МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
НАЦІОНАЛЬНА АКАДЕМІЯ ВНУТРІШНІХ СПРАВ

ЮРИДИЧНИЙ ЧАСОПИС
НАЦІОНАЛЬНОЇ АКАДЕМІЇ ВНУТРІШНІХ СПРАВ

Науковий журнал

Том 15, № 3
2025

Київ
2025

ISSN 2519-4216
E-ISSN 2519-4313

УДК 34
DOI: 10.63341/naia-chasopis/3.2025

Засновник:
Національна академія внутрішніх справ
Рік заснування: 2011

Виходить чотири рази на рік

Рекомендовано до друку та поширення через мережу Інтернет Вченою радою Національної академії внутрішніх справ (протокол № 21 від 29 вересня 2025 р.)

Ідентифікатор медіа в Реєстрі суб'єктів у сфері медіа R30-02448
Рішення Національної ради України з питань телебачення і радіомовлення від 11 січня 2024 року № 26

Журнал входить до переліку фахових видань України
Категорія «Б». Галузь наук – юридичні, спеціальність – 081 «Право»
(наказ Міністерства освіти і науки України від 28 грудня 2019 р. № 1643)

Журнал представлено в міжнародних наукометричних базах даних, репозитаріях та пошукових системах: DOAJ, COPE, ERIH PLUS, SOLO, OUCI, НБУ ім. В.І. Вернадського, UCSB Library, Google Scholar, CrossRef, Worldcat, Dimensions, Litmaps, Фахові видання України, Електронний репозитарій НАВС, Cambridge University Library, University of Oslo Library, University of Hull Library, European University Institute, Leipzig University Library

Юридичний часопис Національної академії внутрішніх справ : наук. журн. / [редкол.: С. Чернявський (голов. ред.) та ін.]. – Київ : Нац. акад. внутр. справ, 2025. – Т. 15, № 3. – 109 с.

Адреса редакції:
Національна академія внутрішніх справ
03035, пл. Солом'янська, 1, м. Київ, Україна
Тел.: +38 (044) 520-08-47
E-mail: naia@lawjournal.com.ua
https://lawjournal.com.ua/uk

MINISTRY OF INTERNAL AFFAIRS OF UKRAINE
NATIONAL ACADEMY OF INTERNAL AFFAIRS

LAW JOURNAL

OF THE NATIONAL ACADEMY OF INTERNAL AFFAIRS

Scientific Journal

Volume 15, No. 3
2025

Kyiv
2025

ISSN 2519-4216
E-ISSN 2519-4313

UDC 34
DOI: 10.63341/naia-chasopis/3.2025

Founder:
National Academy of Internal Affairs
Year of foundation: 2011

Published four times per year

Recommended for printing and distribution
via the Internet by the Academic Council
of National Academy of Internal Affairs
(Minutes No. 21 of September 29, 2025)

Media identifier in the Register of Media Entities R30-02448
Decision of the National Council of Ukraine on Television and Radio Broadcasting
of 11 January 2024 No. 26

The journal is included in the list of professional publications of Ukraine
Category "B". Branch of sciences – legal, specialty – 081 "Law"
(order of the Ministry of Education and Science of Ukraine of December 28, 2019 No. 1643)

The journal is presented international scientometric databases, repositories and scientific systems: DOAJ, COPE, ERIH PLUS, SOLO, OUCI, VNLU, UCSB Library, Google Scholar, CrossRef, Worldcat, Dimensions, Litmaps, Professional publications of Ukraine, Electronic repository NAIA, Cambridge University Library, University of Oslo Library, University of Hull Library, European University Institute, Leipzig University Library

Law Journal of the National Academy of Internal Affairs / Ed. by S. Cherniavskyi (Editor-in-Chief) et al. Kyiv: National Academy of Internal Affairs, 2025. Vol. 15, No. 3. 109 p.

Editors office address:
National Academy of Internal Affairs
03035, 1 Solomianska Sq., Kyiv, Ukraine
Tel.: +38 (044) 520-08-47
E-mail: naia@lawjournal.com.ua
https://lawjournal.com.ua/en

ЮРИДИЧНИЙ ЧАСОПИС
НАЦІОНАЛЬНОЇ АКАДЕМІЇ ВНУТРІШНІХ СПРАВ
Том 15, № 3

Редакційна колегія

LAW JOURNAL
OF THE NATIONAL ACADEMY OF INTERNAL AFFAIRS
Volume 15, No. 3

Editorial Board

ЮРИДИЧНИЙ ЧАСОПИС
НАЦІОНАЛЬНОЇ АКАДЕМІЇ ВНУТРІШНІХ СПРАВ
Том 15, № 3

ЗМІСТ

LAW JOURNAL
OF THE NATIONAL ACADEMY OF INTERNAL AFFAIRS
Volume 15, No. 3

CONTENTS

UDC 343.57
DOI: 10.63341/naia-chasopis/3.2025.09

Analysis of the practice of criminalising advertising of narcotic drugs, psychotropic substances, and their analogues

Oksana Bryskovska*
PhD in Law, Senior Research Fellow
National Academy of Internal Affairs
03035, 1 Solomianska Sq., Kyiv, Ukraine
https://orcid.org/0000-0001-6902-9969

Hennadii Shevchuk
PhD in Law, Associate Professor
National Academy of Internal Affairs
03035, 1 Solomianska Sq., Kyiv, Ukraine
https://orcid.org/0000-0002-0108-6227

Oksana Voluiko
PhD in Psyhology, Associate Professor
National Academy of Internal Affairs
03035, 1 Solomianska Sq., Kyiv, Ukraine
https://orcid.org/0000-0002-3723-5415

Abstract
The relevance of the topic lies in the fact that the information sphere and drug promotion often remain outside the effective legal response. This issue is particularly acute in Ukraine, because war, social instability, and weakening of institutional control contribute to the activation of drug crime, in particular in the information space. The purpose of the study was to assess the need for criminalisation of advertising of narcotic drugs, psychotropic substances, and their analogues in Ukraine. For this purpose, system and structural, comparative, statistical, system, and extrapolation methods were used. It was proved that the increase in the number of people who use narcotic substances by almost one and a half times may be conditioned by, in particular, the easy availability of advertising of narcotic substances in a person's daily life: both offline and online. It was found that during the social instability caused by contemporary changes and the social realities of war, which psychologically traumatise people, suitable conditions for drug trafficking and advertising have emerged. Amendments to the criminal legislation of Ukraine that criminalise advertising of narcotic drugs in Ukraine were proposed, simplifying the investigation and proof of drug-related offences for law enforcement agencies. It was established that, despite the existence of separate prohibitions and norms, the criminal legislation of Ukraine, considering the changes proposed in this paper, can become more effective in protecting the population from drug addiction. In this context, it was particularly important to investigate international experience, in particular, the practices of the European Union, the United States of America, and Canada. Thus, the study of criminalisation

Article's History:
Received: 23.06.2025
Revised: 03.09.2025
Accepted: 29.09.2025

Suggest Citation:
Bryskovska, O., Shevchuk, H., & Voluik, O. (2025). Analysis of the practice of criminalising advertising of narcotic drugs, psychotropic substances, and their analogues. *Law Journal of the National Academy of Internal Affairs*, 15(3), 9-23. doi: 10.63341/naia-chasopis/3.2025.09.

*Corresponding author

of advertising of narcotic drugs and psychotropic substances has scientific and practical significance, since it contributes to the improvement of the criminal legislation of Ukraine, the development of a unified law enforcement practice, and ensuring the protection of society from the spread of crime related to narcotic drugs

Keywords:
drug crime; cryptocurrency; illegal trafficking; administrative and criminal liability; international experience; law enforcement

Introduction

In the context of the armed aggression of the Russian Federation against Ukraine, there is an annual increase in the scale of illegal trafficking in narcotic drugs, psychotropic substances, and their analogues. This trend is conditioned by the significant destructive impact of the criminal actions of the aggressor country on Ukrainian society. Drug use poses a serious threat to the physical and mental health of the population, contributes to the development of mental and somatic diseases, social maladaptation, and personal degradation. People with drug addiction have severe neurological and mental disorders, damage to internal organs, which leads to chronic diseases. Drug addiction forms both physical and mental dependence, is one of the causes of disability and mortality of the population. Special attention should be paid to the problem of drug use by persons who have survived the consequences of military aggression: military personnel, internally displaced persons, people who have lost their homes or loved ones. In an attempt to overcome psychological pain, they may turn to drug use, which, ultimately, only worsens their condition, leading not only to health problems, but also to socio-economic destabilisation. In this regard, it is extremely important to improve the effectiveness of Ukrainian legislation in the field of countering drug trafficking, in particular by criminalising advertising of narcotic drugs, psychotropic substances, and their analogues. This is necessary to prevent profit from psychologically vulnerable individuals who have suffered as a result of military aggression, and to ensure an appropriate level of public health protection.

During 2020-2025, researchers created a significant number of studies on countering illegal trafficking in narcotic drugs and psychotropic substances. However, advertising of narcotic drugs as an independent topic did not receive proper scientific understanding, but was considered only briefly, as a component of the problem of illegal distribution of narcotic substances. In the context of related topics, some studies have focused on drug advertising in general, but without a specific focus on drugs.

Thus, the paper by P. Pokataev *et al*. (2023) analysed the ethical and legal aspects of drug advertising in Ukraine. The researchers investigated the regulatory framework of both national and international levels in the field of pharmaceutical regulation. Special attention was paid to the ethical and legal criteria consolidated in domestic legislation, which form the mechanisms of both state and non-state regulation of advertising activities in the pharmacological sector. Despite the relevance of the topic of drug advertising to the issue of advertising narcotic substances, the latter remained outside the scope of analysis.

N. Horobets *et al*. (2024) considered the Internet as a platform for drug trafficking, characterised the composition of a criminal offence related to the illegal sale of drugs, and substantiated the need to criminalise their distribution via the Internet. In particular, attention was focused on the growing use of cryptocurrencies for settlements in the field of drug trafficking. The researchers emphasised that both in Ukraine and at the international level, there is currently no proper legal regulation of this issue, which requires adequate adaptation of legislation to contemporary technological challenges.

J. Aldridge & D. Décary-Hétu (2016), researching wholesale drug trafficking through online platforms using cryptocurrencies, found that ecstasy, benzodiazepines, and prescription stimulants accounted for the largest wholesale volumes. To a much lesser extent, but still noticeable, was the trade in cocaine, methamphetamine, and heroin. Despite the presence of sellers from 41 countries, wholesale activities were carried out mainly in China, the Netherlands, Canada, and Belgium. The researchers note that the specifics of cryptocurrencies contribute to the expansion of the customer base of illegal traders.

The study by Y. Leheza *et al*. (2023) analysed the experience of law enforcement agencies in the UK, Sweden, Spain, Estonia, the Czech Republic, and the United States in combating the illegal distribution of drugs via the Internet. The importance of preventive measures, in particular, criminal law prevention, and a wide range of assistance to citizens in preventing drug crime was noted. In the course of the study, the researchers determined the algorithm for distributing drugs through social networks, messengers, and instant messaging services. Various payment methods were described, including transfers via electronic payment systems, bank self-service terminals, replenishment of electronic wallets (Global Money, PayPal, Privat24, Oschad24, QIWI, EasyPay), replenishment of a mobile account or leaving cash in a pre-agreed place (so-called "bookmarks").

Y. Kuryliuk *et al*. (2021) noted that one of the most dangerous types of crime is the illegal trafficking of narcotic drugs, psychotropic substances, their analogues and precursors, which has a steady upward trend. The

researchers analysed the current state of drug crime in Ukraine, identified the main problems in the field of counteraction, and suggested ways to improve it. The paper noted that the current drug policy of Ukraine still does not meet the requirements of the state strategy in this area, which significantly complicates effective and timely counteraction to drug crime. The fight against drug addiction and drug trafficking remains a global problem for the international community, because today drug trafficking is one of the most profitable areas of criminal business with a transnational character. The researchers emphasise the increase in the number of people who illegally use drugs, and a corresponding increase in crimes committed on the basis of drug addiction. Strengthening of legislative regulation, improvement of the regulatory framework for anti-drug activities, development of scientific research and introduction of innovative technologies, and effective use of international cooperation mechanisms were identified as priority areas for countering drug crime in Ukraine.

In turn, study by O. Kudermina *et al*. (2019) examined the phenomenon of using advertising services to promote prohibited substances both in the domestic and foreign markets. The researchers focused on hidden forms of advertising of narcotic drugs and emphasised the lack of proper legal regulation of such advertising in the fields of food products, clothing, with the exception of TV and radio programmes, and print publications. The paper also analysed Ukraine's experience in criminalising actions related to drug trafficking, comparing the approaches of some states (in particular, the Netherlands, the Czech Republic, and Portugal) that have taken the path of partial decriminalisation of such actions. Despite the potential benefits of decriminalisation (improving the criminal situation, reducing the burden on law enforcement agencies, and reducing costs), the researchers warned about the risks associated with this approach.

A. Fuller *et al*. (2023) focused on the distribution of illicit drugs through social media, which is particularly dangerous given access to a broad audience, particularly young people, adolescents, and children. The study found that an average of 13 out of 100 social media posts contain signs of drug advertising. The researchers conducted an in-depth analysis of various internet platforms and algorithms for moving from search queries with drug-related keywords to behaviours typical of online sales of prohibited substances. J. Demant *et al*. (2020) analysed 57 Facebook groups created in Sweden. The researchers found that in these groups, various types of drugs were actively offered for sale through messages that, in fact, served as advertising. Both professional dealers and amateurs participated in the trade. M. Dewey & A. Buzzetti (2024) pointed to the growing role of encrypted messengers, in particular Telegram, in the field of drug trafficking. The researchers noted that the combination of anonymity capabilities, rapid community creation and closure, and ease of use on mobile devices is transforming the way drugs are delivered and sold. Such platforms allow advertising and sale of narcotic substances in a relatively open way, which emphasises the need for legislative regulation of advertising of prohibited substances in the digital space.

The purpose of this study was to determine the feasibility of criminalising advertising of narcotic drugs, psychotropic substances, and their analogues in the context of contemporary global challenges associated with the distribution of drug advertising in the digital environment.

Materials and Methods

Both general scientific and special methods of scientific knowledge were used to conduct the scientific research presented in this paper. General scientific methods included deduction, induction, analysis, systematisation, and classification. Among the special methods, empirical, comparison, statistical, extrapolation, system analysis, idealisation, and the hypothesis formation methods were used. The combination of these methods allowed forming a complete conceptual basis for the research, based on which it was possible to achieve this goal. In particular, empirical information about the object of research was collected using the statistical method. The empirical method of cognition provided the possibility of observing and describing phenomena based on the analysis of scientific publications, official reports of state institutions, laws and regulations, legislative initiatives, and information from official web portals of foreign countries related to the research topic. The method of system analysis helped to substantiate the expediency of criminalising advertising of narcotic drugs, psychotropic substances, and their analogues in Ukraine. Based on the extrapolation method, a proposal was modelled to amend the criminal legislation in terms of advertising these substances, which became the basis for formulating recommendations for preventing and minimising such offences.

The normative legal basis of this study was the following acts of national legislation of Ukraine: Constitution of Ukraine[1], Criminal Code of Ukraine[2], Laws of Ukraine "On the National Police"[3], "On Advertising"[4]. These sources, since they regulate public relations in the field of preventing illegal trafficking in narcotic drugs, psychotropic substances, and their analogues. It

[1] Constitution of Ukraine. (1996, June). Retrieved from https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text.
[2] Criminal Code of Ukraine. (2001, April). Retrieved from https://zakon.rada.gov.ua/laws/show/2341-14#Text.
[3] Law of Ukraine No. 580-VIII "On the National Police". (2015, July). Retrieved from https://zakon.rada.gov.ua/laws/show/580-19#Text.
[4] Law of Ukraine No. 270/96 "On Advertising". (1996, July) . Retrieved from https://zakon.rada.gov.ua/laws/show/270/96-%D0%B2%D1%80#Text.

is these regulations that form the basic legal basis from which the study of certain types of crimes is carried out, in particular, those related to illegal advertising for the purpose of selling narcotic substances. In addition, the source of statistical data was the National Report of the Drug Situation in Ukraine 2024 (Public Health Centre, 2024) and General Prosecutor's Office of Ukraine (n.d.).

Results

Addiction to narcotic drugs is dangerous both for the person who uses them and for their social environment, because drug addicts can resort to extreme measures to get the next dose. In conditions of armed conflict, when a significant part of the population suffers psychological and physical injuries, loses housing, property, or loved ones, vulnerability to the effects of advertising narcotic substances, which is presented as a means of temporary relief, increases. Special attention should be paid to the situation among military personnel who have suffered psychological trauma. In such cases, they may refer to drug use as a form of escapism. According to the study conducted by A.O. Sheludko (2023) regarding adaptive and constructive coping strategies in military personnel, 25% of respondents called overeating, drug use, alcohol, etc., a common coping strategy. 65% of respondents indicated that they use such coping strategies (overeating, drug use, alcohol consumption, etc.) "moderately". These individuals need professional psychological or psychotherapeutic support, medical rehabilitation, and social support. Only comprehensive assistance can contribute to their recovery and integration into society. But drug use only worsens their condition, potentially provoking an increase in crime, fatal overdoses, increased levels of victim behaviour, social isolation, etc.

In particular, the study by Y. Sim (2023), using the example of individual states of the United States of America, demonstrated that in states where the receipt of such a narcotic substance as OxyContin was more complex, bureaucratically regulated, the crime rate for the period from 1990 to 2016 increased by: from 0.3% to 0.5%, and in states where the receipt of such a narcotic substance was not limited to the triple prescription programme, that is, people received OxyContin more often, the crime rate increased from 13.2% to 22%. The researcher also added that 30% of criminals who committed property crimes did so in order to purchase narcotic drugs. Empirical evidence suggests that people who are addicted to narcotic substances may also use other illegal drugs. For example, heroin as a substitute for prescription opioids.

In turn, K.I. Didenko (2025) investigated that the use of psychoactive substances (for example, drugs) was often accompanied by changes in the emotional and volitional sphere, which can lead to the development of mental disorders, decreased self-control, increased anxiety and depression. She pointed out that drugs, as psychoactive substances, can significantly change not only the emotional state of a person, but also the ability to control own behaviour, make decisions, and make volitional efforts, which, in turn, affects their social relationships and ability to function effectively in society. The average score among drug-addicted respondents surveyed during the study on the Beck Depression Scale was 18.39 times higher than that of non-drug-addicted respondents.

A separate threat is the impact of drug advertising on young people, adolescents, and children. Advertising of narcotic drugs and psychotropic substances forms a false idea of their admissibility and attractiveness, even if it is not distributed by traditional channels (television, radio). In the digital age, such messages are actively distributed through alternative anonymous sources: Telegram channels, closed forums, social networks, graffiti or QR codes in public places. In particular, A. Fuller *et al*. (2023) conducted a comprehensive study of drug advertising on social networks and found that 3.6% of the videos that were posted on social networks advertised cannabis use. Such videos received 5 million "likes" and were viewed 27 million times. These figures exceed the engagement rates of macro-influencers with 100,000-1 million subscribers receiving an average of 38,000 views per post. M. Dewey & A. Buzzetti (2024) also investigated the sale and advertising of narcotic substances through instant messengers. Researchers have provided empirical evidence gathered during in-depth interviews with drug sellers and buyers that these communities, unlike the outdated form of market relations, improve for participants the experience of purchasing goods (in their case, the experience of purchasing narcotic substances). In 2020, Telegram users of the "StopNarkotik" chatbot helped to block 1,500 email addresses in the Telegram messenger that attackers used to illegally sell drugs via the Internet, including due to photos of inscriptions ("graffiti") and stickers with "advertising drug addresses" indicating GPS coordinates or physical addresses where they were found (Ministry of Internal Affairs of Ukraine, 2020) received by law enforcement agencies.

Contemporary advertising content is becoming increasingly sophisticated – drugs are presented as a "stylish" or "healthy" way to escape from reality. This trend may contribute to a change in the structure of the drug market: new technologies are enabling a mass shift to online retail, encouraging even teenagers and casual users to participate, according to the Public Health Centre of the MHP of Ukraine (2024), the traditional method of purchasing drugs (from dealers and at designated "points of sale") has been replaced by online drug trafficking. In addition, the number of people who produce narcotic substances at home for sale has decreased. The vast majority of respondents bought through conditional "stashes" (47.4%). It was

the older part of respondents who were more likely to prepare drugs at home, compared to the younger part of respondents.

That is why the rapid spread of advertising for narcotic drugs significantly increases social risks, as the process of purchasing them becomes more attractive and accessible. As of 2025, there has been a marked increase in digital drug advertising, which is still aimed primarily at young people. A. Al-Ravi (2022) found in his study that every social network he studied had active drug advertisements. Most of all, he found such advertising on the social network Twitter. The researcher, after analysing previous research on this topic, noticed a trend towards an increase in the number of digital advertising in social networks. Dependence on narcotic substances significantly increases the risk of infection with incurable diseases, in particular, HIV/AIDS, various forms of viral hepatitis, etc. In addition, drug addiction often leads to deterioration or loss of reproductive function, an increase in the number of births of children with disabilities.

The lack of criminalisation of advertising of narcotic substances only worsens the problem, creating conditions for their free distribution. Information on how to contact dealers can be found directly in the image itself, in post captions, or in comments. After agreeing on the terms of purchase – price, delivery method (by mail or in person) – payment is made through online services, in particular PayPal (Fuller *et al*., 2023). Considering that the current criminal legislation of Ukraine provides only for "Inducement to use narcotic drugs, psychotropic substances, or their analogues" (in accordance with Article 315 of the Criminal Code of Ukraine[1], "1. Inducing a certain person to use narcotic drugs, psychotropic substances or their analogues – shall be punishable by restriction of liberty for a term of up to five years or by imprisonment for a term of two to five years. 2. The same action committed repeatedly either in relation to two or more persons, or in relation to a minor, and by a person who has previously committed one of the criminal offences provided for by articles 307, 308, 310, 314, 317 of this Code, – shall be punished by imprisonment for a term of five to twelve years"), which cannot quite fairly replace the criminalisation of "advertising the use of narcotic drugs, psychotropic substances, or their analogues" due to the fact that "advertising" has the meaning of influencing a wider range of persons than "persuasion".

The lack of legal regulation, and the lack of criminal liability for drug advertising both in the offline space and on the Internet, creates a favourable environment for the expansion of illegal trade. Sellers get more opportunities to promote their products in social networks, instant messengers, on platforms, and in mobile applications.

Considering the examples of some other countries, it would be important to mention the states that are members of the European Union. In particular, in accordance with paragraphs 44-46 of Directive 2001/83/EC of the European Parliament and of the Council of 6 November 2001 on the Community code relating to medicinal products for human use[2], it is prohibited in European Union member states to advertise medicinal products that are only available on prescription (including narcotics) to the general public. The Directive, among other purposes, aims to preserve the health of the population, delineate the ethics of advertising, and ensure that non-compliance with the national laws of the member states with each other does not harm all persons residing in the territory of the European Union. For example, Slovakia has brought its national legislation to the standards of the European Union, considering the provisions of the aforementioned Directive in Law of Slovakia No. 147/2001[3] and No. 362/2011[4]. However, T. Peráček *et al*. (2019) argued that such duplication of a rule of law worsens the quality of the law and may lead to the fact that one person can be held accountable twice for the same action that such a person committed once. The researchers argued that such a provision of the law can be improved so that the law not only meets the requirements of the European Union, but also has high-quality content.

Australia also has similar legal provisions in its legislation. According to the Code of Conduct for the Australian Pharmaceutical Industry[5], advertising of prescription-only medicines (including narcotics) directly to consumers is prohibited in the country. This can only be advertised to the doctors themselves, who will later make a professional decision about the need or absence of the need for a certain medicine for a sick person. Similar rules are also established in the legislation in the Controlled Drugs and Substances Act of Canada[6]. In countries such as the United States of America, Ukraine, and Cuba, advertising of drugs and psychotropic substances is not explicitly prohibited. These countries differ in their location, size, and socio-economic situation.

[1] Criminal Code of Ukraine. (2001, April). Retrieved from https://zakon.rada.gov.ua/laws/show/2341-14#Text.
[2] Directive of the European Parliament and of the Council No. 2001/83/EC "On the Community Code Relating to Medicinal Products for Human Use". (2001, November). Retrived from https://eur-lex.europa.eu/eli/dir/2001/83/oj/eng.
[3] Law of Slovakia No. 147/2001 "On Advertising and on Amendments to Certain Laws". (2001, April). Retrived from https://www.slov-lex.sk/ezbierky/pravne-predpisy/SK/ZZ/2001/147/20190101.html.
[4] Law of Slovakia No. 362/2011 "On Medicines and Medical Devices and on Amendments to Certain Laws". (2011, September). Retrived from https://www.zakonypreludi.sk/zz/2011-362.
[5] Code of Conduct for the Australian Pharmaceutical Industry. (2025, March). Retrived from https://code.medicinesaustralia.com.au/code/.
[6] Controlled Drugs and Substances Act of Canada. (1996, June). Retrieved from https://laws-lois.justice.gc.ca/eng/acts/C-38.8/page-1.html#docCont.

Nevertheless, each of these countries has quite well-developed drug markets.

For comparison, in France, which is a member state of the European Union, where there is a ban on advertising medicines that can only be purchased with a doctor's prescription (including drugs), only 3.4% of people used drugs regularly, according to the results of the study by S. Spilka *et al*. (2024). According to the 2023 United States National Survey on Drug Use and Health (2023), in the United States of America, 16.7% of people over the age of 12 struggled with a substance-related disorder, and 9.7% of people over the age of 12 struggled with a drug-related disorder. According to Statistics Canada (n.d.), just 3% of Canadians used illegal drugs in 2019. According to an online survey on the prevalence and frequency of use of certain narcotic and psychotropic substances in Ukraine conducted by the Institute of Psychiatry, Forensic Psychiatric Examination, & Drug Monitoring of the Ministry of Health of Ukraine (2023), 21.6% of respondents reported drug use in the last 30 days, which is 68% of those who reported drug use in the last 12 months. Referring to the National Study of Mental Health and Wellbeing (2023), it can be argued that in 2020-2022, only 3.3% of people in Australia struggled with a substance use disorder. Although accurate statistics on the share of drug users in Cuba are not available, the country's leader, Miguel Diaz-Canel, acknowledged that Cuba in 2024 faced a growing problem of the spread of narcotic substances and drug addiction, which, among other things, is also caused by the fact that drugs are cheaper there, relative to neighbouring countries (Torres, 2024). Thus, considering the above information, it can be assumed that the lack of responsibility for advertising drugs and psychotropic substances, among other possible factors, leads to the expansion of illegal trade, because in countries that do not have such responsibility for advertising drugs and psychotropic substances, the number of dependent persons on drugs and psychotropic substances, or the number of persons who struggled with disorders related to the use of drugs and/or psychotropic substances, was higher than those countries in which responsibility for such advertising is provided for by law.

Criminalisation of advertising of narcotic drugs, psychotropic substances, their analogues, and precursors would provide law enforcement agencies with an additional tool for bringing to justice persons involved in illegal trafficking of these substances, even in cases where drugs were not found directly during the search. After all, often offenders, realising the risk of exposure, destroy or hide narcotic substances until the arrival of investigators, and the funds themselves can be stored in separate premises that are not officially connected with the suspect (for example, informally rented garages, basements, warehouses, etc.). Establishing a storage location for such substances takes time, which plays into the hands of intruders, allowing them to disguise or destroy evidence.

