

DOI: <https://doi.org/10.34069/AI/2023.69.09.18>

How to Cite:

Onyshchenko, S., Burbii, A., Boikov, A., Riabiy, S., Korniiiko, S. (2023). Personal data protection on the internet under martial law: The case of Ukraine. *Amazonia Investiga*, 12(69), 204-215. <https://doi.org/10.34069/AI/2023.69.09.18>

Personal data protection on the internet under martial law: The case of Ukraine

Захист персональних даних в Інтернеті в умовах воєнного стану: приклад України

Received: August 1, 2023

Accepted: September 24, 2023

Written by:


Serhii Onyshchenko¹ <https://orcid.org/0000-0002-9944-5995>**Anastasiia Burbii²** <https://orcid.org/0000-0003-4866-321X>**Andrii Boikov³** <https://orcid.org/0000-0001-7439-1452>**Serhii Riabiy⁴** <https://orcid.org/0000-0002-7854-4193>**Stanislav Korniiiko⁵** <https://orcid.org/0000-0003-1266-8166>


Abstract


The *objective* of this study is to determine the threats to the security of personal data on the Internet as a component of the right to privacy in the conditions of martial law, characteristics and prospects of such legal data protection in the context of Ukraine. *Methodology*: The study used a set of practical methods, namely: formal and legal, comparative forecasting. These methods were used to examine and classify threats to the security of personal data on the Internet under martial law conditions. *Results*: The study identified a number of threats to the security of personal data on the Internet under martial law conditions, including: unauthorized access to personal data, alteration or destruction of personal data, disclosure of personal data to third parties without the consent of the data owner, use of personal data for unlawful purposes. The study also examined factors that complicate data protection during cross-border sharing, including: differences in data protection


Анотація


Метою дослідження є визначення загроз безпеці персональних даних в мережі Інтернет як складової права на приватність в умовах воєнного стану, особливостей та перспектив такого правового захисту даних в умовах України. *Методологія*: У дослідженні використовувався комплекс практичних методів, а саме: формально-правовий, порівняльно-прогнозний. Ці методи були використані для вивчення та класифікації загроз безпеці персональних даних в Інтернеті в умовах воєнного стану. *Результати*: Дослідження виявило низку загроз безпеці персональних даних в Інтернеті в умовах воєнного стану, серед яких: несанкціонований доступ до персональних даних, зміна або знищення персональних даних, розголошення персональних даних третім особам без згоди власника даних, використання персональних даних у протиправних цілях. Дослідження також вивчало фактори, які ускладнюють

¹ PhD in Science of Law, Leading Researcher, Department of Scientific and Organizational, State Scientific Research Institute of the Ministry of Internal Affairs, Kyiv, Ukraine.  WoS Researcher ID: B-2605-2019

² PhD in Science of Law, Senior Researcher, Department of Scientific and Organizational, State Scientific Research Institute of the Ministry of Internal Affairs, Kyiv, Ukraine.  WoS Researcher ID: IQV-5086-2023

³ PhD in Science of Law, Senior Researcher, Department of Scientific and Organizational, State Scientific Research Institute of the Ministry of Internal Affairs, Kyiv, Ukraine.  WoS Researcher ID: IQW-4697-2023

⁴ PhD in Science of Law, Head of the 3rd Research Department, Research Laboratory of Forensic and Special Equipment, State Scientific Research Institute of the Ministry of Internal Affairs, Kyiv, Ukraine.  WoS Researcher ID: IQW-1122-2023

⁵ PhD in Juridical Sciences, Research Officer, State Scientific Research Institute of the Ministry of Internal Affairs, Kyiv, Ukraine.  WoS Researcher ID: IQV-5116-2023



laws and regulations between countries, lack of cooperation between governments on data protection, the complexity of cross-border data exchange processes. *Conclusions:* The findings of the study suggest that increasing the protection of personal data under martial law conditions requires a comprehensive approach that includes regulatory, organizational and communication measures. In particular, it is necessary to: strengthen data protection legislation under martial law conditions, develop cooperation mechanisms between governments on data protection, promote data protection education and awareness among citizens and organizations.

Keywords: right to privacy, personal data, Internet protection, martial law, legal regulation.

Introduction

Back in the early 80s of the 20th century, the urgency of introducing legal mechanisms for privacy protection became evident when the automated processing of personal data became widespread. The ground for this requirement is considered to be the Convention of the Council of Europe on the protection of individuals in connection with automated processing of personal data (GIP Digital Watch, n.d.). Further, a new stage was the Charter of Fundamental Rights of the EU, Article 8 of which set out the right to the protection of personal data as a right that belongs to every person and the need to create an independent body to comply with the rules of its protection (European Union, 2012). With that in mind, it was recognized that the ECtHR should also play an important role (Eskens, 2020, 1118).

Subsequently, independent rules on data protection and processing were adopted in the EU. Accordingly, the main data protection instruments in the EU are considered to be as follows: the General Data Protection Regulation, the Law Enforcement Directive and the ePrivacy Directive. That being said, the Regulation on data protection of EU institutions, bodies, offices and agencies was adopted for the processing of personal data, which was established as the basis for the work of EU institutions when personal data are processed (Jørgensen, 2019, 270; European Commission, 2022, 3).

