



Features of the implementation and limitations of human information rights in the context of external threats and military aggression in Ukraine

Olena Kalmykova

PhD in Law, Professor

Professor National University of Life and Environmental Sciences of Ukraine

03041, 15 Heroiv Oborony Str., Kyiv, Ukraine

<https://orcid.org/0000-0003-2041-8925>

Volodymyr Savchenko*

Postgraduate Student

National University of Life and Environmental Sciences of Ukraine

03041, 15 Heroiv Oborony Str., Kyiv, Ukraine

<https://orcid.org/0000-0003-1254-7276>

Article's History:

Abstract

Received: 17.10.2025

Revised: 20.01.2026

Accepted: 26.02.2026

Published: 27.03.2026

The relevance of the chosen topic lies in the fact that, in the current context, there was a growing interest on the part of the scientific and legislative community in the fourth generation of human rights, namely information rights. At the same time, under the legal regime of martial law at the legislative level, the implementation of such rights by any person may be restricted, but such restrictions must meet certain criteria. The aim of the study was to assess the restrictions on human information rights in wartime through the prism of contemporary theoretical concepts of the protection of these rights. The following methods were used in the work: formal-legal, systemic-structural, and prognostic. It was determined that

Suggested Citation:

Kalmykova, O., & Savchenko, V. (2026). Features of the implementation and limitations of human information rights in the context of external threats and military aggression in Ukraine. *Law. Human. Environment*, 17(1), 42-56. doi: 10.31548/law/1.2026.42.



*Corresponding author

Copyright © The Author(s). This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0 (<https://creativecommons.org/licenses/by/4.0/>)

restrictions on human information rights under martial law must meet the criteria of accessibility, comprehensibility, preservation of the balance between private and public interests, proportionality, and have a legitimate and sufficiently justified purpose. It is concluded that the main measures (tools) for protecting human information rights under martial law should be actions taken by civil society. An analysis of the experience of NATO countries (the United States, Estonia, Latvia) has demonstrated the effectiveness of an integrated approach that combines legislative regulation with educational measures and institutional support. The results of the study confirm the relevance of these changes. It is concluded that only a comprehensive modernisation of the regulatory framework, educational system and institutional support will effectively protect human information rights in the context of modern hybrid challenges. The results of this work can be used to develop regulatory and subordinate regulatory acts on the protection of human information rights

Keywords: information; protection tools; limitation of information rights; information society; security

Introduction

The protection of human rights remains one of the key legal institutions targeted by the activities of the state and authorised bodies. However, in the context of the temporary occupation of parts of Ukraine's territory, the military aggression by the Russian Federation, active hostilities, and the introduction of the legal regime of martial law, the problem of securing human rights and freedoms has become particularly acute. Among the fundamental rights most at risk of limitation during wartime are information rights, specifically the right to access information, freedom of speech, personal data protection, and the right to digital security. In modern information society, these rights are crucial not only for the personal freedom of citizens but also for preserving the democratic order, countering disinformation, and maintaining trust in state institutions.

According to the Freedom House report (2023), Russia's full-scale invasion has significantly undermined internet freedom in Ukraine. Attacks by the Russian army have caused severe damage to internet infrastructure, leading to network disruptions. The Ukrainian government blocks a wide range of Russian websites, including blogs, news portals, social media platforms, and

other online services. According to reports by the Office of the United Nations High Commissioner for Human Rights, information rights are systematically violated in the temporarily occupied territories of Ukraine. There have been documented restrictions on freedom of expression, blocking of Ukrainian media and internet resources, forced Russification of the information space, as well as persecution of journalists and civil activists. Such actions pose serious threats to access to truthful information and to the free formation of public opinion (OHCHR, 2024).

In this regard, the study of the legal mechanisms for protecting human information rights under martial law is extremely relevant, both in the national and international legal contexts. It allows for an assessment of the effectiveness of existing regulatory tools, identification of risks of excessive state interference in the information space, and the development of a legal model that balances security needs with human rights.

Among modern studies concerning the impact of digital transformations on the legal sphere, particular attention should be paid to the work of K. Bieliakov *et al.* (2023), who analysed evolutionary changes in the field of human rights

under the influence of digitalisation. The authors examine the emergence of new rights, the transformation of regulatory principles, the improvement of mechanisms for exercising existing rights, and the introduction of new restrictions and regulatory requirements. The researchers emphasise that these processes are not a deviation but a continuation of the evolution of the legal system, which adapts to the conditions of the digital environment while preserving fundamental legal values.

O.O. Barabash (2024), in own study, stressed that the protection of information rights should not be limited to preventing cyberattacks and personal data leaks but should also take into account the influence of information on an individual's physical and psychological condition, as well as their moral and spiritual values. This approach contributes to the creation of a harmonious and secure information environment that respects the interests of every individual, ensuring the protection of both their data and overall well-being. T.Yu. Tkachuk (2021) noted that in an information society, knowledge formed through the codification of scientific and technical information becomes a key factor influencing the development of the state and law. These processes are directly related to the challenges of legal regulation, particularly in the fields of digital security, information protection, and the stable functioning of the information space. Accordingly, the legal protection of the information environment is viewed as a necessary condition for the realisation of the rights and interests of individuals, as well as a factor in ensuring the stability of public authority and the rule of law.