The introduction of criminal liability for the creation and/or distribution of advertising of narcotic substances will allow law enforcement officers to focus on proving the fact of participation of a person in advertising activities aimed at popularising or selling narcotic drugs. In this case, the main subject of proof will be the presence of signs of advertising of narcotic substances and the involvement of a particular person in its distribution, and not the fact of direct storage or transportation of drugs.

This approach will allows using the results of secret investigative (search) actions in criminal proceedings more effectively. In particular, the ability to document placed ads in Telegram channels or other internet resources greatly simplifies the process of fixing an offence. For example, if, as part of an operational event, a police officer discovers a publication with an offer to buy narcotic substances, even if the seller does not have the goods with them (since they could have already carried out the so-called "stash"), the very fact of the presence of advertising content can serve as evidence in court. Clicking on an Internet link leading to a resource with a similar offer indicates the presence of advertising, which should be the basis for bringing the guilty person to justice.

Moreover, the criminalisation of advertising of narcotic drugs, psychotropic substances, their analogues and precursors will have a significant preventive effect for individuals involved in the creation and distribution of relevant content. These include, in particular, graphic designers who create visual materials of an advertising nature, people who apply graffiti with links to channels or groups in messengers on buildings, bridges, or educational institutions, and those who distribute printed materials with similar content. These individuals are not always direct distributors of drugs – they are often unemployed, teenagers, or socially vulnerable citizens who are looking for quick earnings. Now they are aware that even if they are detained, they face only a minor penalty, because they did not carry out the storage or sale of narcotic drugs included in the list approved by the resolution of the Cabinet of Ministers of Ukraine of May 6, 2000 No. 770[1]. However, their actions cause no less harm, as they contribute to the dissemination of dangerous information among socially vulnerable segments of the population.

The introduction of criminal liability for advertising drugs will effectively deter such activities, as potential offenders will be aware of the reality of more severe legal liability than, for example, administrative

[1] Resolution of the Cabinet of Ministers of Ukraine No 770 "Regulations on the Approval of the list of Narcotic Drugs, Psychotropic Substances and Precursors". (2000, May). Retrieved from https://zakon.rada.gov.ua/laws/show/770-2000-%D0%BF#Text.

liability for petty hooliganism. Hypothetically, this will significantly reduce motivation to participate in such activities and help to prevent the spread of narcotic substances through advertising channels.

At the moment, paragraph 14 of Resolution No. 4 of the Plenum of the Supreme Court of 26 April 2002[1] to a certain extent, fills the gap created by the lack of a definition of a separate crime – advertising of narcotic drugs, expanding the meaning of Article 315 of the Criminal Code of Ukraine[2] (Persuasion to use narcotic drugs, psychotropic substances or their analogues), providing that "persuasion" should be understood as "any intentional nonviolent actions aimed at arousing another person's desire to use these drugs or substances at least once (suggestion, persuasion, advice, etc.)". However, such filling in the gaps of legislation is not always appropriate, because in cases such as this one, it weakens the compliance of such a legislative norm with the principle of "predictability of the law", because in order for the law to be of high quality, it must be easily accessible and understandable to a wide range of people. Moreover, "persuasion to use narcotic drugs" should not imply personal inducement, where the subject of such an action is only one person, and inducement to use drugs to the general public, which is already, in fact, advertising, because inducement to use drugs to the general public has an impact on a larger number of people, and therefore is more dangerous, and therefore, accordingly, for such actions and the sanction should be greater, reflecting the impact that specific actions had.

It is also worth noting that within the framework of this study, the concept of "advertising" is not equated with "propaganda". As noted by J. Denysiuk (2021), propaganda is a form of spreading knowledge and ideas aimed at forming fundamental worldview attitudes that are recognised as acceptable within a particular political or ideological system. This is a much broader concept than advertising. According to paragraph 15 of Article 1 of the Law of Ukraine "On Advertising"[3], advertising is defined as information about a person, idea, and/or product, disseminated for remuneration or for the purpose of self-promotion in any form, with the aim of forming or maintaining consumer awareness and interest in such objects. Thus, advertising is a commercially oriented means of influence that differs both in its functional purpose and regulatory status from propaganda. The concept of "propaganda" is quite broad and ambiguous, which creates the risk of excessive interpretation and, accordingly, possible abuse. The introduction of liability for "propaganda" of drug use can create prerequisites for restricting freedom of expression, in particular, by giving judges excessive freedom to interpret what is and is not propaganda.

Thus, the most appropriate and legally verified approach for Ukrainian legislation is the introduction of criminal liability for "advertisement of narcotic drugs". This term is clearly defined in the legislation, in particular, in the Law of Ukraine "On Advertising"[4], which avoids over-interpretation, ensures legal predictability, effective application of the rule, and reduces the risks of abuse. The ease of establishing the elements of a crime based on the presence of advertising content greatly facilitates the work of law enforcement and judicial authorities, while maintaining a balance between the interests of the state and human rights.

A. Fuller *et al*. (2023) pointed out that despite a significant number of cases of drug advertising on social networks, the researchers concluded that a significant part of transactions takes place within the framework of pre-established contacts with dealers. This model of trade is characterised as a social supply, which further complicates its detection by law enforcement agencies. It is also important that the main audience targeted by advertising remains young people – teenagers and young people, which, given their age vulnerability, poses a particular threat. The researchers noted that platforms popular among teenagers rarely become the objects of systematic scientific research. With this in mind, in the Ukrainian context, it is advisable to conduct further interdisciplinary research, considering exactly the platforms that young people actively use. This would help to better understand the mechanisms of drug distribution in the digital environment and create effective prevention tools.

Based on official statistics, there is a clear upward trend in the number of recorded criminal offenses involving the trafficking of narcotic drugs, psychotropic substances, their analogues or precursors, and other criminal offences that pose a threat to public health. Especially significant is the dynamics of increasing the number of crimes related to the illegal production, manufacture, acquisition, storage, transportation, or shipment for the purpose of sale, and with the illegal sale of narcotic drugs, psychotropic substances, or their analogues. This trend intensified with the beginning of the armed aggression of the Russian Federation against Ukraine. For clarity, the dynamics of committing these offences is presented in Table 1, which allows visually assessing the scale of the increase in drug crime in war conditions.

[1] Resolution of the Supreme Court of Ukraine No. 16 "On Amendments and Supplements to the Resolution of the Plenum of the Supreme Court of Ukraine of April 26, 2002 No. 4 "On Judicial Practice in Cases of Crimes in the Sphere of Trafficking in Narcotic Drugs, Psychotropic Substances, Their Analogues or Precursors". (2009, December). Retrieved from https://zakon.rada.gov.ua/laws/show/v0016700-09#Text.
[2] Criminal Code of Ukraine. (2001, April). Retrieved from https://zakon.rada.gov.ua/laws/show/2341-14#Text.
[3] Law of Ukraine No. 270/96 "On Advertising". (1996, July). Retrieved from https://zakon.rada.gov.ua/laws/show/270/96-%D0%B2%D1%80#Text.
[4] Ibidem, 1996.

Table 1. Comparison of the total number of criminal offences in the sphere of trafficking in narcotic drugs, psychotropic substances, and their analogues for 2021-2025

			2021	2022	2023	2024	2025*
Criminal offences were considered in the reporting period	Illegal production, manufacture, acquisition, storage, transportation, or shipment for the purpose of sale, and illegal sale of narcotic drugs, psychotropic substances, or their analogues	Total	10,994	10,162	14,302	17,601	8,478
		Sales	7,448	6,960	11,651	14,770	6,879
	Total		114,460	134,739	153,240	184,142	90,574
Criminal offences in which persons have been served with a notice of suspicion	Illegal production, manufacture, acquisition, storage, transportation, or shipment for the purpose of sale…	Total	8,323	7,839	11,611	14,971	5,571
		Sales	6,088	5,698	9,913	12,921	6,629
	Total		85,071	88,599	124,574	155,696	7,094
Criminal offences for which the proceedings were sent to the court (paragraphs 2.3 of Article 283 of the Criminal Procedure Code of Ukraine)	Illegal production, manufacture, acquisition, storage, transportation, or shipment for the purpose of sale…	Total	6,330	6,215	9,967	11,914	3,819
		Sales	5,008	4,612	8,655	10,590	4,433
	Total		73,918	77,779	115,141	137,427	55,983
With an indictment	Illegal production, manufacture, acquisition, storage, transportation, or shipment for the purpose of sale…	Total	6,314	6,202	9,909	11,887	3,815
		Sales	4,999	460	8,601	10,569	4,428
	Total		72,792	77,054	114,227	136,735	55,718

Note: 2025* – January-April
Source: developed by the authors based on data from General Prosecutor's Office of Ukraine (n.d.).

It is worth noting that according to statistics, in 2021, the total number of registered criminal offences in the sphere of trafficking in narcotic drugs, psychotropic substances, their analogues or precursors, and other offences against public health amounted to 114,460 cases. In 2022, this figure increased to 134,739, which is 20,279 cases (15%) more. In 2023, 153,240 such offences were recorded, which is 18,501 cases (13%) more than in the previous year. In 2024, 184,142 cases were registered, which is 30,902 (17%) more than in 2023. A similar trend can be traced when comparing January–April 2024 (70,518 cases) with the corresponding period in 2025 (90,574 cases), where the increase was 20,056 cases, or 22%. Thus, there is a steady trend of annual growth in the number of these criminal offences by an average of 22,435 cases, or approximately 17%. This indicates a progressive criminal situation in the field of drug trafficking in Ukraine.

As for specifically crimes related to the illegal sale of narcotic drugs, psychotropic substances or their analogues, 7,448 such offences were taken into consideration in 2021. In 2022, their number decreased to 6,960 (by 488 cases or 7%), but in 2023 the number of such crimes increased sharply to 11,651 (by 4,691 cases or 40.26%). In 2024, 14,770 cases were recorded, which is 3,119 (27%) more. In January-April 2025, 8,478 cases were registered, which is 2,463 (41%) more than in the same period of 2024 (6,015 cases).

This increase in the level of drug crime is conditioned by only to the influence of armed aggression and the active use of cryptocurrencies for anonymous transactions, but also to a sharp increase in open advertising of narcotic drugs and psychotropic substances. Given the constant increase in the number of such crimes, it is obvious that there is a need for legislative changes that would provide effective mechanisms for combating drug trafficking offences and have a preventive effect aimed at denormalising their use. One of the positive side effects of this approach may be a reduction in the number of graffiti advertising prohibited substances on buildings, infrastructure facilities, and in public places.

It is worth emphasising that one of the factors of the spread of drug addiction is the almost free advertising of narcotic drugs. Nowadays, such advertisements can be seen anywhere: in the form of stickers with QR codes, inscriptions on the walls of houses, in underground passages, at public transport stops, near metro stations, and in social networks, instant messengers and anonymous online resources. Such advertising, distributed both in the real space and in the digital environment, creates new opportunities for the sale of drugs, expands the scale and geography of the activities of intruders. However, despite the threat posed by this phenomenon, the current criminal legislation of Ukraine does not provide for liability for advertising narcotic substances.

That is, among the factors that determine the need to criminalise advertising of narcotic drugs, psychotropic substances, and their analogues in Ukraine, the following can be distinguished:

1) growing level of drug advertising in the digital environment. Advanced means of communication (instant messengers, social networks, anonymous forums) have become a powerful tool for popularising and secretly advertising drugs. Moreover, advertising is carried out purposefully for a young audience, using manipulative and psychologically attractive forms of influence.

2) imperfection of the current legislation. The criminal legislation of Ukraine does not clearly define

advertising of narcotic drugs, and also does not regulate the specific signs of a criminal offence related to the promotion of drugs as a commodity. This creates gaps in law enforcement and makes it impossible for law enforcement agencies to respond effectively.

3) low efficiency of administrative and legal measures. Practice shows that administrative responsibility for propaganda or popularisation of drugs does not have the proper deterrent effect, especially in cases of repeated or systemic nature of such offences.

4) distribution of "street" and visual drug advertising. Graffiti, QR codes, and pseudo-marketing are actively used, which avoids direct prohibition, but actually performs the function of an advertising tool. This requires new legal approaches to the qualification of relevant acts.

5) growing social risks and dangers for young people. Advertising drug use leads to a decrease in critical perception of threats, romanticisation of drug culture, and, as a result, to an increase in drug addiction and criminalisation of young people. The study by A. Oksanen *et al.* (2020), demonstrated that the majority of young people who buy drugs using the Internet do so through social networks, which, in fact, contain advertising content of narcotic substances. M.A. Petersen *et al*. (2021) pointed to the unregulated use of so-called "learning stimulants" by young people, especially students, including amphetamines and methylphenidates. The use of such substances without medical indications and medical supervision can have serious long-term health consequences. After analysing the content on Instagram, the researchers concluded that most of the publications related to these drugs were positive and often had an advertising character. Some of them directly offered these substances for sale, which indicates the presence of advertising elements. The study demonstrates a close relationship between social media and drug promotion. A study conducted by J.V. Cristello *et al*. (2023) showed that 75% of adolescents who regularly saw photos of their peers, other young people using drugs or alcohol on social networks were encouraged to also use similar substances, despite the possible risks. In addition, M.A. Motyka & A. Al-Imam (2021) argued in their academic paper that promoting frivolous attitudes to drugs by famous pop culture figures is one of the predictors of the beginning and continuation of drug use for a general audience.

6) need for harmonisation with international practice. In accordance with the provisions of the 1988 UN Convention for the Suppression of Illicit Traffic in Narcotic Drugs and Psychotropic Substances[1], states are required to take effective criminal-law measures to combat all forms of involvement in drug trafficking, in particular, with their advertising and propaganda.

Draft laws aimed at criminalising drug advertising have been repeatedly submitted to the Verkhovna Rada of Ukraine. In particular, in 2021, the Verkhovna Rada Committee on Law Enforcement Issues registered Draft Law of Ukraine No. 5496[2]. The authors of the bill proceeded from the fact that advertising and propaganda of drugs are significantly broader concepts than just inducing them to use them. In particular, they are aimed at a wide audience in order to encourage the use of narcotic drugs and create conditions for their further sale with the receipt of illegal profits. Special attention in the explanatory note was paid to threats related to the use of the Internet, social networks, and instant messengers to spread information about narcotic drugs. Such actions, according to the authors, significantly increase the risks of distribution, marketing and use of drugs, which justifies the need to introduce liability for such actions at the level of criminal law.

In general, the proposed bill deserves a positive assessment, as it is aimed at protecting public health and preventing drug addiction. However, the use of the term "propaganda" in the text, even with subsequent attempts to detail it through exceptions, creates an excessive breadth of interpretation. Given the complexity and variety of life situations, the use of the concept of "propaganda" as a legal category can have negative consequences, in particular – abuse of law enforcement. But the concept of "advertising", clearly defined in the legislation of Ukraine, is narrow and precise enough to achieve the goals of this draft law, including preventing exposure to vulnerable categories of the population and limiting the spread of narcotic substances.

In this regard, it is advisable to introduce a new draft law, which would provide for criminal penalties for advertising narcotic drugs, psychotropic substances, their analogues or precursors, without appealing to the term "propaganda". Such an approach would avoid ambiguous interpretation, promote legal certainty, and make law enforcement more effective and more predictable.

There is also an alternative bill that proposes to introduce liability for advertising narcotic drugs. This refers to the Draft Law of Ukraine No. 7558[3]. This draft law focuses on introducing administrative liability for illegal advertising that violates the architectural

[1] United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances. (1991, November). Retrieved from https://zakon.rada.gov.ua/laws/show/995_096#Text.

[2] Draft Law of Ukraine No. 5496 "On Amendments to the Criminal Code of Ukraine Regarding the Criminalisation of Advertising or Propaganda of Narcotic drugs, Psychotropic Substances, their Analogues or Precursors". (2021, May). Retrieved from https://itd.rada.gov.ua/billinfo/Bills/Card/26587.

[3] Draft Law of Ukraine No. 7558 "On Amendments to the Code of Ukraine on Administrative Offenses and the Criminal Code of Ukraine to Improve Liability for Illegal Placement of Advertising on Territories, Buildings and Structures, as Well as for Advertising of Narcotic Drugs". (2022, July). Retrieved from https://itd.rada.gov.ua/billinfo/Bills/Card/40015.

aesthetics of localities and distorts urban space. The text of the document contains a proposal to criminalise advertising of narcotic substances. The explanatory note to the draft law notes that when determining the type and amount of sanctions, the authors proceeded from the logic of the need to establish liability that is not milder than that provided for in Article 315 of the Criminal Code of Ukraine[1]. – for inducing the use of narcotic drugs, psychotropic substances, or their analogues. This approach is justified given the functional relationship of these crimes, and the consequences that they entail for society, in particular, vulnerable categories of citizens[2].

The adoption of this draft law could be an important step towards comprehensive prevention of offences related to drug trafficking, and would allow responding more effectively to contemporary challenges, including the mass distribution of graffiti advertising drugs, stickers with QR codes, and digital advertising in social networks and instant messengers. It would be appropriate to supplement the Criminal Code of Ukraine[3] with Article 315[1] with the following content:

"Article 315[1]

Advertising of narcotic drugs, psychotropic substances, their analogues or precursors

1. Placement of advertising on territories, buildings, and structures in any form, for the purpose of selling narcotic drugs, psychotropic substances, their analogues or precursors, in particular advertising of technical resources (websites, web pages, electronic communication networks, information (automated) systems, other technical means of electronic communications, etc.) or means of communication (in particular mobile) used for the purpose of selling narcotic drugs, psychotropic substances, their analogues or precursors, is punishable by restriction of liberty for a term of three to seven years or imprisonment for a term of three to seven years.

2. The same action committed repeatedly or by a person who has previously committed one of the criminal offences provided for in articles 307, 308, 310, 314, 317 of this Code, or also committed with the involvement of a minor, is punishable by imprisonment for a term of seven to twelve years.

Note. The terms "website" and "web page" are used in the meaning defined in the law of Ukraine "On copyright and related rights".

The terms "electronic communication network" and "technical means of electronic communications" are used in the meaning defined in the law of Ukraine "On electronic communications".

The term "information (automated) system" is used in the meaning defined in the Law of Ukraine "On information protection in information and communication systems".

Turning to international experience, it is worth noting that the EU Drugs Action Plan 2021-2025[4] stopping the use of logistics and digital channels for the distribution of illicit narcotic drugs in small and medium volumes is identified as one of the key goals. This demonstrates an internationally accepted understanding of the threats posed by the use of the digital space for the distribution of narcotic substances. Considering Ukraine's European integration aspirations, the adaptation of national legislation to the relevant EU standards is relevant and necessary. In particular, legislative initiatives should be aimed at effectively blocking the use of digital channels (social networks, instant messengers, anonymous platforms) for drug distribution and related advertising activities. This approach will not only promote rapprochement with EU legal norms, but will also strengthen internal security and increase the level of protection of public health in the face of hybrid warfare and threats to the information space.

In particular, direct advertising of medicines is prohibited in most high-income countries, with the exception of the United States of America and New Zealand (Menkes *et al*., 2023). Such restrictions are aimed at protecting the health of citizens, in particular, to prevent self-medication. In some countries, certain types of narcotic drugs may also be classified as medicinal products. For example, in Canada, opioids may be recognised as medicinal products[5]. It is stated that no person shall be entitled to seek or receive opium from a medical practitioner unless that person discloses to the medical practitioner information about the acquisition of each substance from the controlled drug lists, and any authorisation to obtain such substances from any other medical practitioner within the preceding thirty days. To address the issue of opioid advertising, there is a pre-screening procedure: the advertising pre-approval agency evaluates all opioid-related medications. Only after the official approval of this agency, which must be recognised by the Canadian Ministry of Health, is the placement of such advertising permitted. Such measures are aimed at preventing advertising of prohibited narcotic substances.

[1] Criminal Code of Ukraine. (2001, April). Retrieved from https://zakon.rada.gov.ua/laws/show/2341-14#Text.
Law of Ukraine No. 580-VIII "On the National Police". (2015, July). Retrieved from https://zakon.rada.gov.ua/laws/show/580-19#Text.
[2] Draft Law of Ukraine No. 7558 "On Amendments to the Code of Ukraine on Administrative Offenses and the Criminal Code of Ukraine to Improve Liability for Illegal Placement of Advertising on Territories, Buildings and Structures, as Well as for Advertising of Narcotic Drugs". (2022, July). Retrieved from https://itd.rada.gov.ua/billinfo/Bills/Card/40015.
[3] Criminal Code of Ukraine. (2001, April). Retrieved from https://zakon.rada.gov.ua/laws/show/2341-14#Text.
[4] EU Drugs Action Plan 2021-2025. (2021, July). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AJOC_2021_272_R_0002.
[5] Controlled Drugs and Substances Act of Canada. (1996, June). Retrieved from https://laws-lois.justice.gc.ca/eng/acts/C-38.8/page-1.html#docCont.

It should also be noted that the International Narcotics Control Board (INCB), an independent body operating under the auspices of the UN, calls on governments to step up efforts to regulate social networks that romanticise drug-related behaviour and encourage the illegal sale of controlled substances. In its annual report, the INCB highlights the growing body of evidence for a link between digital content exposure and drug use, which is particularly reflected in young people – the main audience of social platforms. United Nations (2022) also calls on private sector representatives to actively moderate, self-regulate, and restrict advertising for non-medical drug use.

In the context of the study of the situation in the Nordic countries, J. Demant *et al*. (2020) emphasised that social networks are a common tool for drug distribution. The researchers emphasised that it is the availability of communication channels that is crucial when choosing the media used to distribute drugs and other prohibited substances. In this regard, researchers recommend supplementing police strategies with preventive information campaigns to prevent and limit the spread of narcotic substances.

Thus, around the world, traditional forms of drug sales – when drugs are transferred personally from hand to hand – are gradually being replaced by new formats, in particular online trading. The number of so-called "online dealers" is growing both in Ukraine and in other countries. This is facilitated by the rapid development of digital technologies and the growing anonymity of internet users. The digital environment allows for drug advertising campaigns on a scale that was not possible before the Internet age. The use of advertising by people involved in the sale of drugs plays a significant role in increasing the volume of illegal trade in harmful substances. Therefore, the fight against drug advertising at the legislative level becomes particularly relevant as a component of the overall strategy for countering drug addiction and reducing the level of drug addiction among the population.

Discussion

As the consequences of the spread of drug advertising, in particular, through the Internet, become more and more threatening, researchers around the world are increasingly raising the issue of the need to criminalise such advertising and studying its impact on society. The accumulated results of these studies form a weighty theoretical basis for further development of an effective legal policy in the field of countering drug addiction, in particular, in the aspect of information security. This problem remains relevant and unresolved in a number of countries, including Ukraine.

In this context, the study by A. Oksanen *et al.* (2020) deserves attention, which emphasises that young people are increasingly using social networks as a platform for the purchase and distribution of drugs and other prohibited substances. The study showed that most people who buy drugs online do so through social networks, where there is advertising content of a corresponding nature. The researchers emphasised that social networks promote impulsive decision-making, especially among young people, who are most vulnerable to such influence. In this regard, researchers emphasise the need for increased control over advertising activities in social networks, as one of the key areas of preventive anti-drug policy. The conclusions are quite appropriate, because the study was conducted in a gender-balanced way, based on the responses of adolescents and young people aged 15 to 25 years, considering the psychological state of respondents.

In turn, B.N. Rutherford *et al*. (2022) noted that a large number of videos are distributed on the TikTok platform in which teenagers smoke cannabis to attract attention and gain popularity. Most of the comments on such videos were flattering, and none of them had age restrictions. This indicates that on such social platforms, the demonstration, advertising or even sale of narcotic substances can be carried out openly. Given the results of this study, the findings of these researchers can also be considered as part of a larger phenomenon: trends in increasing advertising in social networks, the target audience of which is teenagers.

M. Gansner *et al*. (2024) focused on the growing number of overdose deaths among adolescents associated with counterfeit prescription drugs purchased through social media. The researchers found that the likelihood of substance use increases significantly on days when adolescents come into contact with relevant digital content published by their peers. The findings support concerns that social media may play a role as an intermediary in shaping drug-related behaviour. This study highlighted the critical need to criminalise drug advertising in the digital environment, which is an important component of the overall strategy to combat drug addiction among young people.

R. Van der Sanden *et al*. (2021) pointed to the growing number of reports about the use of social networks to buy and sell illegal drugs internationally. The survey showed that the main advantages of making purchases through social networks, according to respondents, are "high convenience" (74% of respondents) and "transaction speed" (43% of respondents). Narcotic drugs were purchased from individuals who positioned themselves as drug dealers. The researchers emphasised the importance of integrating social platforms into national drug addiction prevention strategies, especially among young people. The results once again confirmed that the latest digital technologies significantly facilitate the possibility of advertising narcotic drugs. However, a more detailed study of the seller's side, not just the buyer's, would be a valuable scientific addition to this study.

T.V. Shevchenko (2024) noted that the illegal sale of narcotic drugs through electronic information

resources allows malefactors to avoid exposure for a long time and involve more young people in drug addiction. The researcher proposed to amend the legislation, as a result of which an attacker who sold drugs through electronic information resources would receive more punishment than when committing this crime without using such resources. To some extent, the changes proposed by the researcher can serve as an alternative to the changes proposed in this study. However, they did not provide for penalties for persons who did not sell drugs, but only manufactured or distributed their advertising, and therefore such legislative changes cannot fully replace those proposed in this paper.

Conclusions

The subject of this study was the criminalisation of advertising of narcotic drugs, psychotropic substances, and their analogues. The study assessed the need to criminalise advertising of narcotic drugs, psychotropic substances, and their analogues: in particular, the production and distribution of such advertising. The harmfulness of drug use for the individual and for the surrounding society was also emphasised: depressive states, loss of social ties, increased crime, etc. The paper analysed the research on the negative impact of narcotic substances on the mental health of a person dependent on them. It was considered that the number of drug-related crimes increased significantly in 2024, compared to previous years. It was also noted that the distribution of advertising of narcotic drugs often occurs through popular social networks or instant messengers used by teenagers and young people. It was pointed out that it is mainly young people who buy narcotic and psychotropic substances through social networks and instant messengers, who choose this method of purchasing drugs and other prohibited means for convenience. It was proposed to criminalise advertising of narcotic drugs, psychotropic substances, and their analogues. The reasons why it is necessary to criminalise advertising of such substances, and not "propaganda of drug use", were given.

All of the above suggests that, given the increase in the number of crimes related to narcotic drugs and psychotropic substances, and existing research on this topic, the need to criminalise advertising of narcotic drugs and psychotropic substances really exists. This is especially important for protecting teenagers and young people from the impact of advertising narcotic drugs or psychotropic substances on them when using instant messengers and social networks. In general, this topic is very broad and open for further research: in particular, a promising topic for consideration would be the assessment of the impact of drug advertising on different people (different ages, different genders, and different financial opportunities). The limitation of this study was the fact that most countries that prohibit advertising of drugs and psychotropic drugs prohibit it in the context of banning advertising of drugs that require a doctor's prescription (including drugs), and not separately drugs and psychotropic substances, and that, at present, there are no studies on the impact of romanticisation of drug use and psychotropic substances on adolescents and young people, the presence of which would help to better investigate the dangers of drug advertising and draw even more accurate conclusions.

Acknowledgements

None.

Funding

This study was not funded.