Notably, up to date privacy, data protection and security of systems, networks and data are

захист даних під час транскордонного обміну даними, зокрема: відмінності в законах і нормативних актах щодо захисту даних між країнами, відсутність співпраці між урядами щодо захисту даних, складність процесів транскордонного обміну даними. *Висновки.* Результати дослідження свідчать про те, що підвищення захисту персональних даних в умовах воєнного стану потребує комплексного підходу, який включає нормативні, організаційні та комунікаційні заходи. Зокрема, необхідно: посилити законодавство про захист даних в умовах воєнного стану, розробити механізми співпраці між урядами щодо захисту даних, сприяти освіті та обізнаності громадян та організацій з питань захисту даних.

Ключові слова: право на приватність, персональні дані, захист в мережі Інтернет, воєнний стан, правове регулювання.

interdependent phenomena. On the other hand, legal framework is not always adapted to modern computer technologies (Clifford, 2014; Hobokena van & Fathaigh, 2021). At the same time, the development of artificial intelligence gives rise to a wide array of issues related to cyber security. Given the above, the adoption of normative acts in the field of cyber security overall should contribute to the reduction of threats (Mendoza, 2017).

However, the regulation of information security, cyber security, and network security basically does not affect national security issues (Azfar et al., 2018). Accordingly, the protection of personal data on the Internet in the conditions of martial law in rare cases becomes the subject of a scholarly inquiry. From this perspective, of certain relevance to the abovementioned context are intelligence on the peculiarities of working with personal data of persons who are cared for by the International Organization for Migration (2010), following their relocation as a result of armed conflicts.

Notably, all professional and normative regulatory materials are considered to be applicable, although they either relate to peacetime or focus on victims of armed conflict. In the conditions of martial law, an array of threats to the security of personal data and the range of vulnerable persons are more extensive. Martial law creates a new reality in which personal data requires increased protection.

One of the vivid examples that emphasize the need for increased attention to the protection of personal data on the Internet in the conditions of martial law is the situation that has developed today in Ukraine. The experience of the war in Ukraine testifies to the active use of the information space to harm the national security and defense capability of the country as a whole, as well as to commit cybercrimes against individuals. Particularly important in this context is the study of the specifics of the legal mechanism for the protection of personal data on the Internet in the conditions of martial law in the country, as well as the formation of a list of directions for improving such a mechanism.

Hence, the argument in favor of conducting an analysis of the status quo and prospects of the legal mechanism for personal data protection on the Internet in the conditions of martial law is of considerable relevance. From this perspective, it is extremely salient both for Ukraine and for the partners of our state.

Purpose

The purpose of this study is to distinguish the features and prospects for enhancing the legal protection of personal data on the Internet under martial law. In order to achieve it, the following tasks have been set: a) to identify the significance of the right to the protection of personal data in the right to privacy; b) to determine the components of legal mechanism of personal data protection; c) to identify the specifics and set out the classification of the principal threats to the security of personal data on the Internet in the conditions of martial law (using the example of Ukraine); d) to outline the peculiarities of legal protection of personal data in the conditions of martial law and the prospects for improving such protection.

Literature Review

Further research on the outlined topic requires clarification of the basic concepts. Given the choice of Ukraine as the main object of the study, it is proposed to define in accordance with the country's current legislation. So, it is worth outlining the essence of the following key terms:

Confidential information is data, access to which is limited to an individual or legal entity, with the exception of subjects of authority, and which can be distributed in the order determined by them at their will in accordance with the conditions stipulated by them (Law No. 2939-VI, 2023a).

The protection and processing of personal data consists, first of all, of the protection of the fundamental rights and freedoms of a person and a citizen (in particular, such as the right to non-interference in personal life) in connection with the processing of personal data (Law of Ukraine No. 2297-VI, 2010).

Martial law consists of the introduction of a special legal regime in Ukraine or in certain areas of the country in case of armed aggression or threat of attack. Such a regime, among other things, provides for a temporary restriction of the constitutional rights and freedoms of a person and a citizen, as well as the rights and legitimate interests of legal entities caused by a threat (Law No. 389-VIII, 2023b).

In addition, for a better understanding of the subject of research, it is important to outline the range of key threats to the security of personal data on the Internet. They include:

- unauthorized access, processing and publication – involves illegal actions aimed at obtaining access to personal data or their processing and publication without the permission of the owner;
- inadequate data protection by organizations processing personal data, as well as inadequate data security during transmission;
- storage of data beyond the stipulated terms (violation of storage terms);
- cross-border exchange that does not meet the requirements of Ukrainian legislation, etc.

In scholarly research into personal data protection, the sequence as follows can be observed: the right to protect personal data on the Internet as a component of the right to privacy - the legal mechanism for protecting such data - the specifics of the principal threats to the security of personal data on the Internet under martial law - the features of enhancing the legal protection of personal data.

1. Research into the relationship between privacy and data protection yielded the findings that these are two interrelated issues of Internet management (GIP Digital Watch, n.d.). Although the definition of personal data was standardized in international documents a long time ago (OECD Legal Instruments, 1980; European Union, 2012), the present-day classification of the data requires a thorough clarification of the personal data concept due to the emphasis laid on the personal interest of the subject

who is affected by their operation (Yuming, 2019, 95).

2. An important aspect of understanding the legal mechanism for the protection of personal data on the Internet is the vision of threats to their security, such as follows: a) threats in the business sphere, owing to the fact that personal data comprises both a new type of resource (Yuming, 2019, 94, 95) as well as an element of interaction with customers (Urquhart et al., 2018, 317), who may be abused by companies (UN General Assembly, 2013); b) threats to freedom of information and expression of opinion (Farinpour, 2021, 368); c) cybercrime (Bentotahewa et al., 2022, 14); d) threats related to artificial intelligence (GIP Digital Watch, n.d.; Pollicino, 2021).