T. Mikhailina *et al.* (2021) pointed out the need to establish an obligation for transnational information campaigns to open official representative offices in Ukraine. This would contribute to strengthening the protection of the rights of subjects of information legal relations, in particular

through the possibility of judicial protection. In addition, the authors support legislative initiatives to tax transnational information campaigns in Ukraine, which is in line with global trends. However, it is noted that strict state control over the information space is characteristic of totalitarian and authoritarian regimes and cannot be acceptable for democratic societies. In this context, the remarks by O. Antipova (2023) and V.S. Kurylo and O.L. Karaman (2024) on the important role of civil society in preserving information sovereignty are noteworthy.

In the current environment, self-protection measures in information systems, particularly at the corporate level, are becoming increasingly important. The use of financial mechanisms, such as financial liability, is appropriate given the significant profits of information corporations (Yadav *et al.*, 2023). Despite some developments in doctrinal research on the protection of human information rights in the context of military aggression by a neighbouring state, effective instruments for the protection of human information rights in a state of martial law remain unexplored, which will be considered in the course of the study.

Thus, the aim of the study was to examine the legal challenges to the protection of human rights to information in conditions of military aggression and to identify specific instruments of protection that are available under the regime of martial law. To achieve this goal, it was necessary to perform a number of objectives: 1) to define the essence of human information rights; 2) to provide a legal characterisation of restrictions on information rights and to define the criteria for their application; 3) to identify systems of instruments for the protection of information rights under the legal regime of martial law.

Materials and Methods

The research used a combination of general scientific and special legal methods, which was due to

the complex nature of the subject – the legal protection of human information rights in a state of martial law. In particular, general scientific methods (analysis, synthesis, induction, generalisation) were used to study scientific approaches to the concept of “information rights”, to understand the relationship between the right to information, freedom of speech and the right to privacy, and to form the author’s position on the scope and essence of these rights. The essence and content of the basic concepts were studied using a terminological (conceptual-categorical) method, which made it possible to clarify the definition of “human information rights” and their place in the hierarchy of fourth-generation rights.

A formal legal method was used to analyse the current legislation of Ukraine, primarily the articles of the Constitution of Ukraine (1996) and Law of Ukraine No. 389-VIII “On the Legal Regime of Martial Law” (2015). The purpose of analysing this legislation was to clarify the legal grounds, forms and limits of restrictions on information rights under a special legal regime. In the process of revealing the topic and objectives of the study, the practice of the Constitutional Court in cases No. 1-50/2009 (2009) and No. 17-rp/2010 (2010) was analysed. A number of regulatory and legal acts were also examined, including: Law of Ukraine No. 2657-XII “On Information” (1992), Law of Ukraine No. 2163-VIII “On the Basic Principles of Ensuring Cybersecurity of Ukraine” (2017), Draft Law of Ukraine No. 11533 (2024), Resolution of the Council of Judges of Ukraine No. 841-23 (2023). The systemic-structural method helped to identify internal links between norms regulating both general human rights and special restrictions established under martial law. Thanks to the systematisation method, the instruments for protecting human information rights used by the state and the public in conditions of armed conflict were structured.

Results

Concepts, characteristics and essence of the protection of human information rights. In the context of rapid informatisation of society and recognition of the key principles of the information society, human information rights are becoming particularly important. They are not only a set of legal opportunities, but also a priority of vital importance, the implementation of which directly affects human life in the modern world.

According to the Constitution of Ukraine (1996), human rights and freedoms, as well as their guarantees, determine the priorities and direction of the state’s activities, as enshrined in Article 3 (Constitution). Ensuring and upholding human rights and freedoms is the primary duty of the state. Information rights play a key role in this context, as they enable citizens to form beliefs, freely express their opinions, defend their ideas, and monitor the activities of the authorities. The indivisibility and inviolability of the complex of rights and freedoms in the information sphere forms the basis of democratic values in society.

V.D. Chorna and I.V. Alekseenko (2021) view these rights as a set of opportunities to access, create, use, disseminate, comment on, and communicate information on the Internet. A more specific definition of information rights is offered by N.I. Tkachuk (2018) offers a more specific definition of information rights, interpreting them as state-guaranteed opportunities for individuals to satisfy their needs to obtain, use, expand, preserve and protect information necessary for life, communication rights, the right to a safe information environment, etc., which are based on fundamental human rights.

Human information rights are in fact understood as fourth-generation rights. They are characterised by such features as the development and dissemination of information technology solutions, the creation of a global information environment, the transition to modern

socio-economic models, and the transformation of political processes in countries that are forming an information society. In addition, these rights provide for the independence of actions and the choice of lawful behaviour of a person based on the level of access to information. They also consist in protection from incomplete or harmful information, as well as in the security of personal data from unauthorised distribution (Tokarieva, 2023).

In the European legal space, a systematic concept of digital rights is gradually being formed, which is a modern form of realising human information rights in the context of digitalisation. Digital rights cover both traditional rights in the digital environment (the right to freedom of expression, privacy, and access to information) and new ones, in particular the right to access the Internet, digital identity, digital literacy, a safe online environment, and the right to be forgotten. These provisions are based, in particular, on the European Declaration of Digital Rights and Principles for the Digital Decade, adopted by the European Parliament, the Council and the Commission (2022), which defines the values of the EU digital space: respect for human dignity, freedom of choice, participation, non-discrimination and security. The most legally developed and normatively established aspect of digital rights is the right to personal data protection, which is clearly regulated by the General Data Protection Regulation (2016) – a key instrument that defines the boundaries of digital privacy in the EU.