Conflict of Interest

None.

References

[1] Aldridge, J., & Décary-Hétu, D. (2016). Hidden wholesale: The drug diffusing capacity of online drug cryptomarkets. *International Journal of Drug Policy*, 35, 7-15. doi: 10.1016/j.drugpo.2016.04.020.

[2] Al-Rawi, A. (2020). The convergence of social media and other communication technologies in the promotion of illicit and controlled drugs. *Journal of Public Health*, 44(1), 153-160. doi: 10.1093/pubmed/fdaa210.

[3] Australion Bureau of Statisties. (2023). *National study of mental health and wellbeing*. Retrieved from https://surl.li/zercyw.

[4] Cristello, J.V., Litt, D.M., Sutherland, M.T., & Trucco, E.M. (2023). Subjective norms as a mediator between exposure to online alcohol and marijuana content and offline use among adolescents. *Drug and Alcohol Review*, 43(1), 111-121. doi: 10.1111/dar.13620.

[5] Demant, J., Bakken, S.A., & Hall, A. (2020). Social media markets for prescription drugs: Platforms as virtual mortars for drug types and dealers. *Drugs and Alcohol Today*, 20(1), 36-49. doi: 10.1108/dat-06-2019-0026.

[6] Denysiuk, Z.Z. (2021). Propaganda and counterpropaganda in the context of state information policy strategies. *Scientific Notes of Taurida V.I. Vernadsky University*, *Series "Public Administration"*, 2, 46-51. doi: 10.32838/tnu-2663-6468/2021.2/08.

[7] Dewey, M., & Buzzetti, A. (2024). Easier, faster and safer: The social organization ofdrug dealing through encrypted messaging apps. *Sociology Compass*, 18(2), article number e13175. doi: 10.1111/soc4.13175.

[8] Didenko, K.I. (2025). *Psychological features of the emotional-volitional sphere of people who use alcohol and narcotic substances*. (Master's diploma, Zaporizhzhia National University, Zaporizhzhia, Ukraine).

[9] Fuller, A., Vasek, M., Mariconti, E., & Johnson, S.D. (2023). Understanding and preventing the advertisement and sale of illicit drugs to young people through social media: A multidisciplinary scoping review. *Drug and Alcohol Review*, 43(1), 56-74. doi: 10.1111/dar.13716.

[10] Gansner, M., Horton, A.K., Singh, R., & Schuman-Olivier, Z. (2024). Exploring relationships between social media use, online exposure to drug-related content, and youth substance use in real time: A pilot ecological momentary assessment study in a clinical sample of adolescents and young adults. *Frontiers in Child and Adolescent Psychiatry*, 3, article number 1369810. doi: 10.3389/frcha.2024.1369810.

[11] General Prosecutor's Office of Ukraine. (2025). *Registered criminal offenses and results of their pre-trial investigation*. Retrieved from https://gp.gov.ua/ua/posts/pro-zareyestrovani-kriminalni-pravoporushennya-ta-rezultati-yih-dosudovogo-rozsliduvannya-2.

[12] General Prosecutor's Office of Ukraine. (n.d.). *On registered criminal offences and the results of their pre-trial investigation*. Retrieved from https://gp.gov.ua/ua/posts/pro-zareyestrovani-kriminalni-pravoporushennya-ta-rezultati-yih-dosudovogo-rozsliduvannya-2.

[13] Horobets, N., Reznik, O., Riamzina, A., Samsin, R., & Denysenko, S. (2024). Digital markets dynamics and ethical considerations of online drug sales via cryptomarkets. *South Eastern European Journal of Public Health*, 24(1), 600-612. doi: 10.70135/seejph.vi.1403.

[14] Institute of Psychiatry, Forensic Psychiatric Examination, & Drug Monitoring of the Ministry of Health of Ukraine. (2023). *Online survey on the prevalence and frequency of use of certain narcotic and psychotropic substances in Ukraine – 2023*. Retrieved from https://surl.li/hzabgh.

[15] Kudermina, O., Kazmirenko, V., Tagiev, S. R. O., Puzyrov, M., & Samofalov, O. (2019). Actual issues of counterdrug activities under the current conditions of Ukraine and world development. *Journal of Legal, Ethical and Regulatory Issues*, 22(2S).

[16] Kuryliuk, Y., Nikiforenko, V., Filippov, S., Shvedova, H., & Vazhynsky, V. (2021). Current state of drug crime control in Ukraine. *Pharmacology Online*, 2, 1020-1025.

[17] Leheza, Y., Shablystyi, V., Aristova, I., Kravchenko, I., & Korniakova, T. (2023). Foreign experience in legal regulation of combating crime in the sphere of trafficking of narcotic drugs, psychotropic substances, their analogues and precursors: Administrative and criminal aspect. *Journal of Drug and Alcohol Research*, 12(4), article number 236240. doi: 10.4303/JDAR/236240.

[18] Menkes, D.B., Mintzes, B., & Lexchin, J. (2024). Direct-to-consumer advertising: A modifiable driver of overdiagnosis and overtreatment. *BMJ Evidence-Based Medicine*, 29(6), 423-425. doi: 10.1136/bmjebm-2023-112622.

[19] Ministry of Internal Affairs of Ukraine. (2020). *Users of the StopNarkotyk chatbot helped block 1,500 drug addresses*. Retrieved from https://mvs.gov.ua/presscenter/news/Koristuvachi_chat_botu_StopNarkotik_dopomogli_zablokuvati_1500_narkoadres_33548.

[20] Motyka, M.A., & Al-Imam, A. (2021). Representations of Psychoactive Drugs' Use in Mass Culture and Their Impact on Audiences. *International Journal of Environmental Research and Public Health*, 18(11), article number 6000. doi: 10.3390/ijerph18116000.

[21] Oksanen, A., Miller, B. L., Savolainen, I., Sirola, A., Demant, J., Kaakinen, M., & Zych, I. (2020). Illicit drug purchases via social media among american young people. In *Social computing and social media. Design, ethics, user behavior, and social network analysis* (p. 278-288). Cham: Springer International Publishing. doi: 10.1007/978-3-030-49570-1_19.

[22] Peráček, T., Mucha, B., Brestovanská, P., & Strážovská, Ľ. (2019). Legal regulation of drug advertising and its restrictions in the conditions of the Slovak Republic. *European Pharmaceutical Journal*, 66(1), 4-10. doi: 10.2478/afpuc-2019-0001.

[23] Petersen, M.A., Petersen, I.L., Poulsen, C., & Nørgaard, L.S. (2021). #studydrugs–Persuasive posting on Instagram. *International Journal of Drug Policy*, 95, article number 103100. doi: 10.1016/j.drugpo.2020.103100.

[24] Pokataev, P., Bodnarchuk, O., Hryshyna, T., Korolkov, V., & Demianchuk, Y. (2023). Advertising of medicines in Ukraine: An ethical and legal view. *Revista Amazonia Investiga*, 12(64), 348-360. doi: 10.34069/ai/2023.64.04.37.

[25] Public Health Centre of the MHP of Ukraine. (2024). *National Report of the Drug Situation in Ukraine 2024 (based on data from 2023)*. Retrieved from https://phc.org.ua/news/nacionalniy-zvit-schodo-narkotichnoi-situacii-v-ukraini-2024-za-danimi-2023-roku.

[26] Public Health Centre. (2024). *National Report of the Drug Situation in Ukraine 2024 (based on data from 2023)*. Retrieved from https://surl.li/gcxqys.

[27] Rutherford, B.N., Sun, T., Johnson, B., Co, S., Lim, T.L., Lim, C.C.W., & Chan, G.C.K. (2022). Getting high for likes: Exploring cannabis-related content on TikTok. *Drug and Alcohol Review*, 41(5), 1119-1125. doi: 10.1111/dar.13433.

[28] Sheludko, A.O. (2023). *Formation of adaptive and constructive coping strategies in military personnel*. (Master's thesis, National Aviation University, Kyiv, Ukraine).
[29] Shevchenko, T.V. (2024). Illegal sale of narcotic drugs using electronic information resources: Problems of qualification. *Scientific Bulletin of Uzhhorod National University*, 3(84), 408-414. doi: 10.24144/2307-3322.2024.84.3.61.
[30] Sim, Y. (2023). The effect of opioids on crime: Evidence from the introduction of oxycontin. *International Review of Law and Economics*, 74, article number 106136. doi: 10.1016/j.irle.2023.106136.
[31] Spilka, S., Le Nézet, O., Janssen, E., Brissot, A., Philippon, A., & Eroukmanoff, V. (2024). *Trends in illicit drug use levels in France in 2023*. Retieved from https://www.ofdt.fr/sites/ofdt/files/2024-06/tendances_164_eropp.pdf.
[32] Statistics Canada. (n.d.). *Health behaviours and substance use.* Retieved from https://www150.statcan.gc.ca/n1/pub/82-570-x/2023001/section2-eng.htm.
[33] Substunce Abuse and Mental Health Services Administration. (n.d.). *2023 National Survey on drug use and health*. Retrieved from https://www.samhsa.gov/data/data-we-collect/nsduh-national-survey-drug-use-and-health/national-releases/202.
[34] Torres, N.G. (2024). *Illegal drug use and violent crime are on the rise amid crisis, Cuba's leader admits*. Retrieved from https://www.miamiherald.com/news/nation-world/world/americas/cuba/article290353439.html.
[35] United Nations. (2022). *Break the link between illicit drugs and social media: UN-backed report*. Retieved from https://news.un.org/en/story/2022/03/1113642.
[36] Van der Sanden, R., Wilkins, C., Romeo, J.S., Rychert, M., & Barratt, M.J. (2021). Predictors of using social media to purchase drugs in New Zealand: Findings from a large-scale online survey. *International Journal of Drug Policy*, 98, article number 103430. doi: 10.1016/j.drugpo.2021.103430.

Аналіз практики криміналізації реклами наркотичних засобів, психотропних речовин та їх аналогів

Оксана Брисковська
Кандидат юридичних наук, старший науковий співробітник
Національна академія внутрішніх справ
03035, пл. Солом'янська, 1, м. Київ, Україна
https://orcid.org/0000-0001-6902-9969

Геннадій Шевчук
Кандидат юридичних наук, доцент
Національна академія внутрішніх справ
03035, пл. Солом'янська, 1, м. Київ, Україна
https://orcid.org/0000-0002-0108-6227

Оксана Волуйко
Кандидат психологічних наук, доцент
Національна академія внутрішніх справ
03035, пл. Солом'янська, 1, м. Київ, Україна
https://orcid.org/0000-0002-3723-5415

Анотація
Актуальність теми полягає в тому, що інформаційна сфера та просування наркотиків часто залишаються поза межами ефективного правового реагування. Особливої гостроти ця проблема набуває в Україні, адже війна, соціальна нестабільність і послаблення інституційного контролю сприяють активізації наркозлочинності, зокрема, в інформаційному просторі. Метою статті була оцінка потреби в криміналізації реклами наркотичних засобів, психотропних речовин та їх аналогів в Україні. Для цього застосовано системно-структурний, порівняльний, статистичний, системний, екстраполювання методи. Обґрунтовано, що збільшення кількості осіб, які вживають наркотичні речовини, майже в півтора раза може бути пов'язано, зокрема, з легкою доступністю реклами наркотичних речовин у повсякденному житті людини: як офлайн, так і онлайн. З'ясовано, що під час соціальної нестабільності, зумовленої сучасними змінами та соціальними реаліями війни, які психологічно травмують осіб, виникли придатні умови для обігу наркотичних засобів та їх реклами. Запропоновано зміни до кримінального законодавства України, які криміналізують рекламу наркотичних засобів в Україні, спрощуючи для правоохоронних органів розслідування та доведення правопорушень, пов'язаних з наркотиками. Встановлено, що, попри наявність окремих заборон і норм, кримінальне законодавство України, врахувавши запропоновані в цій статті зміни, може стати ефективнішим для захисту населення від наркотичної залежності. У цьому контексті особливого значення набуває вивчення міжнародного досвіду, зокрема практик країн Європейського Союзу, Сполучених Штатів Америки та Канади. Таким чином, дослідження криміналізації реклами наркотичних засобів і психотропних речовин має наукову й практичну значущість, оскільки сприяє вдосконаленню кримінального законодавства України, формуванню єдиної правозастосовної практики та забезпеченню захисту суспільства від поширення злочинності, пов'язаної з наркотичними засобами

Ключові слова:
наркозлочинність; криптовалюта; незаконний обіг; адміністративна та кримінальна відповідальність; міжнародний досвід; правоохоронний орган

UDC 004.056:342.9
DOI: 10.63341/naia-chasopis/3.2025.24

Prospects for state regulation of cryptographic data protection

Mariia Turchina
PhD in Law
Yaroslav Mudryi National Law University
61024, 77 Hryhorii Skovoroda Str., Kharkiv, Ukraine
https://orcid.org/0000-0002-1486-1122

Igor Rudenko*
Master of Science
Yaroslav Mudryi National Law University
61024, 77 Hryhorii Skovoroda Str., Kharkiv, Ukraine
https://orcid.org/0009-0008-3582-3951

Olha Khorolska
Master of Science
Yaroslav Mudryi National Law University
61024, 77 Hryhorii Skovoroda Str., Kharkiv, Ukraine
https://orcid.org/0009-0004-9853-2378

Abstract
The relevance of the study was determined by the need for legal and technical rethinking of state regulation of cryptographic information protection under the conditions of Ukraine's digital transformation. The aim of the article was to identify the effectiveness of the existing regulatory, institutional, and technical model for data cryptographic protection, taking into account the provisions of international standards. The study applied methods of structural-functional analysis, systematic comparison of legal provisions, and content analysis of technical requirements. As a result of the study, it was established that the regulatory field covered two levels of influence – general technical and specialised – yet only approximately sixty percent of the provisions on electronic signature, cryptographic key management, and timestamps corresponded to international technical requirements. Fragmentation in the definition of mandatory certification procedures and the absence of unified regulations in the field of digital identification and electronic seals were recorded. Within the framework of interinstitutional interaction, it was found that only three out of eight functional areas were governed by formalised mechanisms, which complicated the response to cryptographic incidents. Technical analysis confirmed that the average key length in cryptographic algorithms resistant to quantum computing systems exceeded three thousand bits – two to three times higher than the parameters of traditional algorithms – yet the implementation of such solutions into the state certification system was limited. It was also established that only a portion of cryptographic protection hardware complied with

Article's History:
Received: 28.05.2025
Revised: 02.09.2025
Accepted: 29.09.2025

Suggest Citation:
Turchina, M., Rudenko, I., & Khorolska, O. (2025). Prospects for state regulation of cryptographic data protection. *Law Journal of the National Academy of Internal Affairs*, 15(3), 24-44. doi: 10.63341/naia-chasopis/3.2025.24.

*Corresponding author

international technical security level requirements. The practical significance of the study results lay in the potential application for updating the regulatory architecture, forming technical regulations, developing state control procedures, and supporting public authorities, technical expert units, and developers in the implementation of the national cybersecurity strategy

Keywords:
digital identification; electronic signature; certification of means; information security; technical standard; interagency coordination; digital transformation

Introduction

In the field of information security, the importance of forming a comprehensive system of cryptographic protection capable of ensuring the continuity of state information resources and maintaining the confidentiality of critical data is increasing. Under conditions of rapid development of digital services and the expansion of personal and official data processing in the public sector, there arises a need for formalised, legally and technically harmonised regulation of cryptographic mechanisms. The problem lies in the absence of a unified model that would combine the requirements of technical compliance, legal status of protection tools, and organisational responsibility of the entities involved in the implementation of information protection solutions.

The relevance of the studied issue was driven by the limited nature of existing state oversight instruments, the insufficient unification of cryptographic certification procedures, and the lack of standardised models of inter-agency coordination. The need to develop effective mechanisms for technical control, legal authorisation, and centralised monitoring reveals structural deficiencies in the current regulatory and institutional architecture. This issue complicates the implementation of a coherent state policy in the field of information protection and creates risks in processes of electronic identification, digital document management, and the functioning of access management systems to information resources.

In the study by J. Kazimi & H. Thalwal (2024), attention was focused on legal challenges and technological risks associated with modern models of cryptographic protection. As a result, it was established that existing regulatory frameworks largely do not cover the dynamics of quantum threats, creating a gap between the level of regulation and current technical needs. Separately, it was noted that the implementation of cryptographic service control tools in the public sector is uneven. In the work of A. Vargiolu (2022), the approaches of the Organisation for Economic Co-operation and Development to the formation of a global privacy policy were analysed. The author identified that the existence of a single principled approach to encryption in the context of cross-border data exchange contributes to strengthening trust between states but requires technical adaptation in each specific case.

K. Limniotis (2021) examined the significance of cryptography as a tool for protecting fundamental rights and freedoms, emphasising its role in the formation of digital inviolability. It was shown that the use of cryptographic solutions significantly reduces the risk of violations of privacy rights in digital ecosystems. S. Bommareddy *et al.* (2022) focused on the security of medical data, identifying the key role of authentication mechanisms and protection of transmission channels. The authors confirmed that the level of protection directly depends on the technical compatibility of cryptographic protocols with electronic healthcare systems. In the work of Y. Kokarcha & A. Lalueva (2022), the impact of martial law on the protection of personal data on social networks was studied. It was shown that legal guarantees remain limited without an appropriate level of technical cryptographic support.

In the study of M.V. Zinchuk (2024), the legal regulation of confidential information in Ukraine was examined, with emphasis on contradictions between legislation and technical regulations. It was established that the growth of digital threats was not accompanied by a proportional development of state control mechanisms. Y.V. Kostiuk *et al.* (2025) analysed cryptographic protection hardware and the compliance with international standards. It was revealed that hardware solutions certified under international protocols demonstrate higher effectiveness in complex information environments. In the publication by A.K. Yanamala & S. Suryadevara (2024), the interdependence between transparency of certification procedures and the level of trust in cryptographic services was studied. The authors confirmed that the absence of open audit mechanisms significantly reduces the legitimacy of implemented solutions.

A second contribution by A. Vargiolu (2022) consisted in clarifying the international challenges of harmonising cryptographic privacy standards. The analysis established that the inconsistency of technical parameters made operational interaction between state cryptographic platforms impossible. In the study of T. Riebe *et al.* (2022), the dual status of cryptography in the context of security and surveillance was discussed. It was established that the US policy of controlling the export of cryptographic solutions limits the global interoperability of protection tools, which resulted in decreased effectiveness of transnational coordination.

J. Chen (2020) studied the evolution of China's cryptographic legislation, paying attention to the

transition to centralised regulation. It was shown that such a model increases manageability but may hinder technological innovation in the case of strict administrative dependence of the technical sector. In the work of B. Firmansyah & R. Bansal (2024), the processes of cryptographic standardisation under growing complexity of digital platforms were considered. It was found that updates to the regulatory and technical base lag behind developments in the field of post-quantum security, and certification systems demonstrate low adaptability to new infrastructures, including the metaverse and blockchain models.

The analysed academic studies showed the absence of a comprehensive assessment of the effectiveness of the regulatory, institutional and technical model of state cryptographic protection governance under conditions of digital transformation. A systematic analysis of the content of current legal and regulatory acts in comparison with international technical standards – particularly in the field of certification, key management and digital identification – was not presented. The studies did not highlight the structure of powers of authorised cryptographic control bodies, nor did the studies analyse the actual state of inter-agency cooperation in identifying and responding to cryptographic incidents. The results of comparative assessment of classical and post-quantum protection algorithms also remained uninterpreted, which limits the opportunities for forming a modern technical policy in the field of cryptographic certification. These gaps determined the need to conduct a study aimed at integrating legal and technical information protection mechanisms, assessing the level of compliance of national solutions with international standards, and formulating recommendations for updating the regulatory architecture.

The purpose of the study was a comprehensive investigation of the regulatory, institutional, and technical foundations of state governance of cryptographic information protection under conditions of digital transformation, taking into account the requirements of international standards. To achieve this aim, the following objectives were set: to analyse the content and coherence of the main legal and regulatory acts governing cryptographic data protection; to assess the structure of powers of authorised bodies and the nature of inter-agency cooperation in the field of cryptographic control; to determine the level of compliance of national technical requirements with international standards in the areas of certification and digital identification.

Materials and Methods

The study had an applied interdisciplinary nature with a predominance of qualitative analysis, including elements of comparative, regulatory-legal and technical-standardisation approaches, and was based on an extended source base covering the period from 1994 to 2025. The methodology of the study was based on a combination of analysis of regulatory acts, evaluation of technical specifications and institutional modelling of regulatory practices. The analysis was carried out considering the dynamics of regulatory changes, the evolution of cryptographic algorithms, and the transformation of the institutional architecture of executive bodies responsible for the implementation of policy in the field of digital security.

To ensure the completeness of the empirical base, a set of open regulatory acts, technical standards, methodological guidelines and official reports related to state regulation in the field of cryptographic information protection was used. The core of the source base consisted of the current editions of the Law of Ukraine "On Information Protection in Information and Telecommunications Systems"[1], Law of Ukraine "On Cryptographic Protection of Information"[2] and Law of Ukraine "On Electronic Trust Services"[3]. To provide a comprehensive description of the administrative-legal model, the norms of the Code of Ukraine on Administrative Offences[4], Criminal Code of Ukraine[5] та Decree of the President of Ukraine "On the Decision of the National Security and Defence Council of Ukraine of May 14, 2021 "On the Cybersecurity Strategy of Ukraine"[6] were also used. In the field of institutional regulation, the Law of Ukraine "On the State Service for Special Communications and Protection of Ukraine"[7] was involved, along with materials on the activities of the National Security and Defence Council of Ukraine (n.d.), the Security Service of Ukraine (n.d.) and the National Police of Ukraine (n.d.). The technical parameters of cryptographic algorithms were evaluated based on documents from the International Organisation for Standardisation/International Electrotechnical Commission (ISO/IEC): ISO/IEC No. 15408-1 "Evaluation criteria for

[1] Law of Ukraine No. 80/94-VR "On Information Protection in Information and Telecommunications Systems". (1994, July). Retrieved from https://zakon.rada.gov.ua/laws/show/80/94-вр.
[2] Law of Ukraine No. 803-XIV "On Cryptographic Protection of Information". (1999, December). Retrieved from https://zakon.rada.gov.ua/laws/show/803-14.
[3] Law of Ukraine No. 2155-VIII "On Electronic Trust Services". (2017, October). Retrieved from https://zakon.rada.gov.ua/laws/show/2155-19.
[4] Code of Ukraine on Administrative Offenses. (1984, December). Retrieved from https://zakon.rada.gov.ua/laws/show/80731-10.
[5] Criminal Code of Ukraine. (2001, April). Retrieved from https://zakon.rada.gov.ua/laws/show/2341-14.
[6] Decree of the President of Ukraine No. 447/2021 "On the Decision of the National Security and Defense Council of Ukraine of May 14, 2021 "On the Cybersecurity Strategy of Ukraine". (2021, August). Retrieved from https://zakon.rada.gov.ua/laws/show/96/2021.
[7] Law of Ukraine No. 3475-IV "On the State Service for Special Communications and Information Protection of Ukraine". (2006, February). Retrieved from https://zakon.rada.gov.ua/laws/show/911-2006-п.

IT security" (2009), ISO/IEC No. 18033-1 "Encryption algorithms" (2021), and ISO/IEC No. 19790 "Security requirements for cryptographic modules" (2012), as well as using data from the National Institute of Standards and Technology (2008; 2019; 2020). Within the framework of the analysis, the specifications of ISO/IEC No. 7816-4 "Integrated circuit cards" (2020), the results of the Post-Quantum Cryptography (PQC) standardisation project of the US National Institute of Standards and Technology, and the recommendations of the European Union Agency for Cybersecurity (2014) were taken into account. To evaluate certification compatibility, the provisions of the European Telecommunications Standards Institute (2016a; 2016b; 2018) were applied, taking into account the compliance criteria of the Federal Information Processing Standard (FIPS) 140-2 (National Institute of Standards and Technology, 2001). Additionally, the provisions of the updated Regulation of the European Parliament and of the Council "On Electronic Identification and Trust Services for Electronic Transactions in the Internal Market and Repealing Directive 1999/93/EC"[1] were used, which allowed national mechanisms to be compared with the requirements of cross-border regulatory harmonisation.

The method of structural-functional analysis was used to study the organisational structure of state regulation mechanisms in the field of cryptographic information protection. This method allowed for a clear division of responsibilities among the main divisions of the State Service of Special Communications and Information Protection of Ukraine by functional areas, in particular in relation to strategic management, technical expertise, standardisation, and control. The results of the analysis made it possible to compare the institutional structure with approaches used in EU countries and to evaluate its compliance with the European model of regulatory distribution.

The method of comparative law was applied to compare the regulatory acts of Ukraine in the field of cryptographic protection with the relevant acts of EU law. Within this approach, the provisions of Ukrainian laws on information security and cryptographic protection were analysed and compared with the provisions of the European regulation on electronic identification, as well as with the technical standards of the European Telecommunications Standards Institute and the European Union Agency for Cybersecurity. On this basis, the level of harmonisation was established in the areas of certification of cryptographic protection tools, electronic signatures, digital timestamps, key, and seal management.

Content analysis of technical regulations was conducted to determine the requirements for the implementation of cryptographic algorithms, authentication hardware, and the compliance with certification standards. The analysis covered technical profiles of classical algorithms, including Rivest-Shamir-Adleman (RSA), Advanced Encryption Standard (AES), Elliptic Curve Digital Signature Algorithm (ECDSA), and promising post-quantum solutions: Dilithium, Kyber, SABER. The data obtained allowed for a comparative assessment of cryptographic key length, cryptographic robustness, and the level of integration of the mentioned algorithms into national certification procedures. The interpretation of results was carried out by integrating regulatory, institutional, and technical aspects, which made it possible to form a comprehensive model of the current state of cryptographic regulation and its alignment with international approaches. The effectiveness assessment was conducted by comparing legal regulation, organisational functionality, and technical implementation with established international compatibility criteria, which enabled the formulation of generalised conclusions and recommendations.

Results

Regulatory and legal support for cryptographic information protection: evolution and current state in Ukraine. In the process of forming a systemic model of state regulation of cryptographic information protection in Ukraine, a key analytical task is the study of the legal and regulatory foundations that define the legal status and operational conditions of cryptographic security tools. The basis for such regulation is set out in the provisions of the Law of Ukraine No. 80/94-VR[2] and Law of Ukraine No. 803-XIV[3]. These acts establish the principles of technical admissibility, mandatory certification, and the legal regime for the circulation of cryptographic protection of information (CPI) tools, while differing in terms of the structure of subject regulation and the allocation of competencies.

A comparative analysis of these laws allows identifying systemic overlaps in the definition of regulated objects, user categories, and liable entities, while also highlighting differences in the formulation of technical criteria and the scope of supervisory powers of authorised bodies. It is also important to identify gaps that arise in the context of the absence of coordinated procedures for inter-agency verification of CPI tools and legal liability for the unauthorised use. This approach makes it possible not only to identify areas of legislative

[1] Regulation of the European Parliament and of the Council No. 910/2014 "On Electronic Identification and Trust Services for Electronic Transactions in the Internal Market and Repealing Directive 1999/93/EC". (2014, July). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32014R0910.
[2] Law of Ukraine No. 80/94-VR "On Information Protection in Information and Telecommunications Systems". (1994, July). Retrieved from https://zakon.rada.gov.ua/laws/show/80/94-вр.
[3] Law of Ukraine No. 803-XIV "On Cryptographic Protection of Information". (1999, December). Retrieved from https://zakon.rada.gov.ua/laws/show/803-14.

uncertainty, but also to formulate initial provisions for updating the regulatory framework in line with international practices. To visualize the correlation of key legal parameters, a generalised Table 1 is presented below. It reflects the content of the relevant legal and regulatory acts according to the criteria of regulatory subject, categories of entities, requirements for technical tools, institutional control, and legal liability measures in cases of violation of the established procedure for the application of CPI. Such structuring lays the groundwork for further comparative analysis of the effectiveness of legal enforcement practices.