The legal mechanism of personal data protection on the Internet is in itself a complex phenomenon, which encompasses a regulatory framework, a subject, an operator and a data controller with a predefined range of their rights, obligations and liability for violations (OECD Legal Instruments, 1980; Law of Ukraine No. 2297-VI, 2010; Yuming, 2019). That being said, experts underline the utmost relevance of regulatory support (Kaurin, 2019, 2; Bentotahewa et al., 2022, 3). On the other hand, the leading role of the European legal field is recognized (McKay, 2018), attention is drawn to the practice of the ECtHR regarding the protection of personal data (Council of Bars & Law Societies of Europe, 2019, 7; Hörnle, 2019), which contributed to the reform of the legal mechanism of such protection in EU member states (López, 2022).

Despite their rigid character, European standards have become a reference point for the commercial legislation of other countries, such as for instance, Britain and Japan (Bentotahewa et al., 2022, 4). Accordingly, the EU law developed to be a global regulator (Hadjiyianni, 2021), which enabled international transfers of personal data (European Commission, 2022, 9).

The USA elaborated their own approach to personal data protection. On the one hand, it is characterized by certain features such as a greater involvement of the private sector and self-regulation opportunities, and on the other, in the differentiation of confidentiality rules for each sector of the economy. Still, it should be mentioned that this approach allows finding a balance with European economic partners and ensuring the needs of the national security sector (Mendoza, 2017; GIP Digital Watch, n.d.). Using

the said approach would make it possible to operate with the wide bulk of information collected by special services to combat crimes (Zhalimas, 2019, 82).

However, certain problems are inherent in each of the aforementioned approaches, in particular, as follows:

- the inconsistencies of legal regulation. For the EU, these are internal (between member states) and external ones (between the EU and third countries) (Hörnle, 2019);
 - the lack of balance between the state and the private sector (United Nations, 2010, 4; Mendoza, 2017; Hobokena van & Fathaigh, 2021);
 - the choice between economic incentives to protect personal data and the use of considerable fines (McKay, 2018; GDPR.EU, 2018; Singh, 2023).
3. The specifics of the principal threats to personal data security on the Internet in the conditions of martial law emerge from the specifics of such a state. It is a consequence of the most significant threats to national security in the form of an actual or potential armed conflict (Martial Law). What is more, the major problem is the difficulty of finding a balance between private interests and national security, because the situation may justify stricter restrictions on the right to privacy (Council of Europe, 2006; Bentotahewa et al., 2022, 15). The interpretation of this issue can be considered such a threat as the imperfection of normative regulation and the possible abuse of power by state bodies (Christakis & Bouslimani, 2021). Furthermore, Ukraine's experience has shown the relevance of such threats as cyber attacks and hacking by the enemy. In sum, cybercrime during modern armed conflict is currently gaining in its importance (Veselovska et al., 2022, 86).
 4. Although experts do not address the specifics of the legal mechanism for personal data protection on the Internet in the conditions of martial law, certain conclusions can nevertheless be drawn from the existing proposals for enhancing the protection of such data. Notably, they reflect international trends in legal regulation, even those related to technological developments (Kuner & Marelli, 2020, 42). The particular emphasis is placed on the following activities: a) the formation of a common cyber security space at the global and regional levels (Bentotahewa et al., 2022,

15); b) the introduction of a flexible system of personal data security examination; c) the elaboration of a criminological classification in terms of violating such security on the Internet (Veselovska et al., 2022, 89); d) empowering the educational area (e.g., Harvard Online Course, 2023).

Thus, the specifics of the legal mechanism of their protection in the conditions of martial law have not been subjected to a thorough analysis. Accordingly, a research gap has emerged, the elimination of which is of considerable theoretical and practical value.

Methods

In order to achieve the purpose of the study and address research tasks, the selection and generalization of sources that highlight the legal and organizational issues of the functioning of the personal data protection mechanism on the Internet was accomplished. Accordingly, the sources were used in the study for the following purposes:

- a) global and regional legal acts - in order to determine the context and norms that determine the legal status of personal data protection at the international and regional levels; ECtHR practice – to gain insights into the interpretation and application of

human rights in the context of personal data protection;

- b) analytical reports and recommendations of experts regarding the current state and prospects for the development of the legal mechanism for the protection of personal data on the Internet - for the purpose of objective analysis of the current state and directions of development of the legal mechanism for the protection of personal data on the Internet, as well as the formation of proposals;
- c) regulatory documents and experience of Ukraine regarding the protection of personal data during martial law - to understand specific challenges and approaches to the protection of personal data during martial law (Commissioner of the Verkhovna Rada of Ukraine on human rights, 2022).

Such an approach made it possible to a) generalize state-of-the-art approaches to perceiving personal data on the Internet as a component of the right to privacy; b) identify the specifics of martial law impact upon threats to the security of such data and the factors that determine the specifics of the legal mechanism for the protection of such data under martial law, taking into account the experience of Ukraine; c) to outline the principal prospects for enhancing the efficiency of such a mechanism in the conditions of martial law (Figure 1).