Thus, it can be concluded that human information rights belong to the fourth generation of rights and represent a set of opportunities and powers of any person to obtain, use, disseminate and implement information. These rights are guaranteed by the state and its bodies, and are based on fundamental and constitutional rights. The protection of human information rights includes a set of organisational and legal measures

implemented by state and authorised bodies. These measures were aimed at preventing violations, restrictions and abuses in the field of information rights, as well as ensuring accountability for their violation.

Restrictions on human information rights under martial law. Following the introduction of martial law in Ukraine (Decree of the President of Ukraine No. 64/2022, 2022), it became clear that real threats to the life of Ukrainian society and the state necessitate a shift in the balance between private and public interests. This, in turn, requires the application of lawful measures related to the restriction of human rights and the temporary withdrawal of the state from fulfilling certain obligations in this area. Given the key role of information technology in the functioning of the state, society and the economy, the issue of reasonable restrictions on human information rights (in particular, the right to freedom of speech, access to information and protection of personal data) is becoming particularly relevant. The application of such restrictions must be assessed from the perspective of the principle of the rule of law, which requires that any interference be lawful, necessary and proportionate. This becomes a particularly difficult task in the context of the latest challenges associated with the Russian Federation's armed aggression against Ukraine, which poses global threats to information security, digital rights and democratic institutions on an international scale.

The protection by the Ukrainian population of the territories declared in 1991 as belonging to Ukraine from large-scale armed aggression by a neighbouring state has shown, among other things, that in such extremely difficult conditions, the effective implementation of a certain number of information rights is possible. Information rights, implemented through digital technologies, play an important role in ensuring communication, coordination and rapid data exchange in a

state of martial law. There have been numerous cases of digital platforms being used to report on the movements of occupying forces, document war crimes and record violations of international humanitarian law. The use of digital platforms in Ukraine to record the movements of occupying forces, document war crimes and collect evidence for international trials has become a key element in the fight for information security and justice. In particular, the “e-Enemy” app allows citizens to report on the actions of Russian troops, and the data collected is used to create a database of evidence that can be used in international courts (Tech Ukraine, 2022). In addition, the “EyeWitness to Atrocities” app, developed by the International Bar Association, has collected more than 50,000 pieces of digital evidence of war crimes in Ukraine, including shelling of civilian infrastructure and medical facilities. This data, collected with metadata and geolocation, helps to ensure the authenticity and reliability of the evidence (National School of Judges of Ukraine, 2024).

An analysis of Article 34 of the Constitution of Ukraine (1996) shows that it enshrines the right of every person to access information, including the ability to freely collect, store, use and disseminate it in any form at their own discretion. At the same time, the Article provides for certain restrictions on this right, which may be established in order to ensure national security, territorial integrity, public order, prevent riots or crimes, protect public health, protect the rights and reputation of others, prevent the disclosure of confidential information, or preserve the authority and impartiality of justice. Thus, the Constitution of Ukraine (1996) not only guarantees freedom of information, but also regulates its implementation, ensuring a balance between individual rights and public interests. That is why, under martial law, human rights to information may be legally restricted. According to Article 1 of Law of Ukraine No. 389-VIII (2015), martial

law is a special legal regime that may be introduced throughout Ukraine or in certain regions in the event of armed aggression, threat of attack or danger to the country’s independence and territorial integrity. This regime provides for the granting of special powers to state authorities, military command, military administrations and local self-government bodies in order to avert threats, counter armed aggression, ensure national security and preserve the territorial integrity of the state. It also provides for temporary restrictions on the constitutional rights and freedoms of citizens, as well as the rights and legitimate interests of legal entities, which are determined in accordance with the level of threat and the established terms of its application. This provides a legislative basis for an effective response to extraordinary threats, while adhering to the principles of the rule of law.

Among other human information rights that may be subject to restrictions, the following can be highlighted: Article 31 guarantees everyone the right to confidentiality of correspondence, telephone conversations, telegraph and other correspondence; Article 32 – prohibits interference in personal and family life, except in cases specified by the Constitution of Ukraine (1996); Article 34 – enshrines the right of everyone to freedom of thought and speech, as well as to freely express their views and beliefs; Article 41 – guarantees the right to own, use and dispose of property, as well as the results of intellectual and creative activity.

When imposing restrictions on human rights to information, clearly defined legal criteria must be observed that comply with both national legislation and international standards. According to Articles 34 and 64 of the Constitution of Ukraine (1996), such restrictions are permitted only on the basis of law, must have a legitimate purpose, be necessary in a democratic society and comply with the principle of proportionality.

The practice of the Constitutional Court of Ukraine clearly indicates that restrictions on fundamental rights are possible only in cases of justified public necessity and exclusively within the limits established by law (Judgment of the Constitutional Court of Ukraine No. 26-пн/2009, 2009). In this context, it is also important to take into account the latest initiatives, in particular Draft Law of Ukraine No. 11533 (2024), which provides for amendments to the legislation on access to public information under martial law, as well as the scientific and expert opinion on it, which emphasises the need to maintain a balance between security interests and the right to information.