Table 1. Comparative characteristics of Ukrainian laws in the field of cryptographic information protection

Criterion	Law of Ukraine No. 80/94-VR[1]	Law of Ukraine No. 803-XIV[2]
Subject of regulation	Information protection in information and telecommunications systems through the use of technical and software and hardware methods	Organisation, implementation, and regulation of cryptographic protection of restricted access information
Circle of subjects	Owners of information and telecommunications systems, information managers, security administrators, authorised bodies	Business entities developing, supplying or operating CPI and government bodies
Requirements for technical means	The need for certification and compliance of equipment with established safety requirements has been identified	The mandatory nature of state expertise, certification, and the use of only permitted means is outlined.
Control	Control is carried out by relevant state authorities through security audits of information and telecommunications systems.	Licensing, control by the State Service of Special Communications and Information Protection of Ukraine, maintenance of the state register of certified CPI devices
Responsibility	Administrative liability for violation of information protection requirements in information and telecommunications systems	Liability for using uncertified CPIs and conducting activities without a licence

Source: developed by the authors

Comparative Table 1 illustrates the distribution of regulatory functions and the structural differentiation of legal benchmarks in the field of cryptographic information protection. The Law of Ukraine No. 80/94-VR focuses on ensuring the integrity of information infrastructure through technical regulation, which provides for mandatory certification of protection tools, compliance with technical security policies, and the exercise of administrative control. Meanwhile, the Law of Ukraine No. 803-XIV focuses on narrowly specialised aspects of cryptography as a component of information security, providing for licensing of entities, evaluation of cryptographic solutions, and the maintenance of state records of CPI tools.

The functional division of the circle of entities covered by these laws highlights differences in the purpose of regulatory oversight: in the first case, it concerns owners, administrators, and users of information and telecommunications systems; in the second – producers, developers, integrators, and suppliers of CPI tools. This model enables the construction of a hierarchical responsibility structure, in which general information security requirements are specified through a specialised cryptographic control regime. At the same time, a lack of coordination between these subsystems becomes evident, creating grounds for reviewing and updating approaches to the interaction within a unified cybersecurity system.

Within the study of legal and regulatory approaches to cryptographic information protection, it is also important to determine the level of compliance of Ukrainian legislation with international regulatory frameworks. Due to increased demands for cryptographic security of digital platforms – particularly in the areas of key management, CPI tool certification, electronic identification support, and IT product security assessment – the need for harmonising national regulation with standards such as ISO/IEC No. 15408-1 (2009), the European Telecommunications Standards Institute (2016a), the European Union Agency for Cybersecurity (2014), and the recommendations of the National Institute of Standards and Technology (2020) is growing. In this context, Table 2 systematises the compliance of key Ukrainian information security documents with international requirements and allows for an assessment of the current level of legal and technical alignment.

[1] Law of Ukraine No. 80/94-VR "On Information Protection in Information and Telecommunications Systems". (1994, July). Retrieved from https://zakon.rada.gov.ua/laws/show/80/94-вр.
[2] Law of Ukraine No. 803-XIV "On Cryptographic Protection of Information". (1999, December). Retrieved from https://zakon.rada.gov.ua/laws/show/803-14.

Table 2. Compliance of Ukrainian regulatory documents with international standards in the field of CPI

Regulatory document of Ukraine	International standard/document	Comment on compliance
Law of Ukraine No. 803-XIV[1]	National Institute of Standards and Technology SP 800-57, ISO/IEC No. 19790 (2012) – cryptographic key management policy	Provisions are partially harmonised; related principles of key information security policies are used
Law of Ukraine No. 80/94-VR[2]	ISO/IEC No. 27001 (2022) – information security management system	A general information security model is regulated in accordance with ISO No. 27001 (2022), partial coverage
Decree of the President of Ukraine No. 447/2021[3]	ISO/IEC No. 15408-1 (2009) (Common Criteria) – requirements for assessing the security of IT products	Technical requirements are adapted to Common Criteria; national compliance profile is used
Licensing conditions for the provision of services in the field of CPI	eIDAS[4], European Union Agency (2014) for Cybersecurity Guidelines – regulation of electronic identification and cryptographic services	The main requirements are harmonised; differences in the procedure for recognising and using electronic signatures remain

Source: developed by the authors

The analysis of Table 2 demonstrates a gradual, albeit uneven, integration of the national regulatory framework in the field of cryptographic information protection into the architecture of international regulatory standards. Despite existing differences in certification systems, the structure of cryptographic policies, and methods of subject identification, there is a clear movement towards the implementation of the provisions of ISO/IEC No. 15408-1 (2009), ISO/IEC No. 18033-1 (2021), the European Telecommunications Standards Institute (2016a), and the recommendations of the National Institute of Standards and Technology (2020). Particular attention has been given to the adaptation of key management procedures, technical audits of CPI tools, and minimum security criteria aligned with international profiles.

At the same time, Ukrainian regulation retains specific features, driven by the need to align legal norms with national models for the functioning of information systems. This is reflected, in particular, in differences in the procedure for recognising electronic signatures, limited application of unified electronic seal formats, and the absence of a centralised trust infrastructure. In view of this, the further development of harmonisation policy requires not only the formal alignment of technical requirements but also the updating of cross-border verification procedures, standardisation of post-quantum algorithms, and formalisation of mutual recognition of cryptographic certificates.

Within the analysis of the legal and regulatory support for cryptographic information protection, special attention should be paid to the mechanisms of state oversight and legal liability instruments for non-compliance with established requirements. Law enforcement practice in this area serves not only a supervisory but also a preventive function, creating an environment with heightened responsibility for subjects of information interaction. This issue becomes particularly relevant given the increasing role of CPI in public administration, the financial sector, national defence, and digital identity verification. To systematise the main types of violations, corresponding legal measures, and authorities authorised to exercise control, it is appropriate to refer to the generalised Table 3. It provides a structural classification of institutional powers, types of sanctions, and typical oversight application domains, allowing for a comprehensive assessment of the effectiveness of state regulation in the area of legal enforcement within the field of cryptographic protection.

Table 3. Types of CPI violations, sanctions and regulatory authorities

CPI violation type	Liability/sanctions	Competent control authority
Illegal use of uncertified CPI tools	Administrative liability under Article 188-39 of the Code of Ukraine on Administrative Offences[5]: fine up to UAH 1,700 with confiscation of equipment	State Service of Special Communications and Information Protection of Ukraine

[1] Law of Ukraine No. 803-XIV "On Cryptographic Protection of Information". (1999, December). Retrieved from https://zakon.rada.gov.ua/laws/show/803-14.
[2] Law of Ukraine No. 80/94-VR "On Information Protection in Information and Telecommunications Systems". (1994, July). Retrieved from https://zakon.rada.gov.ua/laws/show/80/94-вр.
[3] Decree of the President of Ukraine No. 447/2021 "On the Decision of the National Security and Defence Council of Ukraine of May 14, 2021 "On the Cybersecurity Strategy of Ukraine". (2021, August). Retrieved from https://zakon.rada.gov.ua/laws/show/96/2021.
[4] Regulation of the European Parliament and of the Council No. 910/2014 "On Electronic Identification and Trust Services for Electronic Transactions in the Internal Market and Repealing Directive 1999/93/EC". (2014, July). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32014R0910.
[5] Code of Ukraine on Administrative Offenses. (1984, December). Retrieved from https://zakon.rada.gov.ua/laws/show/80731-10.

Table 3, Continued

CPI violation type	Liability/sanctions	Competent control authority
CPI activities without a licence	Administrative liability under Article 164 of the Code of Ukraine on Administrative Offences[1]: fine from 17,000 to 34,000 UAH with confiscation of equipment	State Service of Special Communications and Information Protection of Ukraine, National Police (in cases of business activity without a licence)
Disclosure or leakage of key information	Criminal liability under Art. 328 or 361 Criminal Code of Ukraine[2]: up to 5 years of imprisonment	Security Service of Ukraine, National Police, Prosecutor's Office
Improper storage or transfer of cryptographic protection means	Warning or fine in accordance with the internal regulations of the State Service of Special Communications and Information Protection of Ukraine or based on the results of the audit	State Service of Special Communications and Information Protection of Ukraine, information security auditors
Use of cryptographic algorithms not permitted for use	Suspension of the certificate of conformity; requirement to remedy the violation	State Service of Special Communications and Information Protection of Ukraine, Technical Committee for Certification

Source: developed by the authors based on Law of Ukraine No. 3475-IV[3], Law of Ukraine No. 803-XIV[4]

The analysis of Table 3 confirms the existence of a multi-level system of legal liability in the field of cryptographic information protection in Ukraine. Under the current legislation, both administrative and criminal sanctions are provided depending on the nature and consequences of the violation. Particular attention is given to liability for conducting activities without a licence, violating certification procedures, and using uncertified CPI tools, which directly impacts the guarantees of confidentiality, integrity, and availability of critically important information in IT systems. The competence of state authorities responsible for supervision in this area is regulated, particularly the State Service of Special Communications and Information Protection of Ukraine, which is authorised not only to impose fines but also to initiate the suspension or termination of operation of tools that do not meet approved requirements. This mechanism ensures both reactive and preventive functions in response to threats associated with the use of vulnerable or illegitimate CPI. The application of criminal liability in cases of unauthorised disclosure or leakage of cryptographic information that constitutes state secrets or is protected within restricted access systems demonstrates the existence of legal instruments focused on protecting critical elements of national security. At the same time, there is a modern need to improve violation detection procedures, particularly through the introduction of digital monitoring mechanisms, post-audit procedures, and risk indicators in the application of CPI.

To ensure effective control, it is advisable to revise interaction practices among state oversight entities performing sanctioning, supervisory, and analytical functions. Specifically, coordination between the State Service of Special Communications and Information Protection of Ukraine, the Security Service of Ukraine, and the National Police of Ukraine should provide for joint responses to violations of cryptographic protection requirements, harmonisation of certification procedures for protective tools, and the rapid exchange of analytical information. Improving the reporting system, introducing transparent decision-making mechanisms, and enhancing the analytical capacity of oversight bodies will serve as an institutional precondition for building trust in the regulator and ensuring the sustainable development of the enforcement environment in the field of cryptographic protection.

Institutional architecture and regulatory powers of the state in the field of cryptographic protection. Within the study of state governance in the field of cryptographic information protection, the analysis of the institutional architecture of the body tasked with implementing the relevant policy becomes crucial. The activities of the State Service of Special Communications and Information Protection of Ukraine, as the central executive authority, are defined by a multi-component structure that includes a functional division of responsibilities among administrative, technical, expert, and supervisory units. This model is aimed at ensuring subject-specific specialisation, consistency in conformity assessment processes, certification, regulatory supervision, and operational response.

The internal distribution of competencies within the State Service of Special Communications and Information Protection of Ukraine is based on the principle of integrated implementation of regulatory and technical tasks. This includes the development of CPI requirements, conducting evaluations, certification, maintaining registers, and coordinating with other cybersecurity bodies. Such an approach avoids

[1] Code of Ukraine on Administrative Offenses. (1984, December). Retrieved from https://zakon.rada.gov.ua/laws/show/80731-10.
[2] Criminal Code of Ukraine. (2001, April). Retrieved from https://zakon.rada.gov.ua/laws/show/2341-14.
[3] Law of Ukraine No. 3475-IV "On the State Service for Special Communications and Information Protection of Ukraine". (2006, February). Retrieved from https://zakon.rada.gov.ua/laws/show/911-2006-п.
[4] Law of Ukraine No. 803-XIV "On Cryptographic Protection of Information". (1999, December). Retrieved from https://zakon.rada.gov.ua/laws/show/803-14.

duplication of functions, ensures hierarchical subordination, and optimises processes of licensing, standardisation, and post-control compliance of cryptographic protection tools.

To visualise the institutional configuration and reflect specialised responsibilities, Table 4 is presented below. It summarises the functional division of responsibilities among the four key structural units of the State Service of Special Communications and Information Protection of Ukraine, which play a decisive role in the organisation and implementation of state policy in the field of cryptographic security. This approach makes it possible to clearly identify the areas of responsibility for each component of the institutional system, providing the basis for further analysis of the effectiveness of the interaction.

Table 4. Functional division of powers between the divisions of the State Service of Special Communications and Information Protection of Ukraine

Unit	Main functions
Administration	General management of the service; strategic planning; coordination of interaction with other bodies
Expert units	Conducting state examination of CPI equipment; preparation of conclusions on compliance; analysis of characteristics
Technical Committee for Standardisation	Development of technical requirements for CPI; adaptation of international standards; maintenance of national compliance profiles
Licensing and Certification Department	Acceptance of applications; organisation of certification procedures; maintenance of registers; monitoring of compliance with conditions

Source: developed by the authors based on Law of Ukraine No. 3475-IV[1]

The analysis of Table 4 allows concluding that there is a structured functional division of responsibilities within the unified system of state governance in the field of cryptographic information protection. The administrative level of the State Service of Special Communications and Information Protection of Ukraine is responsible for strategic planning, managerial coordination, and organisational support in the implementation of CPI policy. Expert departments carry out professional evaluation of cryptographic solutions subject to certification, conduct technical examinations, and formalise conclusions on the compliance of tools with approved technical profiles.

The Technical Standardisation Committee plays a key role in the development of regulatory and technical documents and in the implementation of international approaches, in particular by adapting standards such as ISO/IEC No. 15408-1 "Evaluation criteria for IT security" (2009), ISO/IEC No. 18033-1 "Encryption algorithms" (2021), ISO/IEC No. 19790 "Security requirements for cryptographic modules" (2012), European Telecommunications Standards Institute (2016a; 2016b; 2018), and the European Union Agency for Cybersecurity (2014) to the national regulatory environment. Its activities ensure methodological consistency in certification procedures and unify the criteria for assessing cryptographic security. The Licensing and Certification Department, in turn, is responsible for administering procedures for granting market entities access to provide cryptographic services, verifying compliance with licensing conditions, as well as maintaining certificate renewals and state records.

This division ensures subject-specific specialisation of each unit, which helps to improve the effectiveness of regulatory functions and simplifies communication mechanisms with market participants, licensing authorities, CPI users, and international partners. The internal structure of the State Service of Special Communications and Information Protection of Ukraine corresponds to the typical model of European regulators, which provides for the separation of strategic, technical, expert, and supervisory functions to enhance transparency and reasoned decision-making.

Within the general architecture of cryptographic security governance, coordination among bodies whose powers are distributed across analytics, supervision, law enforcement, and counterintelligence remains crucial. Inter-agency cooperation ensures the functional continuity of processes of prevention, detection, and response to incidents involving violations of the cryptographic information protection regime. To systematise the distribution of responsibilities and cooperation mechanisms among actors in the national cybersecurity system, Table 5 is presented below, summarising the key tasks, coordination formats, and institutional responsibilities of the main bodies involved in CPI policy implementation.

[1] Law of Ukraine No. 3475-IV "On the State Service for Special Communications and Information Protection of Ukraine". (2006, February). Retrieved from https://zakon.rada.gov.ua/laws/show/911-2006-п.

Table 5. Interaction of key bodies in the field of cryptographic protection

Authority	Main tasks in the field of CPI	Forms of coordination	Form of responsibility
State Service of Special Communications and Information Protection of Ukraine	Development of regulatory framework; CPI certification; licensing; technical audit; record keeping	Participation in interdepartmental working groups; coordination with other bodies of regulations and standards	Regulatory responsibility; ensuring technical compliance and certification
National Security and Defence Council of Ukraine	Formation of strategic decisions in the field of cyber defence; coordination of interdepartmental policy	Decision of the National Security and Defence Council of Ukraine; control of the implementation of the cybersecurity strategy through the National Coordination Centre	Political responsibility for the implementation of national decisions in the field of information security
Security Service of Ukraine	Counterintelligence activities in the field of protecting state secrets; investigation of information leaks	Information exchange with the State Service of Special Communications and Information Protection of Ukraine; participation in joint inspections; prompt response to incidents	Criminal procedural liability within the framework of the Criminal Procedure Code of Ukraine[1]; protection of state secret objects
National Police of Ukraine	CPI compliance monitoring	Joint activities with the State Service of Special Communications and Information Protection of Ukraine; coordination of actions in case of violations; prompt reporting of incidents	Criminal and administrative liability within the framework of pre-trial investigation

Source: developed by the authors based on National Security and Defence Council of Ukraine (n.d.), Security Service of Ukraine (n.d.), National Police of Ukraine (n.d.)

The analysis of Table 5 indicates the existence of a coordinated functional distribution among the key bodies involved in the implementation of state policy in the field of cryptographic information protection. The State Service of Special Communications and Information Protection of Ukraine performs the functions of the central regulator, responsible for the development of technical standards, certification of CPI tools, maintenance of state registers, and expert evaluation of technical solutions. Its activities provide the technological and administrative foundation for building a trusted environment in the field of cryptographic security.

The National Security and Defence Council of Ukraine plays a strategic role in setting priorities in the field of cyber protection, in particular through the approval of conceptual documents, coordination of interdepartmental measures, and monitoring the effectiveness of plan implementation within the framework of the National Cybersecurity Coordination Centre. This institutional level creates the framework conditions for uniting the efforts of executive authorities, security forces, and analytical platforms.

The Security Service of Ukraine and the National Police of Ukraine operate within the law enforcement vertical, ensuring compliance with legislation in the field of cryptographic protection. The powers of the Security Service of Ukraine cover the protection of state secrets, the maintenance of counterintelligence regimes in systems with restricted access, and the identification of threats related to the use of CPI tools in critical infrastructure. The National Police focuses on investigating cyber incidents, administrative violations, and the procedural support of crimes related to the unauthorised use of CPI.

This model of interaction is based on a combination of preventive, regulatory, analytical, and law enforcement functions within an integrated institutional system that corresponds to the principles of multi-level information security governance. Ensuring the resilience of cryptographic infrastructure requires continuous coordination among these entities, as well as the updating of rapid response mechanisms, joint audits, and the exchange of technical threat indicators. This approach makes it possible to build an integrated architecture of state governance in the field of CPI, focused on proactive response and maintaining a high level of technological readiness.

Technical standards and cryptographic protection: Modern solutions and certification requirements. Modern technical approaches to cryptographic information protection are based on the use of cryptographic algorithms that must meet criteria of cryptographic robustness, functional compatibility with information systems, and performance in data processing. Over the last decades, classical symmetric and asymmetric cryptographic algorithms – in particular AES, RSA, and ECDSA – have remained dominant. These algorithms provide a sufficient level of protection under the classical computing model; however, the algorithms lose effectiveness in the context of quantum technology development, especially under the influence of Shor's and Grover's algorithms, which can significantly reduce the cryptographic complexity of existing ciphers.

Taking into account these threats from quantum computing, the National Institute of Standards and Technology (2020) launched an open competition to standardise algorithms resistant to quantum attacks. As a result of years of testing, several finalists were

[1] Procedure Code of Ukraine. (2012, April). Retrieved from https://zakon.rada.gov.ua/laws/show/4651-17#Text.

selected, including CRYSTALS-Kyber, CRYSTALS-Dilithium, SABER and others, which form the core of the future PQC standard. These algorithms are based on different mathematical approaches – lattice problems, polynomial homomorphy, code-based structures, and multivariate systems – providing high resistance to attacks using quantum computing machines.

The comparison of classical and post-quantum algorithms is of significant practical importance in the design of CPI technical tools, especially in government and critical information systems. Key characteristics for such analysis include the type of cryptographic scheme, key length, estimated resistance to classical and quantum attacks, as well as the current certification status based on evaluations by the National Institute of Standards and Technology. This approach enables the development of well-grounded recommendations for the gradual implementation of post-quantum algorithms into technical profiles approved by the State Service of Special Communications and Information Protection of Ukraine and helps to avoid the risks associated with outdated cryptographic implementations. To systematise the core characteristics of the most widespread classical crypto-algorithms and prospective post-quantum solutions, Table 6 is provided below. It enables comparative analysis according to basic parameters: type of cryptographic algorithm, key length, resistance level, and certification status. The information presented is relevant for assessing the technical compliance of CPI tools with current and future security standards.

Table 6. Characteristics of classical and post-quantum crypto algorithms

Algorithm name	Type	Key length (bits)	Resistance to attacks	Certification status
RSA-2048	Asymmetric	2048	Medium (vulnerable to quantum attacks)	Standardised (National Institute of Standards and Technology)
ECDSA P-256	Asymmetric	256	Medium (vulnerable to quantum attacks)	Standardised (National Institute of Standards and Technology)
AES-256	Symmetrical	256	High (resistant to Grover attack)	Standardised (National Institute of Standards and Technology)
CRYSTALS-Kyber	Post-quantum (KEM)	768/1024/1536	High (Quantum computing resistant)	Recommended for standardisation (National Institute of Standards and Technology PQC)
Dilithium	Post-quantum (signature)	2048/3072/4096	High (Quantum computing resistant)	Recommended for standardisation (National Institute of Standards and Technology PQC)
SABER	Post-quantum (KEM)	992/1312/1984	High (Quantum computing resistant)	Finalist of the National Institute of Standards and Technology PQC competition

Note: KEM – Key Encapsulation Mechanism
Source: developed by the authors based on ISO/IEC No. 18033-1 (2021), ISO/IEC No. 19790 (2012), European Union Agency for Cybersecurity (2014)

The comparative analysis presented in Table 6 includes digital parameters that allow for a quantitative assessment of the cryptographic strength of algorithms. One of the key criteria is the length of the cryptographic key, which directly correlates with the level of computational complexity for an attacker. In this context, post-quantum algorithms demonstrate significantly higher parameter values. For example, the CRYSTALS-Dilithium algorithm provides for a key length of up to 4096 bits, which exceeds the typical characteristics of classical signature algorithms such as RSA or ECDSA, which use keys of 2048-3072 bits or 256 bits, respectively. The presence of a certification status indicator allows for the evaluation of the level of practical implementation of cryptographic solutions. Classical algorithms have attained international standard status and are components of approved cryptographic profiles, particularly in the recommendations of the National Institute of Standards and Technology (2008; 2019; 2020) and ISO/IEC No. 15408-1 (2009), ISO/IEC No. 18033-1 (2021), ISO/IEC No. 19790 (2012), ISO/IEC No. 7816-4 (2020). Meanwhile, post-quantum algorithms are in the final stages of standardisation, but already demonstrate high potential compliance with protection requirements under quantum computing conditions. This fact provides a foundation for the inclusion in future technical security policies, including at the level of regulations by the State Service of Special Communications and Information Protection of Ukraine, considering the dynamics of post-quantum environment development.

Within the framework of certification and technical regulation of cryptographic protection, the classification of hardware tools implementing key cryptographic functions – such as encryption, authentication, and key generation and storage – is also essential. These hardware-software systems serve as the basic elements of the information security architecture and enable the implementation of cryptographic policy at the level of transactions, state digital services, digital identification systems, and critical infrastructure. The typologisation of CPI tools by functional characteristics, standards

compliance, and application domain allows for the evaluation of the relevance for integration into specialised and multi-segment security solutions.

To systematise the characteristics of such tools, Table 7 is presented below, which summarises the main types of hardware components for cryptographic information protection according to the criteria of device type, implemented functions, compliance standard, and intended use. This approach enables instrumental support for the process of selecting technical solutions in line with the specifics of sectoral tasks and regulatory constraints.

Table 7. CPI hardware classification

Device type	Cryptographic functions	Compliance standard	Scope of use
HSM	Key generation/storage, signing, encryption, authentication	FIPS 140-2 Level 3, ISO/IEC No. 19790 (2012)	State registers, financial transactions, certification centres
Cryptographic token (USB)	Key storage, signature, PIN access	FIPS 140-2 Level 2, ISO/IEC No. 7816-4 (2020)	E-government, digital signature of citizens
Smart card with cryptographic module	Authentication, digital signature, certificate storage	ISO/IEC No. 7816-4 (2020), European Telecommunications Standards Institute TS 102 221	Bank cards, ID documents, access to IT systems
Secure microcontroller (embedded device)	Encryption/decryption, authentication, key protection in IoT systems	ISO/IEC No. 15408 (2009), EAL4+, PSA Certified	Embedded devices, telematics, industrial IoT systems
Virtualised HSM (vHSM)	Key generation, signing, encryption in the cloud environment	ISO/IEC No. 19790 (2012), FIPS 140-3 (in the process of certification)	Cloud services, e-commerce, public cloud platforms

Note: HSM – Hardware Security Module; EAL – Evaluation Assurance Level; PSA – Platform Security Architecture; IoT – Internet of Things; vHSM – Virtualised Hardware Security Module
Source: developed by the authors

Table 7 summarises the types of hardware components that implement the functionality of cryptographic information protection tools, differentiated by architecture, functional purpose, and level of compliance with international security standards. The highest certification reliability indicators are demonstrated by HSMs that meet the requirements of FIPS 140-2 Level 3 (National Institute of Standards and Technology, 2001) or ISO/IEC No. 19790 (2012), and serve as key technological elements in protecting critical cryptographic operations – particularly in certification centres, financial platforms, and national digital signature systems. Meanwhile, smart cards and USB tokens have limited functionality but, due to the ease of implementation and compatibility with popular authentication protocols, are widely used in e-government and registry access systems.

A separate category consists of virtualised HSMs (vHSMs) and secure microcontrollers, which, despite the absence of definitive certification stability, show high potential for use in cloud infrastructure environments, hybrid models of key information storage, and industrial IoT systems. The implementation is becoming increasingly relevant in the context of the gradual migration of national information services to cloud-based architecture, where decentralised cryptographic modules with remote control are needed. This typology makes it possible to conduct a technical-functional assessment of the level of integration of hardware CPI into modern information systems, taking into account certification requirements, compliance with standards, and implementation flexibility.

In the context of further harmonisation of regulatory and technical standards for CPI tools with European and international requirements, it is important to analyse the degree of compliance of national technical norms with the provisions of leading standards and regulations. Of particular importance are the standards of the European Telecommunications Standards Institute (2016a; 2016b; 2018) (in the areas of trust services and electronic signatures), the eIDAS[1] Regulation, and the technical recommendations of the European Union Agency for Cybersecurity (2014) in the fields of electronic identification, communication channel protection, and key management. The alignment of requirements between the State Service of Special Communications and Information Protection of Ukraine and these documents creates a regulatory and legal foundation for the cross-border functioning of public services, including the exchange of certificates, digital signatures, and the verification of identified subjects within the EU.

To illustrate the compliance status of key Ukrainian regulatory documents with the technical requirements of the European Telecommunications Standards Institute (2016a; 2016b; 2018), eIDAS, and the European Union Agency for Cybersecurity (2014), Table 8 is provided below. It reveals the level of harmonisation

[1] Regulation of the European Parliament and of the Council No. 910/2014 "On Electronic Identification and Trust Services for Electronic Transactions in the Internal Market and Repealing Directive 1999/93/EC". (2014, July). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32014R0910.

across specific types of cryptographic services and protocols that are crucial for Ukraine's integration into the European Digital Market and the establishment of a unified trust infrastructure.