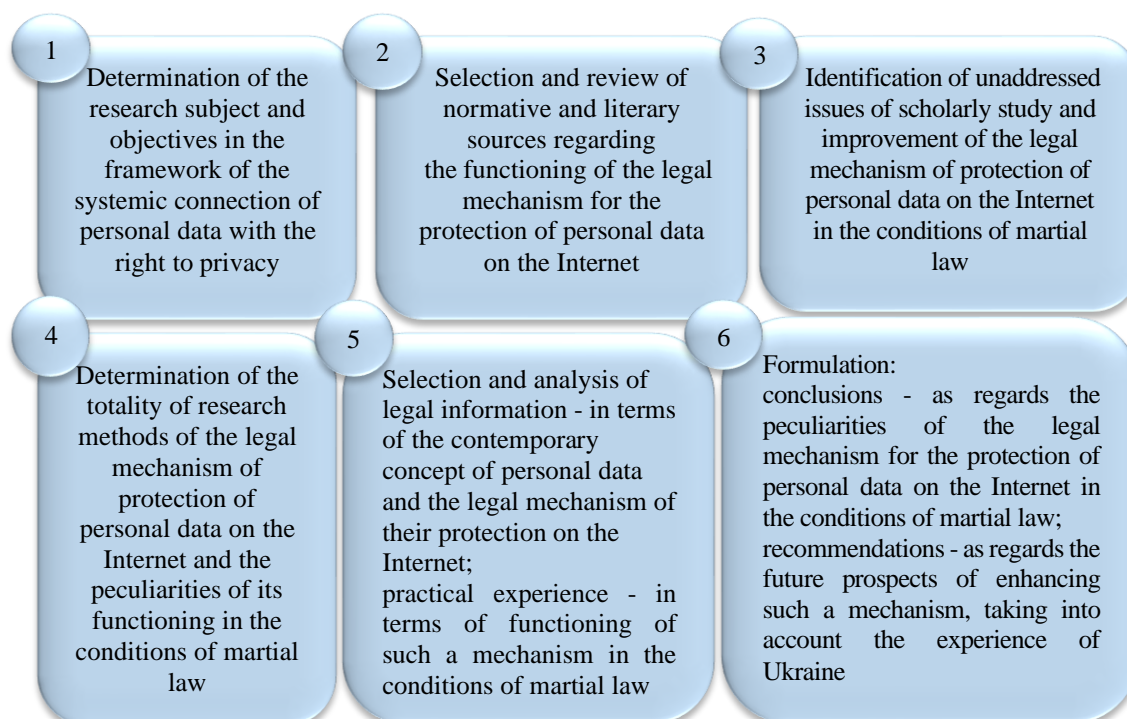


Figure 1. Flowchart of the study
Source: (developed by authors)

The following methods were used in the current study:

- *the system approach method* was applied in order to: a) systematize the approaches to understanding personal data, which made it possible to identify socially significant rights and values that are in conceptual conflict with the protection of personal data (from the point of view of economic and humanitarian approaches); b) form of an extensive classification of threats to the security of personal data, including in the conditions of martial law, with the aim of deepening their understanding, origin and types;
- *the method of descriptive analysis* was used in the process of identifying factors that determine the specificity of the legal mechanism for the protection of personal data in the conditions of martial law, which made it possible to classify and justify such factors;
- *the formal-legal method* contributed to systematization of the key provisions of

normative legal acts in the field of functioning the legal mechanism for the protection of personal data, including in the conditions of martial law, which made it possible to characterize the current state of the problem and identify opportunities for improvement;

- *the comparative forecasting method* enabled comparing foreign approaches to the protection of personal data on the Internet, expert recommendations and Ukraine's experience, which made it possible to identify useful examples and prospects for improving the legal mechanism for the protection of personal data on the Internet in the conditions of martial law for Ukraine.

Results

To consider the peculiarities of the legal mechanism for the personal data protection on the Internet in the conditions of martial law, it is expedient to refer to the state-of-the-art perspective on personal data (see Figure 2).

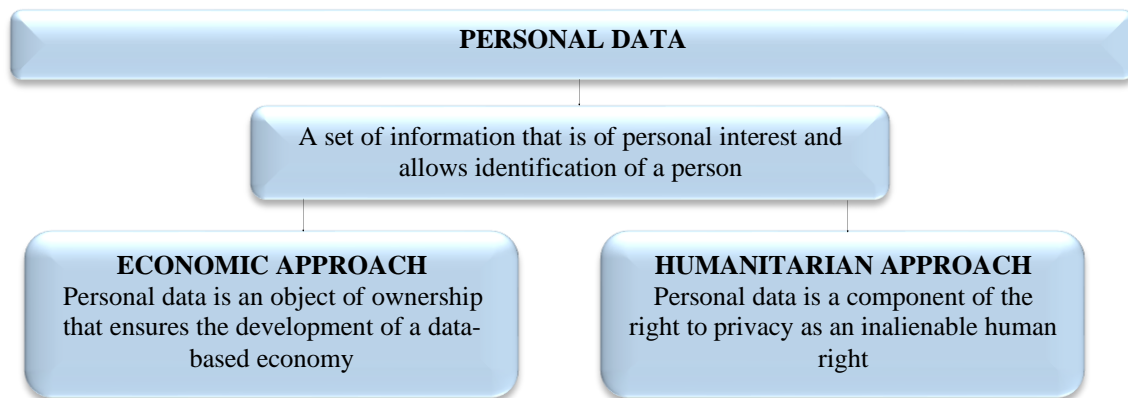


Figure 2. Basic approaches to understanding personal data
Source: (developed by authors)

The presented chart makes it possible to outline those socially significant rights and values that are in conceptual conflict with the personal data protection as follows:

- within the framework of the economic approach, this is the freedom of economic exchange;
- within the humanitarian approach, it is national security as juxtaposed to privacy.

In the context of this study, it is appropriate to rely on a humanitarian approach, emphasizing that martial law justifies strict restrictions on human rights in favor of national security.

However, this does not negate the requirements of personal data protection.