In addition, Resolution of the Council of Judges of Ukraine No. 841-23 (2023) emphasised the importance of transparency of the judiciary even under martial law. The practice of national courts also demonstrates a desire to maintain a balance between public interests and security: for example, legal analyses by the Centre for Democracy and Rule of Law cite a number of cases in which courts uphold citizens' right to access information. For example, the court ordered the disclosure of the minutes of a local government meeting, recognising that the refusal was not duly justified by a threat to security. In another case concerning the refusal to provide a contract on budget funds, the restriction was also found to be disproportionate, as it was not substantiated by specific damage to defence capabilities (Vashchuk-Ogdanska, 2023a).

In the international context, the practice of the European Court of Human Rights (ECHR) regarding freedom of expression and restrictions on information rights involves the application of a "three-step test": (1) the existence of a legal basis for the interference; (2) the pursuit of a legitimate aim (e.g., the protection of national security or public order); (3) compliance of the interference with the requirement of "necessity in a democratic society" (Judgment in *Długolecki v.*

Poland (2009). At the same time, the ECHR has repeatedly emphasised that even in a state of emergency or martial law, the state is not exempt from its obligations to guarantee fundamental rights, in particular by adhering to the principles of proportionality, limited interference and proper judicial review (Shevchenko & Rozkladai, 2012).

In practice, this means that the judiciary in Ukraine must not only acknowledge the fact of martial law, but also assess the legality of restrictions on access to information or freedom of expression through the prism of this test. In particular, Resolution of the Council of Judges of Ukraine No. 841-23 (2023) emphasises the preservation of the principles of openness of justice even under martial law, which should guarantee effective access to information about court decisions and proceedings. The judicial practice of administrative courts shows consistent attempts to balance state interests and information transparency. In particular, in Judgment of the Third Administrative Court of Appeal in Case No. 340/5136/22 (2023), the court ruled that a public authority's refusal to provide information at the request of a citizen was unlawful, as the defendant did not justify what interests could be harmed by its disclosure, did not prove the existence of harm, and did not explain why this harm outweighs the public interest, as required by the so-called three-part test.

In addition, the conclusion to Draft Law of Ukraine No. 11533 (2024) emphasises the importance of ensuring that the digital security protection mechanisms provided for therein do not create unreasonable restrictions on individuals' rights to information. The legislature, like the executive branch, must act within the limits of international standards, implementing changes based on legal analysis and taking into account the conclusions of the ECHR. Thus, the approach developed by the ECHR should not be declarative, but integrated into the actual judicial practice of Ukraine, with mandatory reference to the legal

basis, the legitimacy of the objectives of the restriction and verification of the proportionality of the interference in each specific case.

Restrictions must be based on the principle of legal certainty, which means that any restriction of fundamental human and civil rights and freedoms is possible only if the legal norms governing such restrictions are clearly defined and their predictability is ensured for the persons to whom they apply. This means that such restrictions must be clearly defined, transparent and understandable to the persons concerned (Judgment of the Constitutional Court of Ukraine No. 17-пп/2010, 2010). The aim of these restrictions is to prevent arbitrariness, ensure fairness and limit the interference of the state and its bodies to the minimum, optimal level necessary to achieve legitimate goals.

Therefore, under the legal regime of martial law, restrictions on human information rights are entirely legitimate. However, it is important that such restrictions are based on democratic principles and comply with the requirements of the law, namely: maintaining a balance between public and private interests, compliance with the law, including its clarity and accessibility; having a legitimate and sufficiently justified purpose; the proportionality and reasonableness of such restrictions; respect for human dignity and freedom must be a fundamental principle, and all legal norms and restrictions must be aimed at ensuring the fundamental values of society, preserving its stability and maintaining law and order, justice and security.

Tools (measures) for protecting information rights under martial law. It should be noted that modern society is becoming increasingly integrated into the digital space, which, along with broad opportunities for development, communication and access to information, also creates new challenges and threats, particularly in the areas of security, privacy and human rights

protection. This is especially true for the public sector, which is called upon to serve citizens. A distinctive feature of this sector is that citizens often transfer their data through information and communication systems not out of obligation, but voluntarily (Włodyka, 2024). In addition to principles, the tools used to protect information rights also play an important role. As a rule, measures or instruments of protection in any sphere of social relations are considered key and necessary actions that must be implemented by the subject of protection to ensure the smooth functioning of the relevant social relations.

The system of protection measures can be formulated through the prism of the interaction of three main groups: legal, organisational and technical. Legal measures are a system of techniques and methods enshrined in the law that are aimed at guaranteeing and protecting the information rights of citizens and legal entities. Organisational measures are a set of management and coordination methods and measures that contribute to the effective enforcement and observance of information rights. Technical and software-hardware measures are a set of technological solutions, software and specialised devices used to implement and protect information rights in the digital environment. An example of technical measures is the use of electronic signatures, which ensure authentication, data integrity and the protection of citizens' information rights (Yarema, 2022).

Information rights protection and information security measures are broadly divided into two main groups: those aimed at protecting information systems from damage, and those that prevent information leaks or interception. The first category includes physical protection of military facilities and computer equipment from deliberate damage or destruction, as well as radio-electronic protection aimed at preventing data interception. The second group covers a range of measures, such as protecting information systems

from unauthorised remote access, which is implemented through the introduction of specialised software, including DLP and SIEM systems (Smotrych & Brailko, 2023). Another extremely important element is the protection of state and military classified information from leakage, illegal use or theft, which is achieved through the use of specially protected computer systems and software developed with current cyber threats in mind. At the same time, electronic intelligence tools are being developed and implemented to enable rapid monitoring of the information environment and neutralisation of potential threats.