Table 8. Compliance of Ukrainian technical requirements for CPI with international standards

Service type/protocol	Ukrainian technical requirements	Relevant international standards	Degree of compliance
Qualified electronic signature	Use of certified CPIs; storage of keys on tokens; DSTU 4145 (2002), DSTU 7624 (2014)	European Telecommunications Standards Institute EN 319 411-2, eIDAS[1] Annex I, XAdES, CAdES	High (adapted to European formats and algorithms)
Key management	Key management policies; security profiles; compliance with a comprehensive information security system	European Union Agency for Cybersecurity Guidelines Cryptographic Solutions, National Institute of Standards and Technology SP 800-57	Medium (not fully unified policies and key rotation)
Communication channel encryption	Mandatory use of TLS with Key Certification Authority certificates; cryptographic algorithms according to the CPI registry	European Telecommunications Standards Institute TS 103 097, ISO/IEC 27033-5 (2016), National Institute of Standards and Technology SP 800-52r2	High (certificate formats and cryptographic algorithms are agreed upon)
Digital identification	Qualified electronic signature tools + identification in the Unified State Register of Legal Entities or ID card; verification of the reliability of the supplier	eIDAS Regulation[2], European Telecommunications Standards Institute EN 319 401	Medium (lack of full interaction with eID and eIDAS Bridge)
Trust services (timestamp, seal)	Qualified service systems with CPI certification, archiving and registration in the National Cybersecurity Coordination Centre registry	European Telecommunications Standards Institute EN 319 421, eIDAS Trusted Services, European Union Agency for Cybersecurity Trust Services Guidelines	High (at the level of procedures and technical regulations)

Source: developed by the authors based on Law of Ukraine No. 3475-IV "On the State Service for Special Communications and Information Protection of Ukraine"[3], National Institute of Standards and Technology (2001; 2008; 2020), European Union Agency for Cybersecurity (2014), European Telecommunications Standards Institute (2016a; 2016b; 2018)

The analysis of Table 8 confirms a high degree of conformity between Ukrainian technical requirements and international regulations in the areas of electronic signatures, cryptographic key management, communication channel encryption, and the provision of trust services. The most harmonised areas appeared to be those related to electronic signatures – Ukraine has already implemented cryptographic algorithms, signature formats, and verification protocols in accordance with the XAdES, CAdES specifications and the requirements of eIDAS Annex I. Similarly, the implementation of timestamp and digital seal procedures is based on the requirements set out by the European Telecommunications Standards Institute (2016b), ensuring technological compatibility with European trust platforms.

At the same time, certain areas – particularly digital identification and cryptographic key management – demonstrate the presence of systemic barriers. The main issues include the absence of an integrated eID gateway for cross-border interaction, as well as an underdeveloped key rotation model in line with the recommendations of the European Union Agency for Cybersecurity (2014) and the National Institute of Standards and Technology (2020). These limitations reduce the efficiency of integration with the European trust space and complicate the technical implementation of unified authentication protocols. Addressing the identified shortcomings requires the implementation of interoperable interfaces, harmonised trust management schemes, and technical regulations at the level of intergovernmental coordination.

Despite these challenges, the overall architecture of national technical requirements in the CPI sector shows a stable trend towards unification with the European cyber environment. The measures taken to implement algorithmic compatibility, adapt cryptographic formats, and align certification procedures are forming the regulatory-technological basis for further development of cross-border cooperation. This, in turn, lays the groundwork for Ukraine's full integration into the European Digital Market and inclusion in the pan-European trust infrastructure in the context of e-governance, financial transactions, and the exchange of legally significant electronic data.

Promising directions for the development of state policy in the field of cryptographic protection in the context of digital transformation. In the process of digital transformation of public administration, the issue of legal and technical harmonisation of national legislation in the field of cryptographic

[1] Regulation of the European Parliament and of the Council No. 910/2014 "On Electronic Identification and Trust Services for Electronic Transactions in the Internal Market and Repealing Directive 1999/93/EC". (2014, July). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32014R0910.
[2] Ibidem, 2014.
[3] Law of Ukraine No. 3475-IV "On the State Service for Special Communications and Information Protection of Ukraine". (2006, February). Retrieved from https://zakon.rada.gov.ua/laws/show/911-2006-п.

information protection with EU regulatory requirements is of particular importance. The eIDAS 2.0 Regulation is the central EU legal act[1] establishing unified rules for electronic identification, qualified electronic signatures, electronic seals, and trust services. This document defines not only the functional requirements for the relevant services but also the technical parameters that cryptographic mechanisms, key information carriers, signature generation protocols, and rules for mutual recognition must comply with.

In the context of implementing the provisions of the Association Agreement between Ukraine and the EU, a priority task is to assess the level of conformity of the national regulatory and technical framework with the requirements set out in eIDAS 2.0, particularly concerning the use of certified CPI tools in state digital services.

Special attention is given to the technical compatibility of national qualified electronic signature tools with European signature formats, the interoperability of timestamp and seal mechanisms, and ensuring the legal validity of cross-border digital identification. To systematise the points of convergence and identify existing discrepancies between the provisions of Ukrainian legislation and the norms of eIDAS 2.0, Table 9 is presented below. It summarises the analysis of four key areas that form the foundation of digital trust infrastructure: qualified electronic signature, electronic identification, timestamp, and electronic seal. The comparison is made based on the parameters of regulatory content, technical requirements for the implementation of respective services, and the overall level of harmonisation between the Ukrainian and European systems of standards.

Table 9. Comparison of eIDAS 2.0 requirements and Ukrainian legislation regarding CPI

Direction	eIDAS 2.0 regulations	Requirements of Ukrainian legislation	Degree of harmonisation
Electronic signature	Definition of qualified electronic signature; mandatory use of certified means; unified signature format (XAdES, PAdES)	Use of qualified electronic signature on tokens; DSTU 4145 (2002), DSTU 7624 (2014); certification by the Key Certification Centre	High (by algorithms and media, but not entirely by formats)
Identification	Unified eID for cross-border use; mandatory recognition of digital identity in all EU member states	Identification via ID card, Unified State Register of Legal Entities or Mobile ID; no mandatory cross-border recognition	Medium (no integration into eIDAS Bridge)
Timestamp	Trusted timestamp providers with mandatory certification; evidence preservation according to the European Telecommunications Standards Institute standard	Provision of timestamp services based on national Key Certification Centres; lack of adaptation to European Telecommunications Standards Institute TS 102 023	Low (local policies not in line with European standards)
Electronic seal	Use of secure seal creation tools; legal identification by automated trust services	Signature of legal entities within the framework of qualified electronic signature; use of standard CPIs ; lack of verification automation	Medium (partial compliance without service infrastructure)

Note: XAdES, PAdES are electronic signature formats according to the European Telecommunications Standards Institute

Source: developed by the authors

The analysis of Table 9 makes it possible to identify both key achievements and critical gaps in the harmonisation of Ukrainian cryptographic information protection tools with European requirements. The most adapted areas are those related to the implementation of qualified electronic signatures, where the conformity of algorithms, carriers, and formats (particularly XAdES and CAdES) with the provisions of eIDAS Annex I is noted. Meanwhile, areas related to timestamps and electronic seals remain partially incompatible with the technical specifications of the European Telecommunications Standards Institute (2016b), especially in aspects of validation procedures, centralised management, and trust identifiers.

The provisions on digital identification and trust services require further harmonisation, particularly through accession to the cross-border eIDAS Bridge mechanism and the implementation of a national certification model in accordance with the framework standards of the European Telecommunications Standards Institute (2016a) and the recommendations of the European Union Agency for Cybersecurity (2014). The underdevelopment of an interoperable infrastructure for mutual recognition of identifiers and certificates limits Ukraine's ability to participate in the single European digital trust space, which reduces the effectiveness of legally significant transactions and document flow.

Thus, the generalised analysis indicates the need to modernise the regulatory and technical base towards full cryptographic compatibility with European standards. This includes not only the adaptation of cryptographic algorithms, formats, and certification policies, but also the revision of audit mechanisms, post-certification monitoring, verification procedures,

[1] Regulation of the European Parliament and of the Council No. 910/2014 "On Electronic Identification and Trust Services for Electronic Transactions in the Internal Market and Repealing Directive 1999/93/EC". (2014, July). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32014R0910.

and supervision over the use of CPI tools. Improvement of these components is a necessary prerequisite for Ukraine's inclusion in the EU digital ecosystem, particularly in the area of trust services, digital identification, and electronic document management.

Within the strategic development of state policy in the field of cryptographic protection, a key task is to enhance the effectiveness of the regulatory activity of the State Service of Special Communications and Information Protection of Ukraine. Given the transformational challenges associated with the implementation of post-quantum cryptographic algorithms, the growing volume of state digital services, and the expansion of critical information infrastructure, the need to functionally expand the regulator's competences is becoming more urgent. The systematic implementation of unified technical models for auditing, certification, post-monitoring, and response should be based on risk-oriented approaches to the evaluation of CPI tools. To present such an approach, Table 10 below summarises the prospective regulatory functions of the State Service of Special Communications and Information Protection of Ukraine under conditions of digital transformation.

Table 10. Prospective regulatory powers of the State Service of Special Communications and Information Protection of Ukraine by functions

Function	Promising powers	Regulatory effect
Audit	Conducting post-certification technical audits of CPI tools in critical information systems; creating a risk-indexed audit registry	Strengthening control over the actual use of certified CPIs; identifying discrepancies in the field
Certification	Expanding the scope of certification to include hybrid cryptographic schemes and post-quantum algorithms; implementing a model of mutual recognition of certificates	Increasing the technological compliance of certified solutions to modern cryptographic challenges
Monitoring	Creation of an automated cryptographic monitoring system to detect uncertified tools and vulnerabilities in real time	Ensuring preventive risk identification and increasing the efficiency of regulatory influence
Reaction	Formation of specialised cryptographic incident response teams; participation in CERT/CSIRT; coordination with the National Police, Security Service of Ukraine, National Cybersecurity Coordination Centre	Reducing threat response time; centralising interaction processes in cryptographic incidents

Note: CERT/CSIRT – Computer Emergency Response Team/Computer Security Incident Response Team
Source: developed by the authors

Table 10 systematises the priority directions for strengthening the regulatory function of the State Service of Special Communications and Information Protection of Ukraine, taking into account the full life cycle of cryptographic tools – from development and certification to operation, control, and incident response. In the audit sphere, the introduction of post-certification inspections is proposed, involving technical audits of CPI under real operating conditions. This would allow for the timely detection of deviations from established parameters, the identification of implementation shortcomings, and the formation of feedback for developers of protective tools.

The certification component should transform towards dynamic responsiveness to technological challenges, primarily by incorporating post-quantum algorithms into national cryptographic profiles and implementing mechanisms for mutual recognition of technical certificates with certification bodies of other jurisdictions. This would ensure the interoperability of protective tools and support Ukraine's participation in European trust schemes, particularly in the context of complying with eIDAS 2.0 requirements.

The functional monitoring block envisages a shift from a predominantly reactive to a preventive model of state control. This refers to the creation of a digital monitoring infrastructure for the circulation of CPI tools, enabling real-time detection of uncertified or vulnerable components. Such systems should be capable of autonomous signature analysis, tracking security policy violations, and supporting decisions to block dangerous objects before formal response procedures are initiated.

In the response section, emphasis shifts to the formation of specialised technical-analytical teams capable of rapid detection and neutralisation of incidents in cooperation with other actors of the national cybersecurity system – the Security Service of Ukraine, the National Coordination Centre for Cybersecurity, the Cyber Police, etc. This approach would foster the creation of an integrated model for managing cryptographic risks that combines institutional control, technological analytics, and adaptive regulation based on risk-oriented scenarios. It creates the preconditions for increasing the resilience of Ukraine's information infrastructure and its capacity to adapt to dynamically evolving threats.

The research findings demonstrated the existence of a formed regulatory and institutional framework for cryptographic information protection in Ukraine. The analysis of legal regulation showed that the key provisions of the Law of Ukraine No. 80/94-VR "On Information Protection in Information and Telecommunications Systems"[1] and Law of Ukraine No. 803-XIV

[1] Law of Ukraine No. 80/94-VR "On Information Protection in Information and Telecommunications Systems". (1994, July). Retrieved from https://zakon.rada.gov.ua/laws/show/80/94-вр.

"On Cryptographic Protection of Information"[1] form a complementary structure aimed at ensuring basic information security requirements. At the same time, it was found that inter-agency coordination, technical unification, and control over the circulation of CPI tools require further improvement at the level of regulations, procedures, and accountability.

The assessment of national regulation compliance with international standards – including ISO/IEC No. 15408-1 (2009), ISO/IEC No. 18033-1 (2021), ISO/IEC No. 19790 (2012), ISO/IEC No. 7816-4 (2013), European Telecommunications Standards Institute (2016a; 2016b; 2018), National Institute of Standards and Technology (2008; 2019; 2020), and eIDAS 2.0 – revealed significant harmonisation in the field of electronic signatures, timestamps, and certification procedures. However, gaps were identified in the implementation of electronic identification, key information protection, and integration into the cross-border trust infrastructure. Relevant tasks remain the creation of a centralised eID gateway, the introduction of key rotation mechanisms, and the adaptation of post-quantum cryptographic algorithms to the national technical profile.

Within the framework of the strategic development of state policy, it is recommended to strengthen the powers of the State Service of Special Communications and Information Protection of Ukraine by expanding its audit, certification, monitoring, and response functions. It is advisable to introduce risk-oriented management models, build a digital infrastructure for monitoring the circulation of CPI tools, and create technical-analytical response teams. Moreover, a key task is the development of a unified oversight architecture for CPI with integrated modules for digital monitoring, automated response, and risk analysis, which will ensure continuous control over compliance with cryptographic protection standards. Such an approach makes it possible to ensure institutional resilience of cryptographic protection, alignment with EU technical requirements, and integration into the European digital market based on mutual recognition of trust services. In this context, it is also appropriate to legally consolidate the model of mutual recognition of cryptographic solution certificates within the EU digital market and develop technical requirements for the use of post-quantum algorithms in public services, taking into account standards for cross-border information protection.

Discussion

The conducted study made it possible to outline the structural parameters of the regulatory model for cryptographic information protection that functioned under conditions of digital transformation of public administration. It was demonstrated that the current regulatory framework provided a basic level of technical control, certification of protective tools, and administrative supervision, but showed insufficient adaptability to challenges associated with the implementation of post-quantum solutions and ensuring cross-border trust. The analysis identified achievements in the standardisation of electronic signatures and timestamps, while also revealing institutional and functional barriers to the implementation of integrated solutions for digital identification, cryptographic key management, and unified interaction protocols with the European trust infrastructure. It was established that an effective response to these challenges required expanding the powers of regulatory actors, modernising audit tools, and implementing digital infrastructure for preventive monitoring.

Within the analysis of functional models for managing cryptographic security, it was found that the adaptability of the regulatory architecture remained a critical condition for implementing a digital protection strategy. This was confirmed in the study by G.S. Lampe (2023), which justified the advisability of introducing circular interaction models as a fundamental approach to ensuring the sustainability and coherence of security processes in digital systems. The study emphasised the necessity of cyclical interaction between technical, analytical, and regulatory subsystems as a prerequisite for the effective functioning of the security ecosystem. The results obtained were consistent with this position, as the identified need for the implementation of post-certification audits, risk-oriented tools, and procedural monitoring confirmed the relevance of a comprehensive approach to regulatory management.

The comparison of the provisions of national technical regulations with international CPI standards demonstrated partial harmonisation, primarily in components of electronic signature and timestamp. In this context, the analytics by P. López (2025), devoted to the National Security Framework as a regulatory model for compliance of cryptosystems with transnational requirements, proved relevant. The author identified key parameters for the certification of digital trust elements – qualified signature creation devices and cryptographic modules, which are regulated by eIDAS and the European Telecommunications Standards Institute standards. Comparative analysis confirmed the advisability of expanding the technical jurisdiction of national supervisory authorities, particularly in the field of compliance assessment of certified tools with the requirements of mutual recognition in the digital market.

Special attention within the study was paid to the issues of organisational interaction between information security actors, which significantly influenced the effectiveness of regulation in the field of cryptographic

[1] Law of Ukraine No. 803-XIV "On Cryptographic Protection of Information". (1999, December). Retrieved from https://zakon.rada.gov.ua/laws/show/803-14.

protection. As evidenced in the work by H. Saragih (2025), the level of protection of state digital platforms directly depended on coordinated activity between regulatory and technical structures. The author emphasised that the fragmentation of managerial decisions and the absence of integrated communication channels led to low efficiency of cybersecurity policies. In this context, the conclusions of the study confirmed the systemic issue of insufficient interdepartmental coordination in managing cryptographic risks, which posed a threat of inconsistency in licensing, certification, and rapid response procedures.

In the context of certification and licensing procedures, the issue of digital maturity of public administration systems was of particular importance, as it determined the ability to integrate trust services into the functionality of digital services. The analysis confirmed that the full inclusion of cryptographic protection tools in the infrastructure of e-government required not only technological compatibility but also the existence of formally regulated supervision mechanisms for the use. Similar points were made by K. Balaji (2025), who highlighted the transformational impact of e-government and e-governance on public administrative functions. The author stressed the need to introduce automated tools for verifying the legitimacy of using digital signatures and certificates in state information systems. The results obtained in the study confirmed this need, pointing to the relevance of formalising control procedures for the implementation of CPI within electronic identification services.

The analysis of general trends in the development of the institutional and technological component of regulation confirmed that cryptographic security is gaining strategic importance in the context of the digital transformation of administrative processes. As shown in the analytical work by J. Millard (2023), the effectiveness of implementing digital reforms directly depended on the presence of a balanced regulatory framework, coordinated interdepartmental cooperation, and long-term planning of security policies. The results of the conducted study corresponded with this position: it was proven that the modernisation of the functional model of the State Service of Special Communications and Information Protection of Ukraine is a critical factor in the formation of a resilient system of state oversight, encompassing certification, monitoring, and audit in the field of CPI.

In the part concerning the analysis of the organisational structure of regulatory policy actors, the research findings aligned with the approaches proposed by P. Ciancarini *et al.* (2024), which described the relationship between digital transformation of public administration and the technology lifecycle. It was emphasised that the effectiveness of implementing cryptographic standards is directly related to the flexibility of regulatory mechanisms for managing technological updates. Within the study, it was established that the current operating model of specialised bodies required adaptation to the dynamics of technological changes, particularly through the creation of post-monitoring audit procedures and the maintenance of lifecycle registers for certified CPI tools.

A separate analytical focus within the study was placed on the standardisation of PQC as a key direction of modern regulatory policy. In this context, a related source was the work of S.A. Shamo (2024), which analysed the challenges of harmonising National Institute of Standards and Technology and ISO standards in the field of PQC and defined strategies for international coordination of certification procedures. The authors emphasised that one of the key issues was the incompatibility between national certification schemes and the technical parameters of new cryptographic algorithms. The findings of the study confirmed the relevance of this issue, as the need was identified for the integration of post-quantum solutions into Ukraine's regulatory environment alongside the updating of technical certification profiles and key management policies.

The analysis of post-quantum challenges confirmed that the effective adaptation of the state's cryptographic infrastructure required not only the updating of the regulatory base but also the modernisation of the technical ecosystem for information protection. As evidenced in the study by A. Joshi *et al.* (2024), the implementation of PQC required a comprehensive approach that included support for national certification centres, updates to key management systems, and integration with cross-border interaction mechanisms. These conclusions aligned with the study's results, which underlined the critical necessity for a technical review of CPI tools aimed at increasing resilience to quantum computing.

In the context of interstate coordination of the migration process towards post-quantum cryptographic standards, a relevant position was presented by L. Chen (2024), where emphasis was placed on the need for technical mapping of interconnections between classical and new cryptographic protocols. The author outlined the strategic role of national certification agencies in ensuring the continuity of information protection during the transition to PQC. Within the study, this position was confirmed by the substantiation of the need to create a digital infrastructure for algorithm verification, functionally linked to the powers of the State Service of Special Communications and Information Protection of Ukraine and oriented towards international standardisation requirements.

The study also demonstrated that the technical integration of new algorithms into national security systems was complicated by both hardware complexity and regulatory inertia. In the work of R. Bavdekar *et al.* (2022), the main barriers to implementing PQC were outlined, including incompatibility between the

technical specifications of algorithms and current certification procedures. The authors stressed the need to revise both infrastructural and regulatory components of the digital security system. The facts established in the study confirmed the relevance of these conclusions, particularly regarding the need to expand the powers of certification bodies to assess the compliance of post-quantum protection tools.

As shown in the work by A. Aydeger *et al.* (2024), ensuring quantum resilience involved not only the phased implementation of new algorithms but also the development of coordinated interaction mechanisms between CPI providers, regulators, and critical infrastructure operators. Within the study, this concept was reflected in the development of a model for regulatory expansion of the functions of the State Service of Special Communications and Information Protection of Ukraine, including components of post-monitoring analysis, auditing of cryptographic processes, and rapid response to incidents involving quantum-resistant tools.

The analysis of legal mechanisms regulating liability for violations of the cryptographic protection regime demonstrated the presence of structural gaps in the division of competences between oversight bodies. This was particularly evident in cases of inter-agency cooperation, where the lack of clear joint response procedures complicated the effective application of sanctions. Similar problems were highlighted in the study by O.V. Cardoso (2022), which emphasised the need to form a unified regulatory architecture for aligning the powers of law enforcement and supervisory bodies in the field of cryptographic protection, which is critically important in the context of digitalisation of governance processes. Within the conducted study, this issue was specified by identifying the need to establish clear powers for the State Service of Special Communications and Information Protection of Ukraine, the Security Service of Ukraine, the Cyber Police, and the National Security and Defence Council of Ukraine regarding control over the use of uncertified CPI tools.

The general summary of the legal aspect of cryptographic security was correlated with the analysis proposed by J. Kazimi & H. Thalwal (2024), which characterised the current challenges of harmonising the regulatory environment with the dynamics of digital transformation. The authors emphasised the need to form flexible legal instruments capable of promptly responding to technological changes and maintaining the relevance of certification procedures. The study results confirmed these conclusions, particularly regarding the need to synchronise Ukrainian regulations with the requirements of mutual recognition under eIDAS and adapt liability models to the specifics of digital services.

The relevance of unifying approaches to cryptographic security found further confirmation in the study by T. Bouraffa & K.-L. Hui (2025), which conducted a systematic review of regulatory frameworks in the field of information and network security. The authors pointed out the presence of fragmentation among sectoral regulators, which hindered the effective implementation of unified technical and legal standards in the field of information protection. Within the framework of this study, the observation was specified through the need to form a centralised model of certification and monitoring, which would ensure the integrity of state policy in the field of CPI.

Against the background of the problems of coordinating certification regimes in different jurisdictions, it was established that the issue of legal harmonisation of cryptographic standards retained critical importance for ensuring cross-border digital compatibility. In the work by B. Firmansyah & R. Bansal (2024), barriers arising in the process of standardising cryptographic solutions in digital environments were considered, in particular due to the risks of regulatory incompatibility. The research results confirmed the identified problem, demonstrating discrepancies between the provisions of eIDAS 2.0, the European Telecommunications Standards Institute EN 319, and current national acts, which limited the prospects for mutual recognition of CPI tools at the EU level.

Within the framework of developing technical standards for digital identification, special attention was paid to the problems of transitional regulation related to the use of distributed ledger technologies. As stated in the study by X. Jia *et al.* (2023), the process of standardising blockchain and distributed ledger technology was accompanied by numerous regulatory conflicts, particularly due to the lack of unified approaches to certification and legal classification of objects. The authors emphasised that without overcoming these contradictions, it is impossible to form a digital trust infrastructure compatible with global regulatory requirements. The results obtained within the framework of the study confirmed the presence of similar challenges in Ukraine, particularly in the field of regulation of timestamp procedures and the use of electronic seals.

The legal aspects of protecting digital assets were considered through the lens of liability for violations of the cryptographic security regime, including the use of uncertified tools or non-compliance with key management requirements. In this context, a generalised analytical basis was provided by the study of N. Shaik *et al.* (2025), which systematised the current regulatory approaches to ensuring legal liability in the event of cyber incidents. The study highlighted issues of legal responsibility for cyber violations, in particular tertiary liability, the duty of proper cybersecurity, employer liability for data leaks, and the specifics of legal regulation of cross-border cyber incidents. Within the conducted research, this position was specified in proposals to strengthen the role of the State Service of Special Communications and Information Protection of Ukraine in terms of monitoring, auditing, and responding to violations in the field of cryptographic protection.

A comprehensive analysis of the research results in relation to scientific approaches covering digital security, cryptographic protocols, and regulatory mechanisms demonstrated the systemic nature of the identified problems. It was substantiated that ensuring compatibility with international standards, modernising certification procedures, implementing post-quantum solutions, and strengthening the institutional functions of regulators are key prerequisites for the sustainable development of the CPI sector. All the mentioned areas were found to be interconnected with digital transformation processes, which determines the practical significance for the formation of next-generation cybersecurity policies.

The generalisation of the results made it possible to identify critically important vectors for improving state policy, among which the leading ones remain the integration of legal and technical tools for managing cryptographic risks, the development of digital identity, the unification of key management procedures, and the provision of proper response to security incidents. The effectiveness of state regulation in the field of CPI largely depends on the integrity of the normative, organisational, and technological architecture, which requires further scientific research to adapt it to transnational requirements, in particular the provisions of eIDAS 2.0, and the implementation of risk-oriented models in the processes of state cryptographic oversight.

Conclusions

As a result of the conducted study, it was established that the regulatory and legal framework in the field of cryptographic information protection in Ukraine formed two main levels of regulatory influence: the general technical level, focused in the Law of Ukraine "On Information Protection in Information and Telecommunication Systems", and the specialised one, defined by the Law of Ukraine "On Cryptographic Information Protection". A comparison of the substantive provisions of these acts allowed for the identification of distinctions in regulatory subject, subjects involved, requirements for technical means, and control mechanisms. In particular, it was determined that the first law was oriented towards owners of information and telecommunication systems, and the second – towards developers and suppliers of CPI, which created prerequisites for a dual responsibility regime. It was generalised in a tabular format that only a part of the provisions of these acts aligned with international standards – for example, certification requirements for CPI means only partially conformed to the structure of ISO/IEC 15408 and eIDAS.

Within the institutional analysis, it was recorded that the State Service of Special Communications and Information Protection of Ukraine performed key functions in certification, expertise, licensing, and supervision, while the division of powers between its structural units (Administration, technical committees, expert groups, licensing departments) was clearly outlined by functional criteria. The corresponding table systematised that the administration was responsible for coordination, technical committees for standardisation, and expert groups for technical implementation. It was separately established that, in the sphere of interdepartmental interaction with the Security Service of Ukraine, the National Security and Defence Council of Ukraine, and the National Police, there was partial fragmentation of functions – for instance, the control over electronic signatures and digital marks was implemented simultaneously by several entities without a formalised division of responsibility. In the interaction table, it was revealed that coordination procedures were defined in only 3 out of 8 areas of competence.