In the conditions of martial law, specific threats to the security of personal data appear. They are multifaceted; their impact on national security and on the security of individuals' personal data is systemic. Let us present the classification of these threats on different grounds (see Figure 3).

While classifying the threats according to subjects whose personal data are at risk in a state of war, special attention should be paid to the most vulnerable individuals. Among civilians, these include minors, while among military personnel - war prisoners. The specificity of both

abovementioned groups of subjects lies in the fact that their representatives cannot independently make decisions as regards the disposal of their own personal data. Obviously, they are particularly vulnerable to manipulation and intimidation.

Regarding the types of illegal actions on the Internet and the territory from which the threats originate, the experience of the war in Ukraine shows that virtual space is actively used both to harm the country's defense capabilities and to commit self-serving cybercrimes against individuals.

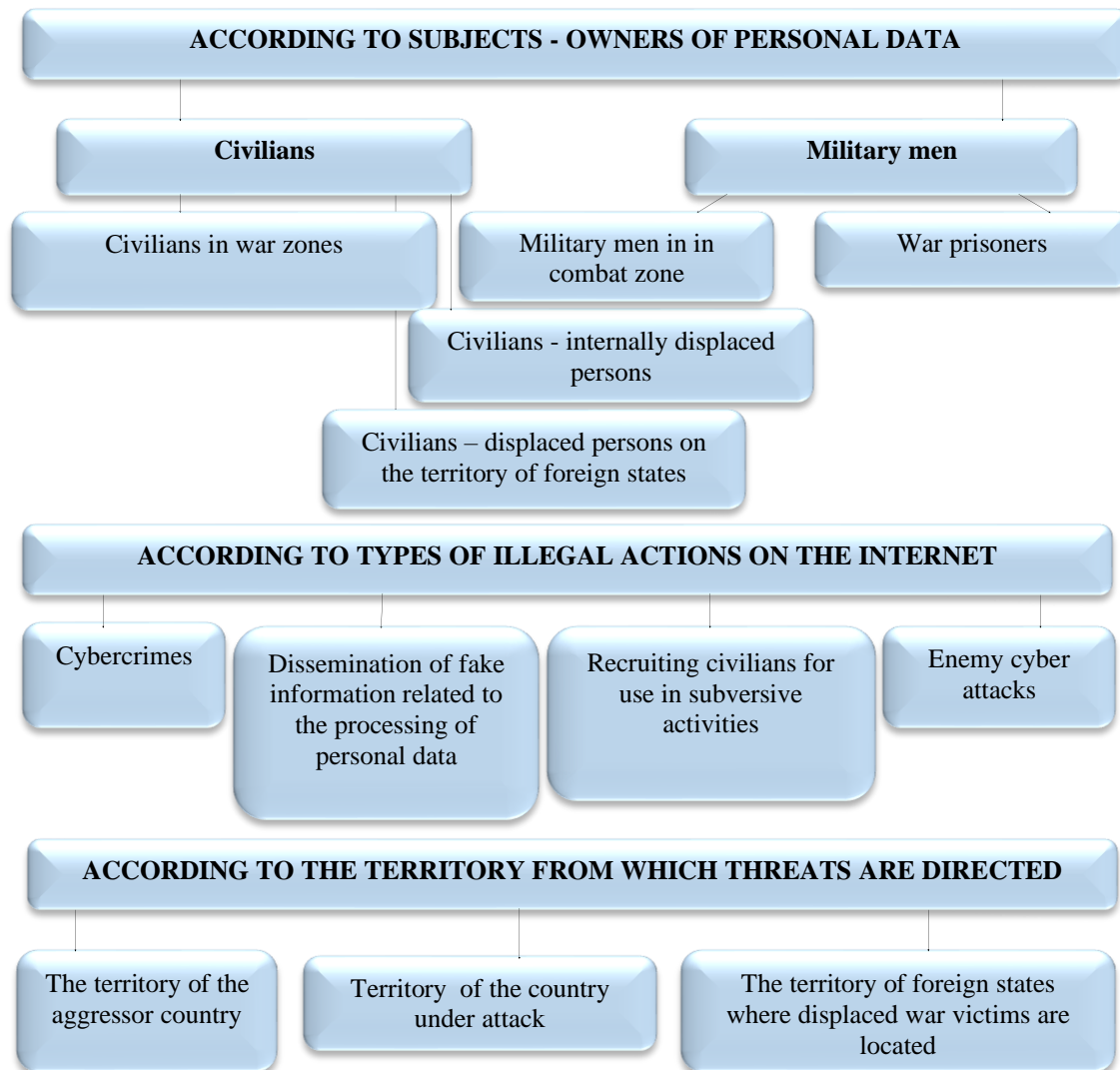


Figure 3. Classification of threats according to security of personal data in the conditions of contemporary armed conflict
 Source: (developed by authors)

The specificity of the legal mechanism for personal data protection on the Internet in the conditions of martial law is not related to its structure but to the organizational and legal aspects of individual elements and their content.

Taking into account the experience of Ukraine, it is expedient to consider the factors that determine this specificity (see Figure 4).