A separate set of measures concerns the information and psychological protection of personnel. In particular, preventive measures are being taken to prevent deliberate psychological influence and manipulation aimed at destabilising the moral and psychological state of military personnel. This includes the correction of information flows broadcast by the enemy in order to prevent the influence of disinformation and deliberate distortion of reality. Considerable attention is also paid to the cybersecurity of communication systems – protection against cyberattacks and unauthorised access. In the current conditions of martial law, special attention is paid to the cybersecurity of communication systems, in particular protection against cyberattacks and unauthorised access. According to a study by V.O. Kucher (2024), the state is actively implementing measures to counter information threats, including the use of social networks to conduct information operations against the enemy. In this context, it is particularly important to analyse effective legal instruments for protecting human rights to information, including the practice of Ukrainian courts and international institutions. For example, Resolution of the Council of Judges of Ukraine No. 841-23 (2023) emphasises the importance of openness of justice and access to public information even in conditions of martial law.

Certain aspects of access to information under restrictions are also considered in court practice, as summarised by the Centre for Democracy and Rule of Law. Ukrainian courts interpret the right to access public information in conditions of security, war and restrictions. In particular, cases are considered where courts have recognised as unlawful the refusal of authorities to provide information under the pretext of martial law, if such refusal was not justified by clear legal grounds. The tendency of courts to require compliance with the principle of proportionality is noted, i.e. weighing the needs of national security against the public interest in access to information. It also emphasises the obligation of public authorities to provide reasoned responses, even in conditions of restricted access, rather than resorting to formal replies. This indicates a strengthening of the role of judicial control in the field of information rights and support for standards of openness even in exceptional circumstances O. Vashchuk-Ogdanska (2023b). At the same time, the European Court of Human Rights, in a number of cases, including *Studio Monitori and Others v. Georgia* (2020), continues to develop standards of proportionality of state interference with freedom of expression and the right to information. Taking these decisions and mechanisms into account allows to assess the effectiveness of current approaches to protecting information rights in emergency conditions, identify challenges for law enforcement, and lay the groundwork for the formation of a balanced, legal model of interaction between the state, society, and digital technologies.

Given the current challenges in the information space, it is advisable to amend Ukrainian legislation in order to specify the concepts and mechanisms for ensuring the information security of military personnel. First, Articles 1, 2, and 4 of Law of Ukraine No. 2163-VIII (2017), the concepts of “information violence”, “information manipulation” and “information displacement”

should be defined in law, and legal liability for such actions should be provided for by amending criminal and criminal procedure legislation. Secondly, it is advisable to develop a special section in Law of Ukraine No. 2657-XII "On Information" (1992) that would regulate the special regime for the circulation of personal and official data of military personnel in the digital environment during martial law. This approach is similar to the experience of Estonia, which has introduced a regime of enhanced protection of military information based on cybersecurity legislation (European Commission, 2018). Thirdly, it would be advisable to include provisions on mandatory training of military personnel in information security in the Regulations on Military Service in the Armed Forces of Ukraine by Citizens of Ukraine (2007), in particular regarding fakes, manipulation, social engineering and malicious software.

According to research, journalists and representatives of civil society organisations in Ukraine demonstrate a significant demand for raising awareness of cyber hygiene and digital security. For example, as part of the Cyber Security Talks programme organised by Internews in 2024-2025, more than 60 participants (journalists, activists, representatives of civil society initiatives) underwent training on the basics of digital hygiene, methods of protection against cyberattacks and the development of cybersecurity policies (High-quality media..., 2025). This confirms the need for regulatory oversight and the creation of institutional mechanisms to ensure coordinated action in the field of information security - for example, by creating a threat monitoring unit within the State Special Communications Service or the Ministry of Defence, modelled on the U.S. Cyber Command.

The effectiveness of the proposed changes is confirmed by the positive experience of the United States, where the Cyber Awareness Challenge programme requires all military personnel to undergo annual certification in information hygiene

(U.S. Department of Defense, 2023). A similar initiative is being implemented in Latvia as part of the Media Literacy and Information Security programme, which covers not only the military but also the civilian population. These examples prove the effectiveness of the state approach to building information resilience by combining legal regulation and educational measures.

Discussion

When analysing information rights under martial law, it is advisable to compare the results obtained with current scientific developments in this field. Based on a comprehensive interpretation of information rights as a component of national security in wartime, the study also proposes a number of new emphases, in particular, the introduction of the terms "information violence", "information manipulation" and "information displacement" into the regulatory field, which are currently absent from legislation but are actively manifested in the information environment. Meanwhile, the article by V.O. Kucher (2024) emphasises the preservation of fundamental human rights even in conditions of martial law. The analysis demonstrates the need to broaden the focus, in particular by legislating new forms of threats that are not covered by existing definitions. The author's conclusions are important in view of the principles of reasonable restriction, but do not cover the need for conceptual and terminological reform of information legislation.

The study by L.I. Rudnyk (2023) proposes a legal justification for restrictions on information rights during martial law. At the same time, these provisions are not fully consistent with the results of this study, as the author does not take into account the evolution of digital threats, in particular content aggression through algorithmic platforms. The reason for the different interpretations may lie in the methodological focus on classical mechanisms of constitutional restriction, while this study focuses on a deeper digital specification.

