.com.ua/news/dokumentuvannia-voiennykh-zlochyniv-iak-pratsiuie-protokol-berkli/

Human Rights Platform NGO. (n.d.). Freedom of speech on the Internet. International and national standards of freedom of speech on the Internet. Retrieved June 30, 2025, from https://ppl.org.ua/bibliotech/mizhnarodni-ta-nacionalni-standarti-svobodi-slova-v-interneti

Human Rights Platform. (2023). War in the digital dimension and human rights: Final report (38 p.). Kyiv: Human Rights Platform. Retrieved June 30, 2025, from https://ppl.org.ua/wp-content/uploads/2023/11/vijna-u-czifrovomu-vimiri-ta-prava-lyudini_pidsumkovij-zvit.pdf

Kravchuk, M., Kravchuk, V., Hrubinko, A., Podkovenko, T., & Ukhach, V. (2024). Cyber security in Ukraine: Theoretical view and legal regulation. *Law, Policy and Security, 2*(2). Retrieved June 30, 2025, from https://lpas.com.ua/journals/vol-2-no-2-2024/cyber-security-in-ukraine-theoretical-view-and-legal-regulation

Lytvyn, & Yarosh. (2024). The impact of disinformation on Ukraine's national security under martial law. *Legal Scientific Electronic Journal, 2,* 290–292. Retrieved June 30, 2025, from http://lsej.org.ua/2_2024/71.pdf

Mazepa, S. (2024). Freedom of speech in the conditions of an armed conflict. In War, hate, propaganda and the Internet: A dangerous combination (SpringerBriefs in Law). Springer. https://doi.org/10.1007/978-3-031-69008-2_6

Mazurenko, L. I. (2022). Information security in the context of the Russian-Ukrainian war: Challenges and threats. *Bulletin of V. N. Karazin Kharkiv National University. Series: Political Science Issues, 42*, 50. https://doi.org/10.26565/2220-8089-2022-42-08

Petryshyn, O. V., & Hilyaka, O. S. (2021). Human rights in the digital age: Challenges, threats, and prospects. *Bulletin of the National Academy of Legal Sciences of Ukraine, 28*(1), 7–35.

Rusakevych, A. (2024). Information security in the conditions of martial law in the aspect of ensuring citizens' information rights. *Law. State. Technology, 2,* 58–62.

Shevchuk, A. V., & Haiduk, I. V. (2022). Protection of personal data in the conditions of martial law in Ukraine. *Law and Security, 2*(85), 103–110. Retrieved June 30, 2025, from https://pb.univd.edu.ua/index.php/PB/article/download/722/585/

Tikhomirov, O. O. (2022). Problems of restricting information rights in the conditions of martial law in Ukraine. *Juris Europensis Scientia, 6*, 62–67.

Vgoru. (n.d.). Internet in wartime: Are restrictions necessary in Ukraine? Retrieved June 30, 2025, from https://vgoru.org/prava-lyudini/internet-v-umovakh-viiny-chy-neobkhidni-obmezhennia-v-ukraini

Zarembo, K., Knodt, M., & Kachel, J. (2024). Smartphone resilience: ICT in Ukrainian civic response to the Russian full-scale invasion. *Media, War & Conflict, 18*(3), 305–324. https://doi.org/10.1177/17506352241236449