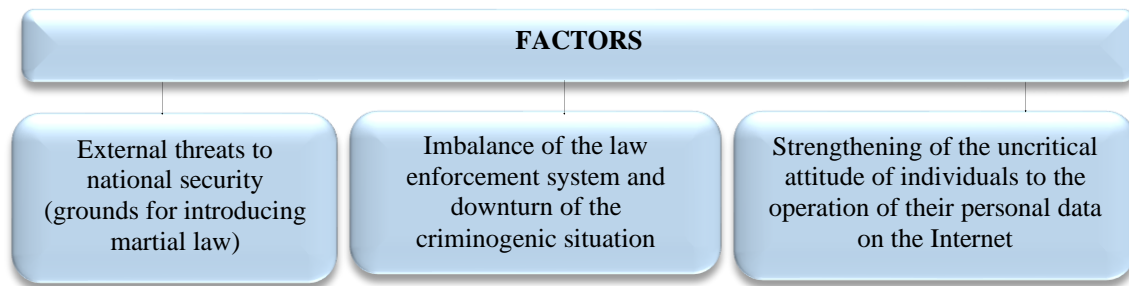


Figure 4. Classification of factors that determine the specificity of the legal mechanism for the protection of personal data in the conditions of martial law (on the example of Ukraine)

Source: developed by authors

In the conditions of martial law, the task of personal data cross-border exchange for law enforcement and humanitarian purposes is gaining growing urgency. In fact, the participants of cross-border exchange are not only state institutions, but also international organizations

that provide humanitarian aid and support to victims of war both on the territory of the country that is subject to aggression and on the territory of other states, including the aggressor state. This feature is basically due to the specific goals of such an exchange (see Figure 5).

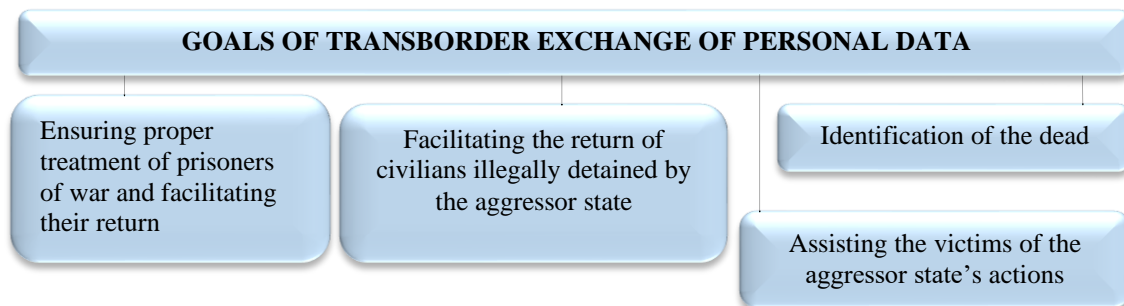


Figure 5. Major goals of cross-border exchange of personal data in martial law conditions

Source: (developed by authors)

The protection of personal data during such cross-border exchange is notably made harder by the factors as follows:

- vulnerability of electronic communication systems of a country under martial law;
- differing operation and protection modes of personal data in foreign states, on the territory of which the displaced persons are located;
- the difficulty of personal data processing and storage monitoring by international organizations involved in humanitarian missions.

Hence, in the conditions of martial law, it is expedient to form such a protection system, in which the state will act as the main controller of handling personal data and the guarantor of their protection. To some extent, it is expedient to extrapolate elements of the US approach in terms of coordinating intelligence and defense actions and involving the relevant data from intelligence agencies to prevent cybercrimes.

Taking into account the aforementioned, in view of the experience of Ukraine, it is possible to set forth the principal areas of enhancing the legal mechanism for the protection of personal data on the Internet in the conditions of martial law (see Table 1).

Table 1.

Promising directions for enhancing the legal mechanism for personal data protection on the Internet in the conditions of martial law (the case of Ukraine)

Promising directions	Content
Normative and legal	<ol style="list-style-type: none"> 1. Prompt entering of changes to legal documents regarding work with personal data, taking into account European standards and US experience. 2. Strengthening the responsibility of personal data security as regards their protection requirements violation.
Organizational and legal	<ol style="list-style-type: none"> 1. Enhancing the work of relevant law enforcement units and special bodies, taking into account the latency of personal data security violations on the Internet. 2. Intensification of work with public institutions to identify relevant violations.
Communicative	<ol style="list-style-type: none"> 1. Interaction with international and foreign partners regarding compliance with personal data security during cross-border exchanges. 2. Intensification of communication and educational work with individuals possessing the corresponding personal data.

Source: collected and structured by authors

That being said, the implementation of the above measures will contribute to the protection of personal data. There are also opportunities to supplement international and European standards, taking into account the peculiarities of contemporary armed conflicts.

Taking into account the above, it is possible to distinguish the following prospects: a) improvement of the national legal mechanism for the protection of personal data on the Internet in the conditions of martial law, drawing on the European standards and foreign experience; b) elaboration of a unified European policy for the protection of personal data on the Internet, taking into consideration the peculiarities of international armed conflicts.

Discussion

The analysis of the legal mechanism for the protection of personal data on the Internet involves consideration of a wider context. The current article shares the standpoint that personal data and their protection are part and parcel of the right to privacy (GIP Digital Watch, n.d.; UN Commission on Human Rights, 1998; UN General Assembly, 2013).

The overall perspective regarding the expediency of considering the functioning of the legal mechanism for the protection of personal data on the Internet through the prism of threats to their security has found extensive coverage in scholarly literature (e.g., Urquhart et al., 2018; Farinpour, 2021). On the other hand, the current study proves that such a vision of threats does not correspond to the conditions of martial law. Currently, armed conflicts produce specific

threats in present-day realia. At the same time, the need to take into account the special needs of vulnerable persons is emphasized (in particular, minors and war prisoners).