The statements by A.S. Chistyakova and D.V. Kostenko (2024) about the transformation of the right to information in wartime seem somewhat debatable, as the work presents mainly institutional analysis without specific proposals for modernising the content of information rights. This is inconsistent with the results of this study, which provides a systematic understanding of new forms of threats. Instead, the study by K.V. Denisenko (2023) emphasises the need to strengthen digital rights during the period of martial law, as well as the importance of adapting legal instruments to new challenges.

The work of D.V. Smotrych and L. Brailko (2023) provides a clear technical classification of information security measures, which is fully supported in this study. The authors point to the need to distinguish between protection against physical and digital threats, which is supplemented in this study by a proposal to institutionalise these mechanisms in legislation. Finally, the Article by V. Minyayluk (2024) justifies the need to update the regulatory and legal framework in terms of cyber threats and information security. However, the author's conclusions are mainly focused on the national level and do not cover aspects of the protection of individual rights, which is the key focus of the present study.

A comparison of the results of this study with current scientific approaches leads to the conclusion that although Ukrainian legal science is generally responding actively to the challenges of information security in a state of martial law, a number of important concepts, phenomena and processes remain conceptually unexplored or only fragmentarily addressed. First and foremost, there is a need for a clear regulatory definition of the latest forms of information influence, which already have practical significance but do not have the appropriate legal status. Thus, the further development of the theory and practice of information rights protection requires a

deeper understanding of new forms of digital harm, a review of legislative approaches, and the establishment of interdisciplinary cooperation between jurisprudence, cybersecurity, and information policy.

Conclusions

During the course of the work, it was possible to identify the peculiarities of regulatory and practical enforcement of information rights in conditions of extraordinary challenges, characterise the mechanisms for their restriction, and determine effective protection tools used in Ukrainian and international practice. The results of the analysis showed that information rights in the conditions of a modern digital state are of decisive importance and require comprehensive legal protection. It was established that human information rights are complex in nature: they cover both access to information and its dissemination, personal data protection, and digital security. At the same time, in a state of martial law, some of these rights are subject to restrictions on the grounds of public interest, national security, and public order. An analysis of current legislation, ECHR practice and Ukrainian courts has shown that restrictions on information rights can only be considered lawful if they comply with the so-called "three-step test" – the existence of a legal basis, a legitimate aim and proportionality of the interference. In particular, the practice of Ukrainian courts shows an attempt to strike a balance between security and openness.

It was also found that digital tools and platforms play an important role in protecting human information rights. Numerous cases have been recorded of the use of applications such as "e-Enemy" and "eyeWitness to Atrocities" to collect and record evidence of violations of international humanitarian law, which not only ensures public control but also enables the prosecution of those guilty of war crimes. It has been established that

the legal model of protection should cover not only traditional institutional mechanisms, but also the latest digital practices.

Summarising the results obtained, it can be noted that effective protection of human information rights in wartime is only possible if there is clear legal certainty regarding the limits of restrictions, judicial control over the proportionality of interventions, and adequate technical and regulatory support for digital mechanisms for recording, monitoring and preserving evidence. Positive dynamics in judicial practice regarding openness, as well as the gradual consolidation of new categories (information violence, information displacement) will demonstrate movement towards a comprehensive legal response to contemporary challenges.

Conceptually, the above indicates the need to expand Ukraine's regulatory framework in the

field of information rights protection, harmonise it with international standards, and ensure the technical and legal integration of digital tools into national security and justice systems. Further research could focus on developing criteria for assessing the effectiveness of digital tools for protecting human rights, formalising new types of information threats, and studying the impact of digital deformation of the information space on the realisation of human rights.

Acknowledgements

None.

Funding

The study was not funded.

Conflict of Interest

None.

References

- [1] Antipova, O. (2023). Strategic communications as a component of state information security. *Law Journal of the National Academy of Internal Affairs*, 13(1), 44-52. doi: [10.56215/naia-chasopis/1.2023.44](https://doi.org/10.56215/naia-chasopis/1.2023.44).
- [2] Barabash, O.O. (2024). The right to information security as a component of the human right to security: Conceptual foundations of the protection of information rights. *Legal Scientific Electronic Journal*, 2, 560-563. doi: [10.32782/2524-0374/2024-2/138](https://doi.org/10.32782/2524-0374/2024-2/138).
- [3] Bieliakov, K., Tykhomyrov, O., Radovetska, L., & Kostenko, O. (2023). Digital rights in the human rights system. *InterEULawEast: Journal for International and European Law, Economics and Market Integrations*, 10(1), 183-207. doi: [10.22598/iele.2023.10.1.10](https://doi.org/10.22598/iele.2023.10.1.10).
- [4] Chistyakova, A.S., & Kostenko, D.V. (2024). Transformation of the right to information in wartime conditions. *Legal Bulletin*, 14, 81-90. doi: [10.31732/2708-339X-2024-14-A11](https://doi.org/10.31732/2708-339X-2024-14-A11).
- [5] Chorna, V.D., & Alekseenko, I.V. (2021). [Human information rights in Ukraine: Problems of legal definition](#). In *Social and digital transformation: Theoretical and practical problems of legal regulation* (pp. 210-214). Kyiv-Odesa: Feniks.
- [6] Constitution of Ukraine. (1996, June). Retrieved from <https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text>.
- [7] Decree of the President of Ukraine No. 64/2022 "On the Imposition of Martial Law in Ukraine". (2022, February). Retrieved from <https://www.president.gov.ua/documents/642022-41397>.
- [8] Denisenko, K.V. (2023). Implementation of digital and information human rights under martial law. *Scientific Bulletin of Uzhgorod University: Series: Law*, 1(77), 90-94. doi: [10.24144/2307-3322.2023.77.1.14](https://doi.org/10.24144/2307-3322.2023.77.1.14).