The technical section of the study showed that the existing means of cryptographic protection included classical algorithms (AES, RSA, ECDSA) and new post-quantum solutions (Dilithium, Kyber, SABER), which differed in key length, level of resistance, and certification status. Table 6 presented that the key length in post-quantum algorithms on average exceeded 3000 bits, which is 2-3 times more than the classical ones. It was also determined that CPI hardware means were divided into HSMs, tokens, smart cards, and virtualised modules, each of which had a specific area of application – for instance, HSMs conformed to FIPS 140-2 Level 3 and were used in state registers. In the comparative table of technical standards, it was shown that Ukrainian requirements partially aligned with European Telecommunications Standards Institute EN 319, eIDAS Annex I and recommendations of the European Union Agency for Cybersecurity, particularly in signature formats (XAdES, CAdES) and cryptographic management. However, in the areas of timestamp, seal, and digital identification, there was incomplete conformity, requiring an update of regulations and interfaces.

The limitations of the conducted study included the lack of full access to technical regulations of all categories of certified CPI means, limited transparency of departmental security standards, and the absence of aggregated public data on violations of the cryptographic regime. This partially complicated the quantitative representation of the compliance level of electronic identification systems with eIDAS 2.0 requirements and the assessment of supervisory procedure effectiveness. In further studies, it would be advisable to focus on analysing the lifecycle of cryptographic means in information-critical systems, forming digital registers of certified algorithms, and creating mechanisms for post-certification auditing.

Acknowledgements

None.

Funding

None.

Conflict of Interest

None.

References

[1] Aydeger, A., Zeydan, E., Yadav, A.K., Hemachandra, K.T., & Liyanage, M. (2024). Towards a quantum-resilient future: Strategies for transitioning to post-quantum cryptography. In *Proceedings of the 15th international conference on network of the future* (pp. 195-203). Castelldefels: IEEE. doi: 10.1109/NoF62948.2024.10741441.

[2] Balaji, K. (2025). E-government and E-governance: Driving digital transformation in public administration. In K. Wongmahesak & J. Ahmad (Eds.), *Public governance practices in the age of AI* (pp. 23-44). London: IGI Global. doi: 10.4018/979-8-3693-9286-7.ch002.

[3] Bavdekar, R., Chopde, E.J., Bhatia, A., Tiwari, K., & Daniel, S.J. (2022). Post quantum cryptography: Techniques, challenges, standardisation, and directions for future research. *arXiv*. doi: 10.48550/arXiv.2202.02826.

[4] Bommareddy, S., Khan, J.A., & Anand, R. (2022). A review on healthcare data privacy and security. In P. Singh, O. Kaiwartya, N. Sindhwani, V. Jain & R. Anand (Eds.), *Networking technologies in smart healthcare: Innovations and analytical approaches* (pp. 165-187). Boca Raton: CRC Press. doi: 10.1201/9781003239888.

[5] Bouraffa, T., & Hui, K.-L. (2025). Regulating information and network security: Review and challenges. *ACM Computing Surveys*, 57(5), article number 126. doi: 10.1145/3711124.

[6] Cardoso, O.V. (2022). Cryptography and law: The case of Brazil. *Digital Law Journal*, 3(3), 8-19. doi: 10.38044/2686-9136-2022-3-3-8-19.

[7] Chen, J. (2020). Regulation and deregulation: Understanding the evolution of the Chinese cryptography legal regime from the newly released Cryptography Law of China. *International Cybersecurity Law Review*, 1(1), 73-86. doi: 10.1365/s43439-020-00003-6.

[8] Chen, L. (2024). Standardisation of and migration to post-quantum cryptography. In X. Lu & C.J. Mitchell (Eds.), *Security standardisation research* (pp. 3-13). Cham: Springer. doi: 10.1007/978-3-031-87541-0_1.

[9] Ciancarini, P., Giancarlo, R., & Grimaudo, G. (2024). Digital transformation in the public administrations: A guided tour for computer scientists. *IEEE Access*, 12, 22841-22865. doi: 10.1109/ACCESS.2024.3363075.

[10] DSTU 4145-2002 "Information technology. Cryptographic protection of information. Digital signature based on elliptic curves. Formation and verification". (2002). Retrieved from https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=68769.

[11] DSTU 7624:2014 "Information technology. Cryptographic protection of information. Symmetric block transformation algorithm. Correction". (2014). Retrieved from https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=65314.

[12] European Telecommunications Standards Institute. (2016a). *ETSI EN 319 411-2 V2.2.2: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates*. Retrieved from https://www.etsi.org/deliver/etsi_en/319400_319499/31941102/02.02.00_20/en_31941102v020200a.pdf.

[13] European Telecommunications Standards Institute. (2016b). *ETSI EN 319 421 V1.1.1: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers providing signature validation services*. Retrieved from https://cdn.standards.iteh.ai/samples/39366/0766c518ead24fcfb5e9bc4cb7527f9c/ETSI-EN-319-421-V1-1-1-2016-03-.pdf.

[14] European Telecommunications Standards Institute. (2018). *ETSI TS 103 097 V1.3.1: Intelligent Transport Systems (ITS); Security; Security header and certificate formats*. Retrieved from https://www.etsi.org/deliver/etsi_ts/103000_103099/103097/01.03.01_60/ts_103097v010301p.pdf.

[15] European Union Agency for Cybersecurity. (2014). *Securing personal data: ENISA guidelines on cryptographic solutions*. Retrieved from https://surli.cc/kulckx.

[16] Firmansyah, B., & Bansal, R. (2024). Standardisation and regulatory challenges in modern cryptography. In B. Gupta (Ed.), *Metaverse security paradigms* (pp. 145-183). London: IGI Global. doi: 10.4018/979-8-3693-3824-7.ch006.

[17] ISO/IEC 27001:2022 "Information security, cybersecurity and privacy protection – Information security management systems – Requirements". (2022). Retrieved from https://www.iso.org/ru/standard/27001.

[18] ISO/IEC No. 15408-1:2009 "Evaluation criteria for IT security". (2009). Retrieved from https://www.iso.org/standard/50341.html

[19] ISO/IEC No. 18033-1:2021 "Encryption algorithms". (2021). Retrieved from https://www.iso.org/standard/76156.html.

[20] ISO/IEC No. 19790:2012 "Security requirements for cryptographic modules". (2012). Retrieved from https://www.iso.org/standard/52906.html.

[21] ISO/IEC 27033-5:2016 "Information technology. Security methods. Network security. Part 5. Securing communications across networks using virtual private networks (VPNs)". (2016). Retrieved from https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=69130.

[22] ISO/IEC No. 7816-4:2020 "Integrated circuit cards". (2020). Retrieved from https://surl.li/rxclpp.
[23] Jia, X., Xu, J., Han, M., Zhang, Q., Zhang, L., & Chen, X. (2023). International standardisation of blockchain and distributed ledger technology: Overlaps, gaps and challenges. *CMES-Computer Modeling in Engineering & Sciences*, 137(2), 1491-1523. doi: 10.32604/cmes.2023.026357.
[24] Joshi, A., Bhalgat, P., Chavan, P., Chaudhari, T., & Patil, S. (2024). Guarding against quantum threats: A survey of post-quantum cryptography standardisation, techniques, and current implementations. In V.S. Shankar Sriram, A. Glory, G. Li & S.R. Pokhrel (Eds.), *International conference on applications and techniques in information security* (pp. 33-46). Singapore: Springer. doi: 10.1007/978-981-97-9743-1_3.
[25] Kazimi, J., & Thalwal, H. (2024). Legal implications and challenges of cryptography and data security: Current trends and future directions. In *Proceedings of the First international conference on technological innovations and advance computing* (pp. 19-27). Bali: IEEE. doi: 10.1109/TIACOMP64125.2024.00014.
[26] Kokarcha, Y., & Lalueva, A. (2022). Peculiarities of personal data protection in social networks: The impact of martial law. *Proceedings of the III international scientific and theoretical conference "Current issues of science, prospects and challenges"* (pp. 70-74). Sydney: SCIENTA.
[27] Kostiuk, Y.V., Skladanny, P.M., Hulak, G.M., Bebeshko, B.T., Khorolska, K.V., & Rzaeva, S.L. (2025). *Information security systems*. Kyiv: Borys Grinchenko Kyiv Metropolitan University.
[28] Lampe, G.S. (2023). Critical success factors for integrating a circular interaction model for security processes in digital transformation. *Ecoforum Journal*, 12(2).
[29] Limniotis, K. (2021). Cryptography as the means to protect fundamental human rights. *Cryptography*, 5(4), article number 34. doi: 10.3390/cryptography5040034.
[30] López, P. (2025). The national security framework as a cybersecurity reference for information cryptosystems. In C.P. Sempere (Ed.), *Governance and control of data and digital economy in the European Single Market: Legal framework for new digital assets, identities and data spaces* (pp. 125-144). Cham: Springer. doi: 10.1007/978-3-031-74889-9_6.
[31] Millard, J. (2023). *Impact of digital transformation on public governance*. Retrieved from https://s4andalucia.es/wp-content/uploads/2023/10/JRC133975_01.pdf.
[32] National Institute of Standards and Technology. (2001). *FIPS PUB 140-2: Security requirements for cryptographic modules*. Retrieved from https://csrc.nist.gov/publications/detail/fips/140/2/final.
[33] National Institute of Standards and Technology. (2008). *NIST Special Publication 800-115: Technical guide to information security testing and assessment*. Retrieved from https://surl.li/mnnfqg.
[34] National Institute of Standards and Technology. (2019). *NIST Special Publication 800-52 Revision 2: Guidelines for the selection, configuration, and use of transport layer security (TLS) implementations*. Retrieved from https://csrc.nist.gov/publications/detail/sp/800-52/rev-2/final.
[35] National Institute of Standards and Technology. (2020). *NIST Special Publication 800-57 Part 1 Rev. 5: Recommendation for key management*. Retrieved from https://surl.li/uujzun.
[36] National Police of Ukraine. (n.d.). *Annual reports*. Retrieved from https://surl.lt/pjhzkk.
[37] National Security and Defense Council of Ukraine. (n.d.). *Accounting for public information*. Retrieved from https://rnbo.gov.ua/ua/Oblik-publichnoi-informatsii.html.
[38] Riebe, T., Kühn, P., Imperatori, P., & Reuter, C. (2022). US security policy: The dual-use regulation of cryptography and its effects on surveillance. *European Journal for Security Research*, 7(1), 39-65. doi: 10.1007/s41125-022-00080-0.
[39] Saragih, H. (2025). The impact of digital transformation on the performance and security of information systems in government institutions. *Pakistan Journal of Life and Social Sciences*, 23(1), 5333-5344. doi: 10.57239/PJLSS-2025-23.1.00416.
[40] Security Service of Ukraine. (n.d.). *Reports*. Retrieved from https://ssu.gov.ua/zvity.
[41] Shaik, N., Chandana, B.H., Chitralingappa, P., & Sasikala, C. (2025). Protecting in the digital age: A comprehensive examination of cybersecurity and legal implications. In S. Barman, S. Koley & S. Joardar (Eds.), *Next-generation systems and secure computing* (pp. 105-135). London: Scrivener Publishing LLC. doi: 10.1002/9781394228522.ch6.
[42] Shamo, S.A. (2024). *Bridging the quantum divide: A comprehensive analysis of NIST and ISO standards for post-quantum cryptography and strategies for global harmonisation*. Retrieved from https://surl.li/pudanm.
[43] Vargiolu, A. (2022). *Cryptography and privacy issues: An OECD framework for global data protection*. doi: 10.13140/RG.2.2.13868.88969.
[44] Yanamala, A.K., & Suryadevara, S. (2024). Navigating data protection challenges in the era of artificial intelligence: A comprehensive review. *Revista de Inteligencia Artificial en Medicina*, 15(1), 113-146.
[45] Zinchuk, M.V. (2024). *Legal support for the protection of confidential information in Ukraine*. Lutsk: Lesya Ukrainka Volyn National University.

Перспективи державного регулювання криптографічного захисту даних

Марія Турчіна
Кандидат юридичних наук
Національний юридичний університет імені Ярослава Мудрого
61024, вул. Григорія Сковороди, 77 м. Харків, Україна
https://orcid.org/0000-0002-1486-1122

Ігор Руденко
Магістр права
Національний юридичний університет імені Ярослава Мудрого
61024, вул. Григорія Сковороди, 77, м. Харків, Україна
https://orcid.org/0009-0008-3582-3951

Ольга Хорольська
Магістр права
Національний юридичний університет імені Ярослава Мудрого
61024, вул. Григорія Сковороди, 77, м. Харків, Україна
https://orcid.org/0009-0004-9853-2378

Анотація
Актуальність дослідження зумовлена необхідністю правового та технічного переосмислення державного регулювання криптографічного захисту інформації в умовах цифрової трансформації України. Метою статті було виявлення ефективності чинної нормативної, інституційної та технічної моделі регулювання криптографічного захисту даних з урахуванням положень міжнародних стандартів. У роботі застосовувалися методи структурно-функціонального аналізу, системного порівняння правових положень і контент-аналізу технічних вимог. У результаті дослідження було встановлено, що нормативне поле регулювання охоплює два рівні впливу – загальнотехнічний і спеціалізований, однак лише приблизно шістдесят відсотків положень щодо електронного підпису, управління криптографічними ключами та часових міток відповідають міжнародним технічним вимогам. Зафіксовано фрагментарність у визначенні обов'язкових сертифікаційних процедур і відсутність уніфікованих регламентів у галузі цифрової ідентифікації та електронної печатки. У межах міжінституційної взаємодії встановлено, що лише три з восьми функціональних напрямів регламентовані формалізованими механізмами, що ускладнює реагування на інциденти криптографічного характеру. Технічний аналіз підтвердив, що середня довжина ключів у криптографічних алгоритмах, стійких до оброблення квантовими обчислювальними системами, перевищує три тисячі бітів, що у два-три рази перевищує показники традиційних алгоритмів, однак імплементація таких рішень у систему державної сертифікації здійснюється обмежено. Також було встановлено, що лише частина апаратних засобів криптографічного захисту відповідає міжнародним вимогам до рівнів технічної безпеки. Практична значущість результатів дослідження полягає в можливості їх застосування для оновлення регуляторної архітектури, формування технічних регламентів, розроблення процедур державного контролю, а також підтримки органів публічної влади, технічних експертних підрозділів і розробників у процесі реалізації національної стратегії кіберзахисту

Ключові слова:
цифрова ідентифікація; електронний підпис; сертифікація засобів; інформаційна безпека; технічний стандарт; міжвідомча координація; цифрова трансформація

UDC 341.233(4): 342.7(477)
DOI: 10.63341/naia-chasopis/3.2025.45

European integration – driving force behind the development of Ukraine's legal culture and the modernisation of its legal system

Andriy Tsvyetkov*
PhD in Law
Academician F.H. Burchak Scientific and Research Institute of Private Law and Entrepreneurship of the National Academy of Legal Sciences of Ukraine
03150, 11 Kazymyr Malevych Str., Kyiv, Ukraine
https://orcid.org/0000-0002-3239-322X

Abstract
The aim of this study was to analyse the development of Ukraine's legal culture under the influence of the strategic course towards European integration, and its impact on the modernisation of the national legal system. The research employed interdisciplinary and terminological approaches, along with dialectical, hermeneutic, historical-legal, comparative-legal, and systems-functional methods, as well as legal modelling. The study clarified the concepts of "legal system" and "legal culture" and provides their characteristics. Its core was an analysis of the role of European integration – both within the Council of Europe and the European Union – in modernising Ukraine's legal system and reforming its structural elements, particularly legal culture. The paper substantiated the importance of adapting Ukraine's legal system to the legal order of the European Union, which entails not only approximating Ukrainian legislation to the EU acquis communautaire, but also embracing the system of legal values and principles, procedures and practices on which EU law is based, and reorienting towards European standards in legal scholarship and legal education. The study analysed national normative legal acts and acts of the European Union largely related to meeting the legal criterion for EU membership. Overall, the results may be useful for a more thorough examination of the evolution of Ukraine's legal system under the influence of European integration – both within the Council of Europe and the European Union – and for the potential development of a draft Concept for Enhancing the Legal Culture of Ukrainian Society, as well as measures aimed at raising the level of legal culture among civil servants and their awareness of EU law

Keywords:
legal integration; legislative adaptation; values; rule of law; legal consciousness; legal education

Introduction

The relevance of this study is determined by the profound transformations taking place in Ukraine's legal system on its path towards integration with the legal order of the European Union (EU). To ensure coherence between national legislation and European legal standards, and to raise the level of legal culture in Ukraine, a comprehensive process of legal-system modernisation is under way. This process envisages entrenching a

Article's History:
Received: 17.04.2025
Revised: 04.09.2025
Accepted: 29.09.2025

Suggest Citation:
Tsvyetkov, A. (2025). European integration – driving force behind the development of Ukraine's legal culture and the modernisation of its legal system. *Law Journal of the National Academy of Internal Affairs*, 15(3), 45-58. doi: 10.63341/naia-chasopis/3.2025.45.

*Corresponding author

system of universal European values, which necessitates increasing the level of legal consciousness among civil servants and the public at large, as well as forming new foundations of legal culture. This applies above all to young people (aged 14-35), making research into legal culture essential for a deeper understanding of the content and vectors of the evolution of Ukraine's legal system under martial law and European integration. The topic is directly linked to the need to improve Ukraine's legal system in order to accelerate alignment with the EU's legal standards. In the absence of such theorisation, it is perhaps unsurprising that, although several versions of the Strategy for the Development of the Justice System and Constitutional Proceedings up to 2029 were submitted to the President of Ukraine for consideration, the final version of this document, as of mid-2025, remains unapproved.

One avenue for improving the legal system, as noted in the literature, is to raise overall legal culture (LC). T. Herklotz (2023) devotes an overview study – rooted in the tradition of legal realism – to the conceptual issues of legal culture, delineating the boundaries of understandings and perspectives that view legal culture as a social practice embedded within a country's institutional framework. The author distinguishes several types of LC – pragmatic, formalistic, and values-oriented – which differently shape the interpretation and application of legal norms. The core problem explored is how different types of legal culture affect the effectiveness and development of the legal system within its institutional environment. The author finds that legal outcomes depend on which type of LC prevails in society and the extent to which it is institutionalised. Considering this in the Ukrainian context, it is noteworthy that society's legal culture comprises a mix of all types, but, as of 2025, it remains in transition, still reflecting residues of Soviet legal formalism.

Y. Chernykh (2023), in turn, analyses Ukrainian LC, emphasising its restructuring under the influence of decommunisation and European legal integration. The author examines how Ukraine's legal system has developed after breaking with the Soviet legal legacy and during the process of approximating Ukrainian legislation to that of the EU. Y. Chernykh (2023) notes that, despite significant progress in modernising the legal system to align with EU standards and in reforming institutions, challenges persist, notably a shortage of professional judges – an issue growing in importance even as positive law remains the dominant channel for norm creation.

Of particular interest is the work of O. Bandurka *et al*. (2023), which examines the evolution of judicial reform in Ukraine and identifies key problems such as corruption, the need to increase the efficiency of justice, and excessive political influence over the judiciary. The article analyses the outcomes of major legislative reforms implemented after the events of the Euromaidan, highlighting positive results such as improved legislation, reorganisation of judicial institutions, and the implementation of anti-corruption measures. At the same time, the researchers conclude that the reforms have not significantly increased public trust in the judiciary and judges – an important element of legal culture that reflects citizens' confidence in the fairness and effectiveness of Ukraine's legal system. According to the President of the Supreme Court of Ukraine, S. Kravchenko (2025), the public's largely negative attitude towards Ukrainian courts is, regrettably, substantially influenced by media coverage, which tends to focus on doubtful decisions, corruption cases, and high-profile scandals. The study underscores the need to ensure judicial independence from political influence and to secure support from international institutions (the Council of Europe, the EU, the United Nations, USAID, the International Development Law Organization (IDLO), and others). It should be noted that a number of judicial officials oppose involving international experts in reforming the judiciary, arguing that such practice would undermine judicial independence (The participation of international…, 2020).

In the study by Y. Kryvytskyi *et al*. (2024), emphasis is placed on the idea that legal reforms are not merely technical processes but public endeavours requiring broad support and a renewal of national values. The authors analyse the course of reform of Ukraine's legal system in the context of EU legal integration and hybrid threats from Russia. The article identifies and explains four sequential stages in adapting national legislation to the EU *acquis communautaire*[1]. To enhance reform in the context of Ukraine's EU integration under hybrid threats, the authors recommend developing a single EU-level strategy to counter such threats. Creating a shared legal space that takes Ukraine's experience into account is also important in light of A. Piszcz & H. Sierocka (2020), who argue that legal culture is not only professional command of the language of law but also the ability to perceive and interpret it in accordance with the cultural context of a specific jurisdiction. This perspective is highly relevant for Ukraine as it advances through stages of European legal integration, since successful implementation of European legal norms requires not only formal translation but also alignment with the culture-legal metaphors and principles characteristic of Ukraine's legal system.

Despite a substantial body of literature on specific aspects of legal culture and the legal system, studies conceptualising their intersectionality remain scarce. In view of this, the hypothesis of the present research

[1] Association Agreement between the European Union and its Member States, of the One Part, and Ukraine, of the Other Part. (2014, May). Retrieved from https://publications.europa.eu/resource/cellar/4589a50c-e6e3-11e3-8cd4-01aa75ed71a1.0006.03/DOC_1

is that European integration intensifies the interdependence between legal culture and the legal system. Accordingly, the article attempts to integrate legal positivist approaches (analysing the legal system as a set of norms and institutions) with legal realist approaches (studying how legal culture affects law enforcement and application).

Materials and Methods

The systematic approach was crucial for the comprehensive study of terminology, as it allowed individual legal terms to be considered as components of a single, interconnected system of legal concepts and terms. Instead of studying terms in isolation, this approach focuses on analysing their interrelationships and interdependencies, not only within the national terminology system, but also in the context of the integration of the Ukrainian legal system into the legal order of the European Union. In interpreting and analysing normative legal acts, a terminological approach was used to enhance understanding of the terms and concepts denoting the phenomena examined in the article, to trace their origins, and to reveal terminological differences between Ukrainian and foreign (primarily Western European) legal traditions. The hermeneutic method helped to disclose and compare the meanings of such terms as legal culture, legal values, legal system, legal order, and legal integration in the legal traditions of Ukraine, European states, and the European Union.

An important place was given to historical-legal and comparative-legal methods, which were used mainly to compare approaches to defining the content of "legal culture" and "legal system" in Ukrainian studies (Chuvakov, 2023) and in international studies (Friedman, 1969; Michaels, 2011). These methods were particularly helpful in comparing approaches to interpreting legal culture and legal consciousness that developed in Ukraine and in Southern European countries (North Macedonia and Croatia) on the eve of their accession to the EU. The study's normative-legal base comprises the provisions of the Constitution of Ukraine[1], Association Agreement between the European Union and its Member States, of the one part, and Ukraine, of the other part[2], Law of Ukraine No. 1629-IV "On the State Programme for Adaptation of Ukrainian Legislation to the Legislation of the European Union"[3], Consolidated versions of the Treaty on European Union[4], and a number of subordinate normative legal acts of Ukraine.

Results

The concept and core features of legal culture. Legal culture is a component of the broader national culture and, at the same time, of the legal system. It entails the formation within society of shared legal values, principles, traditions, procedures, and practices (Mamasharifovna, 2021; Lu & Wang, 2021). The systems of legal values and principles that develop within legal culture must correspond to the level of legal progress achieved by society at each stage of its state–legal development (Lomaka, 2022). The development of legal culture also depends on the state of other forms of culture – economic, political, and informational – which together shape the social order. This interplay among cultural forms determines societal and state attitudes towards law and towards human rights and freedoms (Lukianets-Shakhova *et al*., 2024).

A common view is that legal culture rests on two distinct notions – "law" and "culture" – with the boundary between them being rather blurred. "Law" is a system of generally binding, formally defined rules of conduct, whereas "culture" encompasses shared values and principles and a normative model of behaviour that significantly influences how legal rules are perceived and complied with in society. This interconnection complicates attempts to separate legal norms from the social context in which they operate. R. Michaels (2011) defines legal culture as the cultural context of law that is necessary for law's formation and meaning – covering the place of law in society, the functions of legal sources, and the powers of public authorities and institutions. By contrast, J.Ø. Sunde (2010) understands legal culture as a set of expectations and ideas in the realm of legal relations which are realised through institutional mechanisms (such as judicial procedure, law-enforcement activity, and so forth). Law-making is thus dynamic and dependent on the cultural and social environment that shapes it.

A broader definition is proposed by N. Atamanova & O. Diachenko (2022): legal culture is the aggregate of legal values entrenched in society, arising and developing as the result of socio-legal activity. At the same time, legal culture reflects the social significance of law, expressed in such factors as: the effectiveness and fairness of the legal framework; the state of legality and public order; and the quality of legal consciousness among civil servants and the population as a whole. Legal culture therefore functions as a social regulator,

[1] Constitution of Ukraine. (1996, June). Retrieved from https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text.
[2] Association Agreement between the European Union and its Member States, of the one part, and Ukraine, of the other part. (2014, May). Retrieved from https://publications.europa.eu/resource/cellar/4589a50c-e6e3-11e3-8cd4-01aa75ed71a1.0006.03/DOC_1.
[3] Law of Ukraine No. 1629-IV "On the State Programme for Adaptation of Ukrainian Legislation to the Legislation of the European Union". (2004, March). Retrieved from https://zakon.rada.gov.ua/laws/show/1629-15#Text.
[4] Consolidated Versions of the Treaty on European Union and the Treaty on the Functioning of the European Union Consolidated Version of the Treaty on European Union Consolidated version of the Treaty on the Functioning of the European Union Protocols Annexes to the Treaty on the Functioning of the European Union Declarations Annexed to the Final Act of the Intergovernmental Conference which Adopted the Treaty of Lisbon, Signed on 13 December 2007 Tables of equivalences. (2016, June). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=oj:JOC_2016_202_R_0001.

safeguarding legal order through conscious adherence to legal norms and encouraging citizens to participate in legal processes. It unites legal ideas, knowledge, and practice – from legislation to accepted social behaviour. Most importantly, legal culture directly mirrors the qualitative state of the legal system as a whole: the effectiveness of that system and the degree to which the ideas of democracy, the rule of law, and respect for human and civil rights are embraced at national level depend on society's attitude towards legality and public order.

The content of legal culture is revealed more fully by identifying its distinctive features. Analysis of prior research supports distinguishing the following key characteristics of legal culture:

- it is one of the key elements of the legal system and influences all its components, with the national legal system viewed as the formal embodiment of legal culture;
- knowledge of and respect for law, awareness of its value, understanding of its principles and operating mechanisms, the ability to determine the aims and tasks of legal regulation, and the scope of normative acts;
- the formation in individuals of an orientation towards lawful behaviour and a habit of acting in accordance with legal requirements in everyday life;
- the creation and continuous improvement of the legislative framework and of the mechanisms ensuring its implementation;
- the legislative entrenchment and guarantee of fundamental human and civil rights;
- a high level of legal consciousness among civil servants and society at large – preconditions for individuals' awareness of their rights and freedoms and their readiness to use lawful mechanisms for protection; this implies improvements to the system of legal education;
- ongoing dialogue with other national legal cultures, leading to mutual influence and permeation and enabling legal integration (Petryshyn, 2015).

The level of legal culture in society is uneven and should therefore be differentiated according to its bearers. The broadest by subject is the legal culture of society, commonly linked to a system of legal values, customs, and established views shared by a state's population. This form presupposes a high level of legal awareness among the general public; the legal sophistication and effectiveness of domestic legal and legislative systems; an efficient judiciary; widespread compliance with legal norms; and public trust in state and local authorities. This type of legal culture significantly influences the creation, interpretation, and application of legal norms at the national level (Del Mar & Giudice, 2010).