The vision of the legal mechanism structure for the protection of personal data (OECD Legal Instruments, 1980) with a heavy focus on the relevance of normative and legal support is substantiated (Kaurin, 2019, 2; Bentotahewa et al., 2022, 3). Alongside with the said standpoint, the current study proves that the specificity of this mechanism in the conditions of martial law is related to the organizational and legal aspects of the functioning of individual elements and their content. Taking into account the experience of Ukraine, the classification of factors that determine this specificity is presented.

The position regarding the significance of control functions in legal mechanism for the protection of personal data on the Internet is supported (Bentotahewa et al., 2022). That said, taking into account the conditions of martial law, the expediency of implementing the US approach is emphasized, within which due attention is devoted to observing the national security interests (Killam, 1989; Mendoza, 2017). Accordingly, it is justified that in the conditions of martial law it is the state that should act as the principal controller of handling personal data and the guarantor of their protection.

While sharing the engagement in cross-border exchange of personal data in the field of law enforcement (European Commission, 2022, 14-15; European Parliament and of the Council, 2016), the present article significantly expands this issue with an indication of the factors that

complicate the protection of personal data during such an exchange, specifically under martial law conditions.

The relevant scholarly research into the issue of enhancing the legal mechanism for personal data protection is presented in literature on the topic (for instance, Bentotahewa et al., 2022). However, the current study emphasizes that the gap of covering the issues of martial law has not been bridged. Therefore, it is relevant to support the positions of authors who study the experience of Ukraine (for instance, Veselovska et al., 2022, 89). The current study emphasizes the expediency of comprehensive regulatory, organizational, as well as communication measures to be taken. It is proposed to scaffold the elaboration of a unified European policy for the protection of personal data on the Internet, taking into account the characteristic features of international armed conflicts.

Conclusions

It was determined that the legal regulation of personal data protection and professional intelligence do not cover the specifics of a state of war, although certain international organizations, such as IOM for instance, have experience in handling personal data of persons displaced during armed conflicts. As for the practice of foreign countries, the legal framework of the EU is mainly focused on ensuring economic activity, in the USA considerably more attention is devoted to the protection of personal data drawing on the national security interests.

It is shown that the right to personal data and their protection is an indispensable component of the right to privacy. That said, in the conditions of martial law, public interests still have priority. Accordingly, it is concluded that the legal mechanism of their protection in the conditions of martial law relies on the specifics of threats to the security of personal data, related to the organizational and legal aspects in functioning of its individual elements and their content. It is emphasized that the relevance of cross-border personal data exchange for law enforcement and humanitarian purposes is gaining its significance. Moreover, the factors that complicate the protection of personal data during such an exchange are highlighted. It is substantiated that in the conditions of martial law, it is the state that should act as the principal controller of handling personal data and the guarantor of their protection.

Taking into account the experience of Ukraine, promising directions for enhancing the legal mechanism for protecting personal data on the Internet are outlined. Further perspective is aimed at fostering the effectiveness of the national legal mechanism for such protection. It is also expedient to form a unified European policy for the protection of personal data on the Internet, taking into account the specific features of international armed conflicts.

Bibliographic references

- Azfar, A. M., Zhou, R., Wang, D., & Fahad, A. (2018). Mapping the knowledge of national security in 21st century a bibliometric study. *Cogent Social Sciences*, 4(1), 1542944. <https://doi.org/10.1080/23311886.2018.1542944>
- Bentotahewa, V., Hewage, Ch., & William, J. (2022). The Normative Power of the GDPR: A Case Study of Data Protection Laws of South Asian Countries. *SN Computer Science*, 3(183). <https://doi.org/10.1007/s42979-022-01079-z>
- Christakis, Th., & Bouslimani, K. (2021). National Security, Surveillance, and Human Rights. In: R. Geiß & N. Melzer (Eds.). *The Oxford Handbook of the International Law of Global Security* (pp. 38-84). <https://doi.org/10.1093/law/9780198827276.003.0039>
- Clifford, D. (2014). EU Data Protection Law and Targeted Advertising: Consent and the Cookie Monster - Tracking the crumbs of online user behavior. *Journal of Intellectual Property, Information Technology and E-Commerce Law*, 5(3). Retrieved from <https://www.jipitec.eu/issues/jipitec-5-3-2014/4095>
- Commissioner of the Verkhovna Rada of Ukraine on human rights. (2022). Regarding the protection of personal data in the conditions of martial law. [File PDF]. Retrieved from <http://surl.li/gapoz>
- Council of Bars & Law Societies of Europe. (2019). *CCBE Recommendations on the Protection of Fundamental Rights in the Context of 'National Security'*. <https://acortar.link/F4hvRt>
- Council of Europe. (2006). *Opinion on the Protection of Human Rights in Emergency Situations adopted by the Venice Commission at its 66th Plenary Session*. Retrieved from [https://www.venice.coe.int/webforms/documents/CDL-AD\(2006\)015.aspx](https://www.venice.coe.int/webforms/documents/CDL-AD(2006)015.aspx)
- Esken, S. (2020). The personal information sphere: An integral approach to privacy and related information and communication