- [9] Draft Law of Ukraine No. 11533 “On Amendments to the Civil Code of Ukraine and Certain Other Laws of Ukraine Regarding the Peculiarities of Providing Information on Public Electronic Registers, the Holder of which is the Ministry of Justice of Ukraine, and Certain Other Public Electronic Registers”. (2024, August). Retrieved from <https://itd.rada.gov.ua/billinfo/Bills/Card/44802>.
- [10] European Commission. (2018). *Action plan against disinformation*. Retrieved from <https://salo.li/A340c98>.
- [11] European Parliament, the Council and the Commission. (2022). *European Declaration on Digital Rights and Principles for the Digital Decade*. Retrieved from <https://salo.li/5BD61C7>.
- [12] Freedom House. (2023). *Freedom on the Net 2023: Ukraine*. Retrieved from <https://freedomhouse.org/country/ukraine/freedom-net/2023>.
- [13] General Data Protection Regulation (GDPR). (2016, April). Retrieved from <https://eur-lex.europa.eu/eli/reg/2016/679/oj>.
- [14] High-quality media – thriving communities. (2025). Retrieved from <https://internews.ua/project/programi-z-pidtrimki-regionalnih-media-u-2024-mu>.
- [15] Judgement of the European Court of Human Rights in Case No. 23806/03 “Długolecki v. Poland”. (2009, May). Retrieved from [https://hudoc.echr.coe.int/eng#{%22itemid%22:\[%22001-91475%22\]}](https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-91475%22]}).
- [16] Judgement of the European Court of Human Rights in Cases Nos. 44920/09 and 8942/10 “Studio Monitori and Others v. Georgia”. (2020, January). Retrieved from <https://salo.li/02bf068>.
- [17] Judgment of the Constitutional Court of Ukraine No. 17-пн/2010 in Case No. 1-25/2010. (2010, June). Retrieved from <http://www.ccu.gov.ua/sites/default/files/ndf/17-rp/2010.doc>.
- [18] Judgment of the Constitutional Court of Ukraine No. 26-пн/2009 in Case No. 1-50/2009. (2009, October). Retrieved from <http://www.ccu.gov.ua/sites/default/files/ndf/26-rp/2009.doc>.
- [19] Judgment of the Third Administrative Court of Appeal in Case No. 340/5136/22. (2023, March). Retrieved from <https://clarity-project.info/court/decision/109686646>.
- [20] Kucher, V.O. (2024). Human rights and information security in conditions of military aggression. *Scientific Bulletin of the Uzhhorod National University. Series Law*, 81(1), 125-130. doi: 10.24144/2307-3322.2024.81.1.19.
- [21] Kurylo, V.S., & Karaman, O.L. (2024). Security of civil society and its role in ensuring national security in the context of the war of the Russian Federation against Ukraine. *Social Pedagogy: Theory and Practice*, 3, 44-54. doi: 10.12958/1817-3764-2024-3-44-54.
- [22] Law of Ukraine No. 2163-VIII “On the Basic Principles of Ensuring Cybersecurity of Ukraine”. (2017, October). Retrieved from <https://zakon.rada.gov.ua/laws/show/2163-19#Text>.
- [23] Law of Ukraine No. 2657-XII “On Information”. (1992, October). Retrieved from <https://zakon.rada.gov.ua/laws/show/2657-12#Text>.
- [24] Law of Ukraine No. 389-VIII “On the Legal Regime of Martial Law”. (2015, May). Retrieved from <https://zakon.rada.gov.ua/laws/show/389-19#top>.
- [25] Mikhailina, T., Hotsuliak, Y., & Hel, A. (2021). Protection of the rights of subjects of information legal relations from violations on the Internet. *Entrepreneurship, Economy and Law*, 7, 62-68. doi: 10.32849/2663-5313/2021.7.10.
- [26] Minyayluk, V. (2024). On the problem of ensuring information security in the conditions of the legal regime of martial state. *Law&Border*, 4(2), 108-129. doi: 10.32453/law_border/t1b33x66.