Y. Kryvytskyi (2023) notes that, within a society's legal culture, there may exist: first, legal subcultures which, while differing from it in certain values, elements, or stances, broadly align with the overarching culture; and, second, a legal counter-culture comprising values, views, theories, orientations, and activities of social groups that openly oppose the prevailing legal culture and are thus in a state of antagonistic contradiction – or even open confrontation – with it (Petryshyn, 2015). Until recently, the legal counter-culture of criminal communities and extremist groups was considered the most dangerous. Under conditions of Russian aggression against Ukraine, however, the counter-culture associated with collaborationism has become the primary threat to the state and its legal system (Rubashchenko *et al.*, 2024).

Legal culture of specific social groups develops within particular communities and professional or social strata. It does not conflict with society's legal culture, though it may display minor specificities. Of particular importance is the legal culture of lawyers (which can itself be differentiated into the cultures of judges, prosecutors, advocates, etc.). It is generally characterised by a theoretical level of legal consciousness and by skills used in law-making, law-application, and legal interpretation. This form is crucial for the development of the legal system as a whole and for its integration into the legal orders of integration associations, notably the European Union (Herklotz, 2023).

The legal culture of the individual is linked to an individual's body of legal knowledge, convictions, attitudes, and behaviour. It presupposes awareness of one's rights and freedoms, as well as of legal duties. Its formation is substantially influenced by legal upbringing, legal education, legal communication, legal information, and personal life experience (Drapushko & Gorinov, 2021). Accordingly, legal culture is of exceptional significance for the development of the national legal system (Čehulić, 2021). It ensures that legislation aligns with social values and moral norms, which in turn positively affects levels of law-abiding behaviour. A developed legal culture is a prerequisite for the successful functioning of a democratic, social, law-governed state and, consequently, for the stable development of society.

The essence and key elements of the legal system. According to Y. Kryvytskyi (2023), the legal system is a fundamental legal concept denoting the totality of interrelated legal phenomena and processes that form society's legal sphere as an integrated whole. It is a complex, multi-level structure consisting of diverse yet related components with shared objectives and the capacity for autonomous development and self-organisation. Y. Kryvytskyi (2023) stresses that the legal system is not static; it is in constant motion, changing and improving over time under the influence of objective social laws and of the challenges facing society at particular stages of state-legal development (for example, the inability of European governments to perform state functions effectively on their own prompted the launch of integration processes culminating in the European Union, founded on an autonomous legal order distinct from both international law and the laws of the Member States).

L.M. Friedman (1969), for his part, defines the legal system as a single, comprehensive structure that is not limited to a set of normative acts. He argues that legal systems comprise: the normative apparatus (laws) created by state actors at all levels; the constellation of state institutions that implement and enforce legal norms in society (judges, lawyers, law-enforcement bodies, etc.); and the mechanisms that connect these institutions to one another in their interaction with society.

Thus, a legal system is a systematised legal structure combining the normative component with the presence of legal institutions and mechanisms that regulate compliance with legal rules. Although each state operates on the basis of an autonomous national legal system, the purpose of such systems is shared across countries: to provide the preconditions for the effective functioning and development of a society grounded in legality, justice, public order, and democracy (Burgin & Mestdagh, 2020).

As a rule, any legal system can function effectively where members of society behave lawfully; conflicts are resolved through legal mechanisms and procedures; offences are prevented; and legal education, upbringing, and scholarship are developed. This does not exclude the possibility or necessity of coercive enforcement when certain actors evade compliance or engage in unlawful behaviour. The complexity of any legal system is indicated by the presence of certain structural levels. Normative level: the body of legal norms that make up the system of law, in which ideal conceptions of justice are objectified and the needs of legal regulation and a society's mentality are reflected. Here, norms are grouped into structured blocks according to legal tradition (for Ukraine, belonging to the Romano-Germanic family, these are institutions, sub-branches, and branches of law). This level also includes the system of legislation – an ordered set of all normative acts in force regulating social relations. Institutional level: the unified system of state-legal institutions (principally supreme state bodies, courts, law-enforcement agencies, and other actors) involved in developing, adopting, interpreting, applying, and ensuring compliance with the law. The configuration of these bodies has national specificities. Ideological level: the complex of legal ideas, concepts, principles, and values underpinning the legal system and defining its specificity, including affiliation with a legal family and the potential for legal integration within inter-state unions. At this level, society's attitude towards law and other elements of the legal system takes shape, as does recognition of the need for reform or modernisation. Functional level: the mechanisms for creating, interpreting, and applying legal norms, as well as the study of violations and the imposition of corresponding sanctions. It is at this level that the effectiveness of the national legal system is determined – its capacity for development and improvement, the maintenance of legality and public order, the protection of rights and freedoms, and the promotion of social progress (Bogachova & Magda, 2021).

The elements of the legal system play a vital role in creating a coherent framework for regulating social relations; through their interaction they make the legal system a flexible and effective instrument of society – typically allowing timely reform in a changing environment. The specificity of a legal system can also be revealed through several basic features. Systemicity (structuredness) is provided primarily by the system of law, whose norms are differentiated by subject-matter and method of regulation into branches and institutions. The structure of the system of law, in turn, serves as a guide for the structure of the system of legislation, although the two do not fully coincide. Legal scholarship and legal education are likewise largely oriented towards the structure of the system of law. Integrity is ensured by the orientation of all structural elements to a single aim: establishing a stable public order and a regime of legality. Dynamism means the legal system is in a process of constant development and self-improvement, interacting with other national legal systems and with international law – and, for European states, with EU law as the legal order of an integration association that Ukraine seeks to join.

Legal culture as an integral component of Ukraine's legal system. Given the ideological dimension of the legal system, legal culture is one of the decisive factors in its development. The significance of legal culture for the proper functioning and evolution of the legal system lies in its capacity to influence the effectiveness of legal norms and the operation of legal institutions. Where a mature legal culture has formed in society – one grounded in a system of values and principles – individuals are more inclined to comply consciously and voluntarily with established norms, and state institutions enjoy greater legitimacy and public trust. Conversely, where legal culture is immature, poor legal awareness, disregard for and distrust of the law, as well as of legal procedures and mechanisms, tend to be more prevalent. This, in turn, erodes the legal system and its elements, with the result that the state's ability to maintain public order and the rule of law is significantly reduced.

An indicator of a society's mature legal culture is its attitude to the principle of the rule of law, enshrined in Article 8 Constitution of Ukraine[1]. The domestic legislator defines this principle as follows: the Constitution has the highest legal force, and therefore other normative legal acts are adopted on its basis and must conform to it; the norms of the Constitution, as the Basic Law, are norms of direct effect, which guarantees individuals the right to apply directly to a court for the protection

[1] Constitution of Ukraine. (1996, June). Retrieved from https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text.

of their constitutional rights and freedoms. In view of Ukraine's integration into the European Union – whose legal order is likewise based on the principle of the supremacy of EU law (Komarova & Lazovski, 2024) – Article 9 of the Constitution of Ukraine acquires particular importance for the national legal culture and for the development of Ukraine's legal system: it stipulates that international treaties in force, consent to the binding nature of which has been given by Parliament, form an integral part of Ukrainian legislation.

Consolidated versions of the Treaty on European Union[1] underlined that it draws inspiration from Europe's cultural, religious, and humanist heritage, from which have developed the universal values of the inviolable and inalienable rights of the person, freedom, democracy, equality, and the rule of law. Ukraine's legal culture – having spent much of the twentieth century within the Soviet Union – differs significantly from the broader European legal heritage; this has complicated its political and legal integration into the EU. Aware of this problem, the Ukrainian authorities initiated a process of decommunisation (freeing public life from the consequences of communist ideology, deconstructing the Soviet mythology of the Second World War and gradually forming in its place a Ukrainian perspective on the war (Honcharenko, 2025)), which proceeded slowly after the collapse of the Union of Soviet Socialist Republics (USSR) and covered primarily the spheres of education and upbringing. The decommunisation process gained spontaneous momentum in 2014 during the Revolution of Dignity (Kasianov, 2024). Its legal foundations developed gradually. Decree of the President of Ukraine No. 432/2009[2], a general dismantling of monuments and memorials dedicated to persons involved in organising and carrying out the Holodomors and political repressions during the Soviet period was initiated. This process was effectively slowed during President V. Yanukovych's tenure. The Revolution of Dignity gave fresh impetus to decommunisation, symbolised by the "Lenin-fall" (leninopad) organised by civil society groups (similar processes once took place in the countries of Eastern Europe) (Grytsenko, 2019). In January 2015, civic initiatives received the approval of the Ministry of Culture, after which the organised dismantling of monuments linked to communist figures began. On 9 April 2015, the Verkhovna Rada adopted a package of four laws – Law of Ukraine No. 314-VIII[3], Law of Ukraine No. 315-VIII[4], Law of Ukraine No. 316-VIII[5], Law of Ukraine No. 317-VIII[6], which spurred the renaming of administrative units.

These processes met with some resistance, primarily among those citizens whose political and legal consciousness had been formed under the influence of Soviet ideology and the glorification of events and figures of the Soviet era. Thus, On Behalf of Ukraine Decision of the Constitutional Court of Ukraine No. v009p710-19 "In the Case on the Constitutional Petition of 46 People's Deputies of Ukraine on the Compliance with the Constitution of Ukraine (Constitutionality) of the Law of Ukraine "On the Condemnation of Communist and National Socialist (Nazi) Totalitarian Regimes in Ukraine and the Prohibition of the Propaganda of Their Symbols"[7] was challenged before the Constitutional Court by a group of MPs. However, on 16 July 2019 the Constitutional Court of Ukraine – demonstrating the maturity of the legal culture of its members – upheld the constitutionality of the Law.

A logical continuation of decommunisation was the course towards "de-Russification", which gained particular urgency and public support after the start of Russian aggression in February 2022. On 21 March 2023, Parliament adopted Law of Ukraine No. 3005-IX "On the Condemnation and Prohibition of the Propaganda of Russian Imperial Policy in Ukraine and the Decolonization of Toponymy"[8], which brought decolonisation processes within a legal framework. By this Law, the Verkhovna Rada recognised Russian imperial policy as criminal and condemned it, prohibited its

[1] Consolidated Versions of the Treaty on European Union and the Treaty on the Functioning of the European Union Consolidated Version of the Treaty on European Union Consolidated Version of the Treaty on the Functioning of the European Union Protocols Annexes to the Treaty on the Functioning of the European Union Declarations Annexed to the Final Act of the Intergovernmental Conference which Adopted the Treaty of Lisbon, Signed on 13 December 2007 Tables of Equivalences. (2016, June). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=oj:JOC_2016_202_R_0001

[2] Decree of the President of Ukraine No. 432/2009 "On Additional Measures to Commemorate the Victims of the Holodomor of 1932-1933 in Ukraine". (2009, June). Retrieved from https://zakon.rada.gov.ua/laws/show/432/2009#Text.

[3] Law of Ukraine No. 314-VIII "On the Legal Status and Commemoration of the Fighters for the Independence of Ukraine in the 20th Century". (2015, April). Retrieved from https://zakon.rada.gov.ua/laws/show/314-19#Text.

[4] Law of Ukraine No. 315-VIII "On the Perpetuation of the Victory over Nazism in the Second World War of 1939-1945". (2015, April). Retrieved from https://zakon.rada.gov.ua/laws/show/315-19#Text.

[5] Law of Ukraine No. 316-VIII "On Access to Archives of Repressive Bodies of the Communist Totalitarian Regime of 1917-1991". (2015, April). Retrieved from https://zakon.rada.gov.ua/laws/show/316-19#Text.

[6] Law of Ukraine No. 317-VIII "On the Condemnation of Communist and National Socialist (Nazi) Totalitarian Regimes in Ukraine and the Prohibition of the Propaganda of their Symbols". (2015, April). Retrieved from https://zakon.rada.gov.ua/laws/show/317-19#Text.

[7] On Behalf of Ukraine Decision of the Constitutional Court of Ukraine No. v009p710-19 "In the Case on the Constitutional Petition of 46 People's Deputies of Ukraine on the Compliance with the Constitution of Ukraine (Constitutionality) of the Law of Ukraine "On the Condemnation of Communist and National Socialist (Nazi) Totalitarian Regimes in Ukraine and the Prohibition of the Propaganda of Their Symbols". (2019, July). Retrieved from https://zakon.rada.gov.ua/laws/show/v009p710-19#Text.

[8] Law of Ukraine No. 3005-IX "On the Condemnation and Prohibition of the Propaganda of Russian Imperial Policy in Ukraine and the Decolonization of Toponymy". (2023, March). Retrieved from https://zakon.rada.gov.ua/laws/show/3005-20#Text.

propaganda and symbols, and defined mechanisms for implementation.

Despite these measures, it must be acknowledged that the Ukrainian authorities were late in adopting them. This conclusion is borne out, above all, by the phenomenon of collaborationism, which manifested itself from 2014 and became widespread after the Russian aggression of 2022. The prevalence of this phenomenon – particularly in the spheres of education, training, and culture – testified to the deformation of the legal consciousness of many Ukrainian citizens, whom the aggressor country regarded as targets of its ideological influence (Dobrobog *et al*., 2023; Chuvakov, 2023; Zhytnyi, 2024). This situation prompted the Verkhovna Rada to refine criminal liability for offences against the foundations of national security involving such conduct (Rubashchenko & Movchan, 2023). Under present conditions and for the post-war period, it is envisaged that educational and outreach activities aimed at instilling the European system of values among Ukrainian citizens will be intensified (Todorov, 2020; Kalinicheva & Bulvinska, 2023; Komarova, 2024). It is evident that criminal-law measures alone cannot remedy the deformation of legal consciousness or the formation of counter-culture in Ukrainian society.

Membership of the Council of Europe as a factor in democratising Ukraine's legal culture and legal system. The history of Ukraine's legal integration into the legal order of a united Europe dates back to its very independence: Resolution of the Supreme Council of the Ukrainian SSR No. 581-XII "On the Implementation of the Declaration on the State Sovereignty of Ukraine in the Sphere of Foreign Relations"[1] instructed the Council of Ministers to direct efforts towards ensuring our state's direct participation in the pan-European process and European structures.

Co-operation with the Council of Europe has been of great importance for the development of the national legal culture and the modernisation of the legal system. It began in 1992 [2], when Ukraine started working with the Council's advisory body on constitutional law – the European Commission for Democracy through Law (the Venice Commission). Ukraine became a full member of the Venice Commission in December 1996 after the entry into force of Law of Ukraine No. 547/96-vr "On Ukraine's Accession to the Partial Agreement on the European Commission "For Democracy through Law"[3]. The Commission's work is crucial for post-socialist countries seeking to align their legislative and law-enforcement practices with European standards in democracy, human rights, and the rule of law. Focusing its interpretive legal activity on three areas (democratic institutions and fundamental rights; constitutional justice; elections, referendums, and political parties), the Venice Commission exerts both direct and indirect influence on the development of Ukraine's legal system and legal culture (its opinions have been taken into account by the European Court of Human Rights in cases against Ukraine). As noted on the official website of the Council of Europe Office in Ukraine, the Commission's opinions and other documents have repeatedly been cited not only in Ukrainian legal scholarship but have also served as a theoretical basis for addressing current problems in legislative work, and are used as persuasive arguments when forming the legal positions of the Constitutional Court and other judicial bodies. Overall, the Commission's assessments of constitutional and legislative acts are perceived as important indicators of whether Ukraine's legal system is developing and functioning in accordance with European standards and values (Council of Europe Office in Ukraine, n.d.).

Ukraine acceded to the Council of Europe in November 1995 pursuant to Law of Ukraine No. 398/95-VR "On Ukraine's Accession to the Statute of the Council of Europe"[4] Accession entailed commitments to implement seventy measures aimed at completing the reform of the judicial and penitentiary systems; combating corruption and money-laundering; creating conditions for the enforcement of European Court of Human Rights judgments; and ensuring Ukraine's participation in Council of Europe treaties, among others. The first major results in fulfilling these commitments included adoption of the Constitution of Ukraine[5] and of basic constitutional laws; new editions of civil, criminal, civil-procedure, and criminal-procedure legislation; Law of Ukraine No. 5076-VI "On the Bar and Legal Practice"[6], and a revision of the role and functions of the Prosecutor General's Office (State Tax Service of Ukraine, n.d.). Monitoring and oversight of the implementation of Ukraine's obligations began immediately through the State Interdepartmental Commission for Implementing the Norms and Standards of the Council of Europe in Ukrainian Legislation, established by Order of the President of Ukraine No. 48-96-rp "On the Establishment of the State Interdepartmental Commission on the

[1] Resolution of the Supreme Council of the Ukrainian SSR No. 581-XII "On the Implementation of the Declaration on the State Sovereignty of Ukraine in the Sphere of Foreign Relations". (1990, December). Retrieved from https://zakon.rada.gov.ua/laws/show/581-12#Text.
[2] Committee of Ministers Resolution No. (92)29 "On Ukraine". (1992, September). Retrieved from https://search.coe.int/cm#{%22CoEIdentifier%22:[%2209000016804f7beb%22],%22sort%22:[%22CoEValidationDate%20Descending%22]} .
[3] Law of Ukraine No. 547/96-vr "On Ukraine's Accession to the Partial Agreement on the European Commission "For Democracy through Law". (1996, November). Retrieved from https://zakon.rada.gov.ua/laws/show/547/96-%D0%92%D0%A0#Text.
[4] Law of Ukraine No. 398/95-VR "On Ukraine's Accession to the Statute of the Council of Europe". (1995, October). Retrieved from https://zakon.rada.gov.ua/laws/show/398/95-вр#Text.
[5] Constitution of Ukraine. (1996, June). Retrieved from https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text.
[6] Law of Ukraine No. 5076-VI "On the Bar and Legal Practice". (2012, July). Retrieved from https://zakon.rada.gov.ua/laws/show/5076-17.

Implementation of the Norms and Standards of the Council of Europe into the Legislation of Ukraine"[1].

Significant for embedding pan-European legal values within legal culture was Ukraine's accession to the European Convention on Human Rights[2]. Ratification of the Convention on 17 July 1997 meant that Ukraine undertook to bring its national legislation into line with the international standards enshrined in the Convention (as is well known, the Council of Europe's human-rights acquis – conventions, agreements, protocols and other legal acts – comprises 173 instruments). Initially, the Verkhovna Rada proceeded rather slowly with amending its human-rights legislation in accordance with these obligations. This prompted a debate in the Parliamentary Assembly on 27 January 1999. The Assembly concluded that, during the transition from totalitarian to democratic statehood, Ukraine had failed to achieve a clear separation between the judicial, legislative and executive branches; progress on legislation to reform the judicial system and the prosecution service was limited; and adherence to the constitutional principle of the rule of law was undermined by non-enforcement of court decisions and rising corruption and crime. These and other shortcomings led the Parliamentary Assembly, Resolution No. 1179 "Honouring of Obligations and Commitments by Ukraine"[3] to state that unless substantial progress in meeting its obligations was achieved by the start of the June 1999 session, the Assembly would be compelled to annul the credentials of the Ukrainian parliamentary delegation until full compliance; and to recommend that the Committee of Ministers begin suspending Ukraine's right of representation pursuant to Article 8 Statute of the Council of Europe[4].

A change in Ukraine's approach to fulfilling its obligations to the Council of Europe occurred after the Verkhovna Rada adopted, on 23 February 2006, Law of Ukraine No. 3477-IV[5]. The preamble emphasised that its adoption was linked to the need to enforce judgments of the European Court of Human Rights in cases against Ukraine; to eliminate the causes of Ukraine's violations of the European Convention on Human Rights[6] and its Protocols; to introduce European human-rights standards into Ukrainian judicial and administrative practice; and to create preconditions for reducing the number of applications lodged with the European Court of Human Rights (ECtHR) against Ukraine. According to the official website of the Permanent Representation of Ukraine to the Council of Europe, as at 31 December 2020 Ukraine ranked third among member states by number of cases (10,400 applications against Ukraine, accounting for 16.8% of the total) pending before the ECtHR (Permanent Representation of Ukraine to the Council of Europe, 2020). In the view of the Ukrainian judge of the ECtHR, M. Hnatovskyi, this situation stems primarily from unresolved structural problems in the functioning of Ukraine's legal system (including conditions of detention in remand centres and penal colonies; the length of criminal and civil proceedings; and insufficient grounds for remand in custody when choosing preventive measures), which, regrettably, have gone unresolved for more than twenty years. Cases against Ukraine are, in fact, repetitive; the ECtHR has long had mechanisms for handling such situations, yet they remain substantively unaddressed domestically. The number of ECtHR cases against Ukraine could, in the judge's opinion, be reduced through the use of the constitutional complaint mechanism, thereby enabling the Constitutional Court to address human-rights issues in Ukraine (The European Court of..., 2023).

Pursuant to Article 15 European Convention on Human Rights[7] a High Contracting Party may, in time of war, take measures derogating from its obligations under the Convention. In 2022, Ukraine availed itself of this right and informed the Secretary General of the Council of Europe that, for the period of martial law, it might introduce emergency measures in accordance with its own legislation (Article 8 Law of Ukraine No. 389-VIII[8]), namely the possibility of restricting constitutional rights and freedoms provided for in Articles 30-34, 38, 39, 41-44 and 53 of the Constitution of Ukraine[9], as well as temporarily restricting rights and legitimate interests provided for in Articles 4(3), 8, 9, 10, 11, 13, 14

[1] Order of the President of Ukraine No. 48-96-rp "On the Establishment of the State Interdepartmental Commission on the Implementation of the Norms and Standards of the Council of Europe into the Legislation of Ukraine". (1996, March). Retrieved from http://zakon2.rada.gov.ua/laws/show/48/96-рп.

[2] European Convention on Human Rights. (1950, November). Retrieved from https://www.echr.coe.int/european-convention-on-human-rights.

[3] Resolution No. 1179 "Honouring of Obligations and Commitments by Ukraine". (1999, January). Retrieved from https://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=16671&lang=en.

[4] Statute of the Council of Europe. (1949, May). Retrieved from https://rm.coe.int/1680306052.

[5] Law of Ukraine No. 3477-IV "On the Execution of Judgments and Application of the Case Law of the European Court of Human Rights". (2006, February). Retrieved from https://zakon.rada.gov.ua/laws/show/en/3477-15.

[6] European Convention on Human Rights. (1950, November). Retrieved from https://www.echr.coe.int/european-convention-on-human-rights.

[7] European Convention on Human Rights. (1950, November). Retrieved from https://www.echr.coe.int/european-convention-on-human-rights.

[8] 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#Text.

[9] Constitution of Ukraine. (1996, June). Retrieved from https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text.

and 16 of the European Convention on Human Rights, Articles 1, 2 and 3 of the Additional Protocol to the Convention, and Article 2 of Protocol No. 4 to the Convention. In 2024, Ukraine reviewed its notification and removed reservations concerning the restriction of a certain set of rights (in particular, references to certain points of Article 8 Law of Ukraine No. 389-VIII[1] were deleted as they did not concern derogation from the Convention, and the list of articles potentially subject to derogation was reduced). It should be stressed that derogation from obligations must not be interpreted as an admission that the state will be unable to guarantee the rights enshrined in the European Convention on Human Rights (see the explanatory notes to Article 15 of the Convention). In notifying a derogation, Ukraine – like other states in similar circumstances – indicated that the measures it might take may involve derogation from its obligations under the Convention (Ministry of Justice of Ukraine, 2024).

Thus, in 2006, Ukraine changed its approach to fulfilling its obligations to the Council of Europe, focusing on implementing the decisions of the European Court of Human Rights, preventing repeated violations of the Convention, and reducing the number of appeals to the Court. Despite these efforts, as of 2020, Ukraine ranked third in terms of the number of cases considered by the ECHR. The main reason for this is deep systemic problems in the country's legal system, which have remained unresolved for over 20 years. The introduction of a constitutional complaint mechanism could help reduce the number of such cases.

Adaptation of Ukrainian legislation to the EU *acquis communautaire* as a condition for Ukraine's successful legal integration into the European Union. In parallel with Ukraine's entry into the Council of Europe, its foreign-policy course towards European integration proceeded through co-operation with the European Union, initiated by the Partnership and Co-operation Agreement between the European Communities and their Member States, and Ukraine (signed in 1994, in force since 1998)[2]. The preamble to the Agreement emphasised the importance of ensuring the rule of law, and Article 59 provided for multifaceted co-operation in the field of education, creating conditions for the mutual penetration of the legal cultures of the European Union and Ukraine – something that positively influenced the development and modernisation of Ukraine's legal culture. The current state of Ukraine's legal integration is defined by the Association Agreement between the European Union and its Member States, of the One Part, and Ukraine, of the Other Part[3]. The Agreement refers to more than 400 EU legislative acts across over 30 different areas to which Ukrainian legislation must be approximated. Such legislation must, in full and as precisely as possible, be aligned with the relevant EU law, taking account of changes therein and incorporating them into the approximated legislation. The state must also ensure the most effective possible application of such legislation, reforming the relevant public authorities where necessary. The leading role in the approximation process rests with the Verkhovna Rada of Ukraine. It should also be noted that Ukrainian courts may apply provisions of the Association Agreement directly where a specific provision contains a clearly formulated obligation whose implementation does not depend on special measures by domestic authorities – that is, where it has "direct effect".

The main strand of Ukraine's legal integration with the European Union has been the adaptation of national legislation to the EU *acquis communautaire*, which has, to some extent, touched virtually every element of the national legal system. A matter of great, though underestimated, importance is the Europeanisation of legal scholarship and legal education, since these elements of the legal system shape the legal consciousness of public officials – particularly future lawyers – and provide doctrinal justification for the directions of Ukraine's state-legal development. In this connection, higher-education institutions and legal research institutes must free themselves from outdated doctrines, theories and concepts, especially those borrowed from Soviet and contemporary Russian legal traditions. Instead, curricula for legal bachelor's, master's and doctoral programmes should include components that help learners to embrace European legal values and to understand EU law, taking account of its complex structure and distinctive system of sources.

It should be noted that a current shortcoming of legal scholarship is a significant imbalance in the training of Doctors of Juridical Science and PhDs in international law, as well as in the representation of international-law specialists among the membership of the National Academy of Legal Sciences of Ukraine. This problem reflects the Soviet disdain for the discipline of international law – a legacy not yet overcome in Ukraine. As of 2025, in the Department of Public Law and International Law of the National Academy of Legal Sciences of

[1] 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#Text.

[2] Partnership and Cooperation Agreement between the European Communities and their Member States, and Ukraine – Protocol on Mutual Assistance Between Authorities in Customs Matters – Final Act – Joint Declarations – Exchange of Letters in Relation to the Establishment of Companies – Declaration of the French Government. (1998, February). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=oj:JOL_1998_049_R_0003_002.

[3] Association Agreement between the European Union and its Member States, of the one Part, and Ukraine, of the Other Part. (2014, May). Retrieved from https://publications.europa.eu/resource/cellar/4589a50c-e6e3-11e3-8cd4-01aa75ed71a1.0006.03/DOC_1.

Ukraine, international law is represented by only one corresponding member, namely M.V. Buromenskyi (National Academy of Legal Sciences of Ukraine, n.d.).