- rights. *The Journal of the Association for Information Science and Technology*, 71, 1116-1128.
<https://doi.org/10.1002/asi.24354>
- European Commission. (2022). *First report on the application of the Data Protection Regulation for European Union institutions, bodies, offices and agencies (Regulation 2018/1725)*. Retrieved from <https://acortar.link/PxrVBo>
- European Parliament and of the Council. (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*. Retrieved from <https://eur-lex.europa.eu/eli/reg/2016/679/oj>
- European Union. (2012). Charter of Fundamental Rights of the European Union. *Official Journal of the European Union*, C326, 391-407. Retrieved from <https://acortar.link/jAkrP9>
- Farinpour, R. (2021). A snapshot of recent developments regarding EU counterterrorism policies and legislation. *ERA Forum*, 22, 363-370. <https://doi.org/10.1007/s12027-021-00694-2>
- GDPR.EU. (2018). *What are the GDPR Fines?* Retrieved from <https://gdpr.eu/fines/>
- GIP Digital Watch. (n.d.). *Privacy and data protection*. Retrieved from <https://dig.watch/topics/privacy-and-data-protection>
- Hadjiyianni, I (2021). The European Union as a Global Regulatory Power. *Oxford Journal of Legal Studies*, 41(1), 243-264. <https://doi.org/10.1093/ojls/gqaa042>
- Harvard Online Course. (2023). *Data Privacy and Technology*. Retrieved from <http://surl.li/htlxb>
- Hobokena van, J., & Fathaigh, R. Ó. (2021). Smartphone platforms as privacy regulators. *Computer Law & Security Review*, 41, 105557. <https://doi.org/10.1016/j.clsr.2021.105557>
- Hörnle, J. (2019). Juggling more than three balls at once: multilevel jurisdictional challenges in EU Data Protection Regulation. *International Journal of Law and Information Technology*, 27(2), 142-170. <https://doi.org/10.1093/ijlit/eaz002>
- International Organization for Migration. (2010). *IOM Data Protection Manual*. Retrieved from <https://publications.iom.int/books/iom-data-protection-manual>
- Jørgensen, R. F. (Ed.). (2019). *Human rights in the age of platforms*. Cambridge, MA: The MIT Press.
- Kaurin, D. (2019). Data Protection and Digital Agency for Refugees. *World Refugee Council Research Paper*, 12.
- Killam, E. W. (1989). Martial Law in Times of Civil Disorder. *Law and Order*, 37(9), 44-47. Retrieved from <https://acortar.link/nQK5Km>
- Kuner, Ch., & Marelli, M. (Eds.). (2020). *Handbook on Data Protection in Humanitarian Action. 2nd ed. International Committee of the Red Cross*. <https://acortar.link/beIY7q>
- Law of Ukraine No. 2297-VI. On the protection of personal. *Verkhovna Rada of Ukraine*, dated June 1, 2010. Retrieved from <https://zakon.rada.gov.ua/laws/show/2297-17#Text>
- Law No. 2939-VI. On access to public information. *Verkhovna Rada of Ukraine*, as of October 8, 2023. Retrieved from <https://zakon.rada.gov.ua/laws/show/2939-17#Text>
- Law No. 389-VIII. On the legal regime of martial law. *Verkhovna Rada of Ukraine*, as of October 19, 2023. Retrieved from <https://zakon.rada.gov.ua/laws/show/389-19#Text>
- López, M. L. V. (2022). Spanish criminal procedure examined: successes, opportunities and failures in the adaptation to EU requirements. *ERA Forum*, 23, 127-139. <https://doi.org/10.1007/s12027-022-00698-6>
- McKay, C. (2018). Complying with International Data Protection Law. *University of Cincinnati Law Review*, 84(2), Art. 4. Retrieved from <https://scholarship.law.uc.edu/uclr/vol84/iss2/4>
- Mendoza, M. A. (2017). *Challenges and implications of cybersecurity legislation*. Welivesecurity. Retrieved from <https://acortar.link/L0eRW8>
- Pollicino, O. (2021). *Digital Private Powers Exercising Public Functions: The Constitutional Paradox in the Digital Age and its Possible Solutions*. ECHR. Retrieved from <https://acortar.link/6Yc7DJ>
- OECD Legal Instruments. (1980). *Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*. Retrieved from <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188>
- Singh, K. (2023). *Microsoft to pay \$20 million to settle US charges for violating children's*

- privacy. Reuters. Retrieved from <https://acortar.link/nruAaL>
- UN Commission on Human Rights. (1998). *Report of the Representative of the Secretary-General, Mr. Francis M. Deng, submitted pursuant to Commission resolution 1997/39. Addendum: Guiding Principles on Internal Displacement.* E/CN.4/1998/53/Add.2. Retrieved from <https://www.refworld.org/docid/3d4f95e1.html>
- UN General Assembly. (2013). *The right to privacy in the digital age.* Retrieved from <https://digitallibrary.un.org/record/764407#record-files-collapse-header>
- United Nations. (2010). *National Human Rights Institutions History, Principles, Roles and Responsibilities.* New York: Geneva.
- Urquhart, L., Sailaja, N., & McAuley, D. (2018). Realising the right to data portability for the domestic Internet of things. *Pers Ubiquit Comput*, 22, 317-332. <https://doi.org/10.1007/s00779-017-1069-2>
- Veselovska, N., Krushynskiy, S., Kravchuk, O., Punda, O., & Piskun, I. (2022). Criminal and Legal Countermeasures against Cybercrime in the Conditions of Martial Law. *International Journal of Computer Science and Network Security*, 22(12), 85-90. <https://doi.org/10.22937/IJCSNS.2022.22.12.11>
- Yuming, L. (Ed). (2019). *Data Rights Law 1.0: The Theoretical Basis Key Laboratory of Big Data Strategy.* Peter Lang Ltd.
- Zhalimas, D. (2019). Balancing National Security and Human Rights: Current Regional Challenges. In: *Human rights and national security: the role of the body of constitutional jurisdiction: a collection of materials of the international scientific and practical conference* (pp. 82-84). Kyiv: VAITE. https://ccu.gov.ua/sites/default/files/prava_lyudyny_i_nac._bezpeka_0_0.pdf