- [27] National Scholl of Judges of Ukraine. (2024). *Digital "witnesses" of war crimes*. Retrieved from <https://nsj.gov.ua/ua/news/tsifrovi-svidki-voennih-zlochiniv/?utm>.
- [28] Office of the United Nations High Commissioner for Human Rights (OHCHR). (2024). *Human rights situation during the Russian occupation of territory of Ukraine and its aftermath: 24 February 2022 – 31 December 2023*. Retrieved from <https://ukraine.ohchr.org/en/human-rights-situation-during-russian-occupation-territory-ukraine-and-its-aftermath-EN>.
- [29] Regulations on Military Service in the Armed Forces of Ukraine by Citizens of Ukraine. (2008, December). Retrieved from <https://zakon.rada.gov.ua/laws/show/1153/2008#n17>.
- [30] Resolution of the Council of Judges of Ukraine No. 841-23. (2023, November). Retrieved from <https://zakon.rada.gov.ua/rada/show/v0008414-23#Text>.
- [31] Rudnyk, L.I. (2023) Legal principles of restricting the right to access information under martial law. *Bulletin of NTUU "KPI". Political Science. Sociology. Law: Collection of Scientific Works*, 4(60), 32-39. doi: 10.20535/2308-5053.2023.4(60).296975.
- [32] Shevchenko, T.S., & Rozkladai, I.E. (Eds.). (2012). *Freedom of expression in times of crisis*. Kyiv: Moskalenko O.M.
- [33] Smotrych, D.V., & Brailko, L. (2023) Information security in martial law. *Scientific Bulletin of Uzhhorod National University. Series: Law*, 2(77), 121-127. doi: 10.24144/2307-3322.2023.77.2.20.
- [34] Tech Ukraine. (2022). *How Ukraine is crowdsourcing digital evidence of war crimes*. Retrieved from <https://salo.li/EC51bE1>.
- [35] Tkachuk, N.I. (2018). [Human and civil information rights and freedoms in Ukraine: Definition of terms and concept correlation](#). *Information and Law*, 2(25), 17-30.
- [36] Tkachuk, T.Y. (2021). [Philosophical reflections on the information society in the context of a security-creating paradigm](#). *International Journal of Electronic Security and Digital Forensics*, 13(1), 105-113.
- [37] Tokarieva, K. (2023). [Ensuring human information rights in social networks](#). *Actual Problems of Jurisprudence*, 4, 88-93.
- [38] U.S. Department of Defense. (2023). *Cyber Awareness Challenge 2023*. Retrieved from <https://public.cyber.mil/training/cyber-awareness-challenge/>.
- [39] Vashchuk-Ogdanska, O. (2023a). *Restrictions on access to public information during war: what does judicial practice say? Access to the truth*. Retrieved from <https://dostup.org.ua/blogs/publications/obmezhenia-dostupu-do-publichnoi-informatsii-pid-chas-viiny-proshcho-hovoryt-sudova-praktyka>.
- [40] Vashchuk-Ogdanska, O. (2023b). *Judicial practice on access to public information*. Retrieved from <https://cedem.org.ua/analytics/dostupu-sudova-praktyka/>.
- [41] Włodyka, E.M. (2024). Cyber security as a research subject: Quantitative and qualitative analysis of data in Scopus database covering in 2020-2024. *Cybersecurity and Law*, 12(2), 131-145. doi: 10.35467/cal/188564.
- [42] Yadav, A.K., Singh, A.K., & Indraves. (2023). Global legal contexts for the protection of human rights: A comparative analysis. *Journal of Law and Sustainable Development*, 11(5), article number e1179. doi: 10.55908/sdgs.v11i5.1179.
- [43] Yarema, O.H. (2022). The system of legal means of ensuring information security. *Analytical and Comparative Jurisprudence*, 4, 237-241. doi: 10.24144/2788-6018.2022.04.43.

Особливості реалізації та обмеження інформаційних прав людини в умовах зовнішніх загроз та військової агресії в Україні

Олена Калмикова

Кандидат юридичних наук, професор
Національний університет біоресурсів і природокористування України
03041, вул. Героїв Оборони, 15, м. Київ, Україна
<https://orcid.org/0000-0003-2041-8925>

Володимир Савченко

Аспірант
Національний університет біоресурсів і природокористування України
03041, вул. Героїв Оборони, 15, м. Київ, Україна
<https://orcid.org/0000-0003-1254-7276>

Анотація

Актуальність обраної тематики полягає у тому, що в умовах сьогодення все більшої зацікавленості з боку наукової та законодавчої спільноти виникає до четвертого покоління прав людини, а саме інформаційних. При цьому, в умовах правового режиму воєнного стану на рівні законодавства, може бути обмежено реалізацію таких прав будь-якою людиною, проте такі обмеження мають відповідати певним критеріям. Метою дослідження була оцінка обмежень інформаційних прав людини в умовах війни крізь призму сучасних теоретичних концепцій захисту цих прав. В роботі були використані наступні методи: формально-юридичний, системно-структурний, прогностичний. Визначено, що обмеження інформаційних прав людини в умовах воєнного стану мають відповідати критеріям доступності, зрозумілості, збереження балансу приватних та публічних інтересів, пропорційності та мати легітимну та достатньо обґрунтовану мету. Підсумовано, що основними заходами (інструментами) захисту інформаційних прав людини в умовах воєнного стану мають бути дії громадянського суспільства. Аналіз досвіду країн НАТО (США, Естонії, Латвії) засвідчив ефективність інтегрованого підходу, який об'єднує законодавче регулювання з освітніми заходами та інституційною підтримкою. Результати дослідження підтверджують актуальність зазначених змін. Зроблено висновок, що лише комплексна модернізація нормативної бази, освітньої системи та інституційного забезпечення дозволить ефективно захистити інформаційні права людини в умовах сучасних гібридних викликів. Результати цієї роботи можуть бути використані для опрацювання нормативно-правових та підзаконних нормативно-правових актів щодо захисту інформаційних прав людини

Ключові слова: інформація; інструменти захисту; обмеження інформаційних прав; інформаційне суспільство; безпека