A positive practice introduced in the early 2000s is the involvement by the Ministry of Justice and other central executive bodies of scholars to conduct comprehensive comparative-law studies of the conformity of Ukrainian legislation with the EU *acquis communautaire*. Today, the Ministry's website provides around forty comparative-law studies on various aspects of the conformity of Ukrainian law with the *acquis communautaire* (Central Interregional Directorate of the Ministry of Justice, n.d.).

Updated legal scholarship and education are intended to streamline domestic legal terminology and gradually align it with pan-European legal terminology – without which the integration of Ukrainian law into EU law, uniform understanding and interpretation, and correct application of legal norms would be problematic (Moroz, 2020). An especially acute issue remains the translation into Ukrainian of the vast body of EU law. Although back in 2005 Ministry of Justice of Ukraine Order No. z0921-09 "On Approval of the Procedure for the Translation of Acquis Communautaire Acts into the Ukrainian Language"[1] was adopted, Ukraine is still far from completing this task. The legislative, executive and judicial authorities, as well as law-enforcement bodies, must have a sufficiently high level of awareness and understanding of the basic principles (Dudyk *et al*., 2024), procedures and institutions of the European legal order; accordingly, the professional development of public officials – especially those engaged in law-drafting – on EU law and its application remains a priority driven by the adaptation process.

Discussion

Updating legal culture – one of the most important conditions for modernising Ukraine's legal system – has become particularly urgent and practically significant given the acceleration of the state's course towards integration into the European Union. Ukraine's acquisition of candidate status has provided additional incentives to embed EU legal standards within the domestic legal system and to complete reforms aimed at the consistent acceptance and implementation, at all levels of the legal system, of the principles of the rule of law, the independence and effectiveness of the judiciary, and the guarantee of the full spectrum of human rights and freedoms (Lomaka *et al*., 2025). The success of this process depends directly on the extent to which, above all among public officials, academics and educators, the system of values of a united Europe and the principles, legal procedures and practices of EU law are embraced – thereby aligning Ukraine's legislative, law-enforcement and interpretive activities with pan-European legal standards.

Russian aggression against Ukraine has tested the resilience of its legal system, demonstrating its capacity to adapt to challenges in emergency conditions. Today, the interaction of two factors – European integration and martial law – creates an environment in which the legal culture of society, of particular social groups and of individuals is a crucial driver of the national legal system's development. Thus, J. Bengoetxea (2022) analysed the institutional theory of law, focusing on its three components – norms, order and institutions – in order to create a conceptual basis for comparative studies of legal culture. The author established a link between law, as an institutional normative order, and its ability to adapt to the historical and cultural features of a legal system's functioning. In particular, he stressed the importance of distinguishing branches of law for comparative analysis, which enables the formation of objective indicators for comparing legal cultures. J. Bengoetxea (2022) also examined the role of conflicts and their resolution within the national legal order, and raised questions about fairness and equity in the application of legal norms and mechanisms.

Both this study and J. Bengoetxea's (2022) work examine legal culture through the lens of institutional and normative aspects that are integral to any legal system. The distinctive feature of the present study is its focus on the relationship between Ukraine's legal culture and legal system, especially in the context of European integration. By contrast, J. Bengoetxea's (2022) research is more general and concerns the use of institutional theory to compare different legal cultures. Overall, both studies emphasise the need to employ clear institutional criteria that take account of the complexity and uniqueness of legal systems and cultures.

For her part, M. Králiková (2022) focused on Ukraine's borrowing of EU legal norms, procedures and practices to improve domestic anti-corruption mechanisms. She analysed the effectiveness of applying EU standards and tools in combating bribery, concluding that, despite active EU support, Ukraine's reform of its anti-corruption system faces difficulties linked to resistance within certain social groups. In author's view, despite some progress in tackling corruption, the problem of ensuring the effectiveness of these reforms remains unresolved.

Both M. Králiková's (2022) research and the present study address the obstacles arising from societal resistance to reforms. Such resistance is undoubtedly linked to low levels of legal culture among certain individuals and social groups. This study devotes greater attention to a comprehensive examination of the phenomenon of national legal culture and its development under the

[1] Ministry of Justice of Ukraine Order No. z0921-09 "On Approval of the Procedure for the Translation of Acquis Communautaire Acts into the Ukrainian Language". (2009, September). Retrieved from https://zakon.rada.gov.ua/laws/show/z0921-09#Text.

influence of external geopolitical factors – issues not at the heart of M. Králiková's (2022) work. Importantly, both studies conclude that, while EU-driven reforms have improved institutional systems in Ukraine, significant barriers remain in the form of corruption.

K. Wolczuk (2021) likewise drew attention to European integration as a factor in the development of the legal system, focusing particularly on the post-Euromaidan period (from November 2013 to February 2014). She notes that the Association Agreement between the European Union and its Member States, of the one part, and Ukraine, of the other part [1], was designed not only to ensure economic and political partnership between the Parties, but also to drive deep institutional reforms in Ukraine. K. Wolczuk (2021) emphasises that, after 2014, European integration became an effective instrument for modernising both state and legal institutions in Ukraine, supported by the EU, and that the assistance provided by the EU to Ukraine has been exceptional compared with that given to other candidate countries (e.g., Georgia, Moldova).

Comparing K. Wolczuk's (2021) study and the present one, both highlight the transformational role of European integration in developing Ukraine's legal system and system of governance. However, while K. Wolczuk (2021) focuses primarily on reforms to improve state institutions in meeting the political criteria for EU membership, this study is devoted specifically to legal culture as a driver of Ukraine's legal system. It also pays attention to the transformation of societal legal consciousness and to the role of socio-political factors in that process. In general, both K. Wolczuk (2021) and the authors of this study offer similar assessments of the impact of European integration on state-legal reforms in Ukraine.

F. Besimi (2025) analysed North Macedonia's integration into the EU, focusing on obstacles such as blockades by neighbouring states on the one hand and domestic political instability on the other. He underscored the country's commitment to EU accession despite the difficulties, arguing for membership as a means to meet obligations to the European community and to resolve disputes with neighbouring states, particularly Bulgaria. Overall, the article examined internal and external factors slowing the state's integration process.

Compared with F. Besimi's (2025) study, the present research likewise treats European integration as a factor influencing the development of Ukraine's legal and political systems, but differs in its regional focus and its emphasis on the interdependence of legal culture and the legal system. In general, both studies agree on the importance of EU integration for Ukraine and North Macedonia, though they differ in context and subject matter.

Analysis of the above publications allows us to conclude that there is a consensus among foreign and domestic researchers recognising European integration as a driver of reforms to national legal cultures and systems in EU candidate countries. Legal integration objectively promotes the entrenchment of the value of the rule of law within national legal cultures. The studies reviewed highlight the need to raise the qualitative level of legal culture, especially among public officials and within Ukrainian society as a whole; to foster civic engagement; and to combat manifestations of collaborationism. An important factor in democratising the legal system and all its elements is the reform of legal education and the overcoming of outdated legal traditions that hinder the process of adapting Ukrainian legislation to the EU *acquis communautaire*. Overall, the authors concur that, notwithstanding visible progress driven by European integration, further development of Ukraine's legal system and its elements – including legal culture – continues to be constrained by a range of internal and external challenges.

Conclusions

Legal culture is a driving force in the construction and modernisation of Ukraine's legal system, of which it is a constituent part. The evolution of legal culture is linked to Ukraine's state-legal development, the formation of national identity, and the articulation of a national idea. The trajectory, sophistication and effectiveness of the national legal system thus depend significantly on the qualitative state of legal culture. This article has shown that European integration stimulates not only legislative approximation but also the transformation of legal notions and values that shape legal culture. Legal culture is not merely an object but also a factor in reforming the legal system – particularly at its ideological and functional levels. The effectiveness of law-enforcement and adjudication depends on the legal consciousness of public officials and citizens, directly linking the cultural component with legal practice. The impact of legal culture is evident in judicial reform, where – even with updated legislation – problems of public trust in the courts persist, indicating cultural barriers to the realisation of norms. The legal system cannot be modernised without a profound conceptual re-thinking and embedding of European legal values – that is, the institutionalisation of elements of a new legal culture – confirming an intersectional analytical approach in which legal culture and the legal system are viewed not in isolation but in dynamic interaction.

Since Ukraine chose the strategic course of joining the Council of Europe and the European Union, European integration has acted as a catalyst for the development of legal culture and the reform of the legal

[1] Association Agreement between the European Union and its Member States, of the One Part, and Ukraine, of the Other part. (2014, May). Retrieved from https://publications.europa.eu/resource/cellar/4589a50c-e6e3-11e3-8cd4-01aa75ed71a1.0006.03/DOC_1.

system. Through the adaptation of Ukrainian legislation to the legal standards of the Council of Europe and the EU, significant progress has been achieved in democratising legislative, law-enforcement and interpretive practice and in entrenching the principles of the rule of law. Changes in legal scholarship and legal education are of critical importance in modernising the legal system. This entails rejecting outdated doctrines, theories, concepts, procedures and practices borrowed from the legal traditions of the former Soviet Union and contemporary Russia, and embracing conceptual approaches based on Europe's system of legal values and principles. In this connection, the introduction of a normative ban on the use of Russian-origin information sources in scholarly work should be viewed positively.

A promising avenue for further research is to assess the impact of Russian aggression on the development of Ukraine's legal system and legal culture, and to conduct comparative-law studies of the influence of European integration on reforms to national legal systems in the countries of Eastern and Southern Europe.

Acknowledgements

None.

Funding

The study was not funded.

Conflict of Interest

None.

References

[1] Atamanova, N., & Diachenko, O. (2022). Legal culture and its role in shaping the rule of law of the modern Ukrainian state. *New Ukrainian Law*, 1, 82-87. doi: 10.51989/nul.2022.1.12.

[2] Bandurka, O., Teremetskyi, V., Boiko, V., Zubov, O., & Patlachuk, V. (2023). Current situation of judicial reform in Ukraine: Problems and ways of their solution. *Lex Humana,* 15(4), 55-72.

[3] Bengoetxea, J. (2022). Legal institutions as comparators of legal cultures. *Oñati Socio-Legal Series*, 12(6), 1647-1673. doi: 10.35295/osls.iisl/0000-0000-0000-1361.

[4] Besimi, F. (2025). The path of North Macedonia to the European Union is the only way forward. In A. Stojkov & T. Warin (Eds.), *Western Balkans and the future of Europe*: *Between an enlargement and a commitment fatigue* (pp. 165-178). Cham: Springer. doi: 10.1007/978-3-031-86465-0_8.

[5] Bogachova, L.L., & Magda, E.V. (2021). Legal system of Ukraine: Current state and development trends. *Legal Scientific Electronic Journal*, 4, 28-30. doi: 10.32782/2524-0374/2021-4/4.

[6] Burgin, M., & Mestdagh, K.D.V. (2020). Complexity of legal processes and systems. *Proceedings*, 47(1), article number 17. doi: 10.3390/proceedings2020047017.

[7] Čehulić, M. (2021). Perspectives of legal culture: A systematic literature review. *Journal of Sociology*, 51(2), 257-282. doi: 10.5613/rzs.51.2.4.

[8] Central Interregional Directorate of the Ministry of Justice. (n.d.). *Comparative legal studies*. Retrieved from https://centraljust.gov.ua/ndd/european_integration/law_network/comperative_legal_researches.

[9] Chernykh, Y. (2023). An introduction to Ukrainian legal culture. In S. Koch & M.M. Kjølstad (Eds.), *Handbook on legal cultures: A selection of the world's legal cultures* (pp. 1145-1170). Cham: Springer. doi: 10.1007/978-3-031-27745-0_26.

[10] Chuvakov, O. (2023). Current issues of the improvement of the criminal law protection of the basics of national security of Ukraine. *Odesa National University Herald. Jurisprudence*, 25(2), 36-40. doi: 10.32782/2304-1587/2023-25-2(37)-7.

[11] Council of Europe Office in Ukraine. (n.d.). *Supporting constitutional and legal reforms in Ukraine (Phase 4)*. Retrieved from https://www.coe.int/en/web/kyiv/supporting-constitutional-and-legal-reforms-in-ukraine-phase-4.

[12] Del Mar, M., & Giudice, M. (2010). *Legal theory and the social sciences*. London: Routledge.

[13] Dobrobog, L.M., Bereznyak, V.S., Makashov, A.V., & Tkach, Y.O. (2023). *Collaborative activity as a criminal phenomenon: An analytical review.* Dnipro: Dnipropetrovsk State University of Internal Affairs.

[14] Drapushko, R.G., & Gorinov, P.V. (2021). Current challenges and threats of the legal culture of youth. *Analytical and Comparative Jurisprudence*, 4, 18-22. doi: 10.24144/2788-6018.2021.04.3.

[15] Dudyk, I., Rezvorovych, K., Melnyk, V., Gayevaya, O., & Tumalavičius, V. (2024). Strategies for Ukraine's legal integration into the EU: Learning from the experience of Central and Eastern Europe. *European Political and Law Discourse*, 11(6), 13-21. doi: 10.46340/eppd.2024.11.6.2.

[16] Friedman, L.M. (1969). Legal culture and social development. *Law & Society Review*, 4(1), 29-44. doi: 10.2307/3052760.

[17] Grytsenko, O. (2019). *Decommunization in Ukraine as a Public Policy and as a Cultural Phenomenon.* Kyiv: Institute of Political and Ethno-National Studies named after I.F. Kuras, NAS of Ukraine; Institute of Culturology, NAS of Ukraine.

[18] Herklotz, T. (2023). *Legal cultures*. Oxford: Oxford University Press.

[19] Honcharenko, N. (2025). Transformation of the historical narratives of the Second World War and the decommunisation of memory policy in Ukraine. *Australian Journal of Politics & History*, 71(2), 297-311. doi: 10.1111/ajph.13040.
[20] Kalinicheva, H., & Bulvinska, O. (2023). The role of higher education in the development of United European values during the post-war reconstruction of Ukraine. *Problems of Education*, 2(99), 24-43. doi: 10.52256/2710-3986.2-99.2023.02.
[21] Kasianov, G. (2024). In search of lost time? Decommunization in Ukraine, 2014-2020. *Problems of Post-Communism*, 71(4), 326-340. doi: 10.1080/10758216.2023.2198135.
[22] Komarova, T., & Lazovski, A. (2024). *Case law of the Court of Justice of the EU on the rule of law and its significance for Ukraine*. Kyiv: Pravo-Justice.
[23] Komarova, T.V. (2024). EU values as a guide for Ukrainian legal system. *Problems of Legality*, 2024, 61-82.
[24] Králiková, M. (2022). Importing EU norms: The case of anti-corruption reform in Ukraine. *Journal of European Integration*, 44(2), 245-260. doi: 10.1080/07036337.2021.1872559.
[25] Kravchenko, S. (2025). *Trust in the court: Important considerations based on facts*. Retrieved from https://supreme.court.gov.ua/supreme/pres-centr/zmi/1775192/.
[26] Kryvytskyi, Y. (2023). The influence of legal culture on the effectiveness of the implementation of legal reform. *Law Review of Kyiv University of Law*, 2, 22-27. doi: 10.36695/2219-521.2.2023.03.
[27] Kryvytskyi, Y., Kuznetsova, L., Chekaliuk, V., Maidaniuk, I., & Khriapynskyi, A. (2024). The legal system reform of Ukraine in the context of EU integration and hybrid threats. *Sapienza: International Journal of Interdisciplinary Studies*, 5(4), article number e24077. doi: 10.51798/sijis.v5i4.879.
[28] Lomaka, V. (2022). Legal culture of society in the context of European integration. *Problems of Legality*, 159, 105-128. doi: 10.21564/2414-990X.159.268418.
[29] Lomaka, V., Novikov, Y., Yakoviyk, I., Tragniuk, O., & Sych, M. (2025). The role of European integration in the development of legal awareness of the Ukrainian society. *Portucalense Legal Journal*, 37, 501-523. doi: 10.34625/issn.2183-2705(37)2025.ic-24.
[30] Lu, J., & Wang, J. (2021). Corporate governance, law, culture, environmental performance and CSR disclosure: A global perspective. *Journal of International Financial Markets, Institutions and Money*, 70, article number 101264. doi: 10.1016/j.intfin.2020.101264.
[31] Lukianets-Shakhova, V., Pysarchuk, V., Sokh, K., Malatsai, I., & Tkachenko, V. (2024). Ukraine's journey towards European integration: Successes and future outlook. *Multidisciplinary Reviews*, 8, article number 2024spe077. doi: 10.31893/multirev.2024spe077.
[32] Mamasharifovna, N.F. (2021). Legal culture and the main factors of its formation. *EPRA International Journal of Multidisciplinary Research*, 7(5), 187-190.
[33] Michaels, R. (2011). Legal culture. In H. Basedow, K.J. Hopt & R. Zimmermann (Eds.), *Oxford handbook of European private law*. Oxford: Oxford University Press.
[34] Ministry of Justice of Ukraine. (2024). *Regarding the derogation from obligations under the Convention for the Protection of Human Rights and Fundamental Freedoms*. Retrieved from https://www.kmu.gov.ua/news/shchodo-vidstupu-vid-zoboviazan-za-konventsiieiu-pro-zakhyst-prav-liudyny-i-osnovopolozhnykh-svobod.
[35] Moroz, O. (2020). Problems of adapting Ukrainian legislation to the legislation of the European Union. *Almanac of International Law*, 23, 21-28. doi: 10.32841/ILA.2020.23.03.
[36] National Academy of Legal Sciences of Ukraine. (n.d.). *Corresponding members of the National Academy of Legal Sciences of Ukraine*. Retrieved from https://nals.com.ua/correspondent_members/.
[37] Permanent Representation of Ukraine to the Council of Europe. (2020). *Ukraine and the European Court of Human Rights*. Retrieved from https://coe.mfa.gov.ua/en/partnership/ukraine-and-court.
[38] Petryshyn, O.V. (2015). *Theory of state and law: A guide for preparing for state exams*. Kharkiv: Pravo.
[39] Piszcz, A., & Sierocka, H. (2020). The role of culture in legal languages, legal interpretation and legal translation. *International Journal for the Semiotics of Law*, 33(3), 533-542. doi: 10.1007/s11196-020-09760-3.
[40] Rubashchenko, M., & Movchan, R. (2023). Criminal offenses against state security in the draft of the new Criminal code of Ukraine. *Analytical and Comparative Jurisprudence*, 3, 328-341. doi: 10.24144/2788-6018.2023.03.60.
[41] Rubashchenko, M.A., Yakoviyk, I.V., Shulzhenko, N.V., Zaitsev, O.V., & Kharytono, S.O. (2024). Collaborationism as a historical, social and legal phenomenon. In *Collaborationism in temporarily occupied territories: Problems of legal assessment, guaranteeing human rights and freedoms and reintegration of territories* (pp. 14-190). Kharkiv: Pravo.
[42] State Tax Service of Ukraine. (n.d.). *Fulfillment of Ukraine's obligations to the Council of Europe*. Retrieved from https://tax.gov.ua/diyalnist-/mijnarodne-/arhiv/integratsiya-ukraini-do-es/spivrobitnytstvo-z-radou_es/chlenstvo-v-radi-evropy/vukonania-zoboviazan.

[43] Sunde, J.Ø. (2010). Champagne at the funeral: An introduction to legal culture. In J.Ø. Sunde & K.E. Skodvin (Eds.), *Rendezvous of European legal cultures* (pp. 11-28). Bergen: Fagbokforlaget.
[44] The European Court of Human Rights already has many lawsuits related to the Russian Federation's war in Ukraine – ECHR judge representing Ukraine. (2023). Retrieved from https://court.gov.ua/press/interview/1510856/.
[45] The participation of international experts in the formation of the HQCJ contradicts the independence of the judiciary – Volodymyr Matsko. (2020). Retrieved from https://surl.li/qhrefh.
[46] Todorov, I. (2020). The integrative role of Jean Monnet educational programs in the formation of European community values: Ukrainian content. *International Scientific Bulletin*, 1(21), 139-150. doi: 10.24144/2218-5348.2020.1(21).139-150.
[47] Wolczuk, K. (2021). State building and European integration in Ukraine. In A. Tyushka & T. Schumacher (Eds.), *The European Union and its eastern neighbourhood: Whither "Eastern Partnership"?*. London: Routledge. doi: 10.4324/9781003083634.
[48] Zhytnyi, O. (2024). Immunity of the combatant: Criminal and legal aspects. *Law & Society,* 9, 54-58.

Європейська інтеграція – рушійна сила розвитку правової культури України, модернізації її правової системи

Андрій Цвєтков

Кандидат юридичних наук
Науково-дослідний інститут приватного права і підприємництва
імені академіка Ф.Г. Бурчака Національної академії правових наук України
03150, вул. Казимира Малевича, 11, м. Київ, Україна
https://orcid.org/0000-0002-3239-322X

Анотація
У дослідженні проаналізовано розвиток правової культури України під впливом реалізації стратегічного курсу на європейську інтеграцію, її роль у модернізації національної правової системи. У процесі дослідження застосовано міждисциплінарний і термінологічний підходи, діалектичний, герменевтичний, історико-правовий, порівняльно-правовий, системно-функціональний методи, а також метод правового моделювання. Розкрито зміст понять «правова система» та «правова культура», наведено їхню характеристику. Центральним елементом дослідження став аналіз ролі європейської інтеграції (у межах Ради Європи та Європейського Союзу) у процесі модернізації правової системи України, а також реформування її структурних елементів, зокрема правової культури. Обґрунтовано важливість адаптації правової системи України до правопорядку Європейського Союзу, що передбачає не лише наближення законодавства України до *acquis communautaire* ЄС, а й сприйняття системи правових цінностей і принципів, процедур і практик, на яких ґрунтується право ЄС. Приділено увагу переорієнтації на європейські стандарти правової науки та юридичної освіти. Під час дослідження проаналізовано національні нормативно-правові акти та акти Європейського Союзу, що здебільшого стосуються виконання правового критерію набуття членства в Європейському Союзі. Результати дослідження можуть бути корисні для ґрунтовнішого дослідження еволюції правової системи України під впливом процесів європейської інтеграції у межах Ради Європи і Європейського Союзу, а також для можливого розроблення проєкту Концепції підвищення правової культури українського суспільства, а також заходів, спрямованих на підвищення рівня правової культури державних службовців, їх обізнаності в праві Європейського Союзу

Ключові слова:
правова інтеграція; адаптація законодавства; цінності; верховенство права; правова свідомість; правове виховання

UDC 347.78:355.4
DOI: 10.63341/naia-chasopis/3.2025.59

Intellectual property rights as proactive means of narrative field protection in the context of information warfare and counter-propaganda

Marianna Prysiazhniuk*
Postgraduate Student
University of Bucharest
050663, 90 Panduri Str., Bucharest, Romania
https://orcid.org/0000-0001-6636-7620

Abstract
The Russian-Ukrainian war shows that information and cognitive space are critical dimensions of confrontation and aggression. Strategic narratives, on the other hand, are both a resource and a target for attacks. The study aimed to identify the potential of intellectual property rights as a means of asymmetrical counteraction to information threats through semiotic control, the establishment of authentic meanings, and ensuring the dominance of national narratives in the narrative field. The research was conducted using a methodology based on dogmatic analysis of Ukrainian and international legal acts, systemic-structural and conceptual approaches to narrative typology, as well as elements of interdisciplinary analysis in the field of security and communications and analysis of specific cases. Based on the results of the study, conclusions were proposed regarding the narrative field, which is a multi-level structure of strategic, regional and local narratives, each of which can become the subject of protection in the legal field. This approach can reinforce traditional tools for countering propaganda (fact-checking, strategic communications, sanctions), which cannot ensure political and legal superiority, while the use of intellectual property mechanisms makes it possible to legitimise national counter-narratives and thus prevent their exploitation by the aggressor. National legislation and international mechanisms that create the basis for the legal protection of authentic meanings were analysed. The study concluded that this approach has advantages in terms of democratic standards, as the IP approach does not restrict freedom of speech or focus on censorship, but instead offers forms of protection for the expression of content and the rights of the author. Accordingly, intellectual property instruments can be used as a proactive tool in the context of strengthening information security, as they reinforce the strategic discourse of the state. The proposed approach may, in the future, become the basis for the formation of a policy to protect national narratives and strengthen information sovereignty

Keywords:
strategic discourse; strategic narrative; narrative field; legal protection of meanings; intangible assets; legal legitimation; semiotic control

Article's History:
Received: 11.06.2025
Revised: 05.09.2025
Accepted: 29.09.2025

Suggest Citation:
Prysiazhniuk, M. (2025). Intellectual property rights as proactive means of narrative field protection in the context of information warfare and counter-propaganda. *Law Journal of the National Academy of Internal Affairs*, 15(3), 59-69. doi: 10.63341/naia-chasopis/3.2025.59.

*Corresponding author

Introduction

Russian aggression against Ukraine continues not only in conventional but also in unconventional ways. The information war takes various forms: propaganda campaigns, disinformation campaigns, misinformation and malinformation campaigns, etc., and the search for adequate legal mechanisms to counteract it remains relevant. Accordingly, the information space acts as a continuation of the confrontation and an additional theatre of confrontation, in which meanings and semantic constructions are both resources and means of confrontation. Therefore, the key instrument and semantic form that organises certain words, events, and facts into the desired "architecture" is narrative. In practice, narrative can be embodied in various products of intellectual activity and forms of authorial expression.

The legal dimension of information confrontation, ranging from security aspects to strategies for countering various forms of information intervention, is the subject of research of a range of Ukrainian and foreign scholars. The philosophical and theoretical foundations of information warfare are considered as a space for intellectual confrontation in which "manipulative tactics acquire the status of a dominant means of influence" (Diatlova *et al.*, 2025). V. Petrenko (2025) emphasises the importance of protecting intellectual property rights as an innovative approach integrated into Ukraine's national security system. The author argues that intellectual capital and intellectual security are components of the state's humanitarian security, and that effective protection of intellectual property rights requires the creation of an innovative system for their commercialisation, including in the field of military-industrial cooperation. At the same time, while rightly emphasising that intellectual property instruments can be a means of forming competitive advantages, the researcher does not sufficiently address their semantic significance for strengthening the information and semantic field of the state as an environment in which information warfare is unfolding, which is only partially reflected in proposed definition of the category of "intellectual capital".

S. Mazurenko (2025), analysing trends and copyright infringements in the media space during the war, noted that the legal vacuum that arises as a result of the unlawful use of content potentially creates several long-term threats. These include a loss of trust in information sources and institutions that disseminate information through the media, as well as a distortion of reality and context in the context of irresponsible and unlawful use of information products. At the same time, such conclusions would also be valid for a broader analytical framework that considers not only information content but also other objects of intellectual property rights. This is particularly relevant considering the nature of Russian aggression, which includes signs of systematic expropriation of Ukrainian intellectual capital, its integration into the Russian cultural and legal environment, and the simultaneous destruction of Ukrainian identity. Such practices are confirmed by numerous examples both during the years of full-scale invasion and in a broader historical context, which gives reason to consider them as a deliberate strategy of symbolic and legal expansion.

M. Vedeniapina & M. Pidvysotska (2024) consider the issue of intellectual property rights violations in a broader context. The study emphasised that in wartime, there is an increased range of threats related not only to the spread of disinformation and pirated content, but also to cyberattacks targeting commercially sensitive information that constitutes intellectual property. The study highlighted the problem of the unlawful use of such objects in temporarily occupied territories, where the lack of adequate legal protection creates conditions for systematic abuse and expropriation.

The legal mechanisms for protecting intellectual property in the context of armed conflict were highlighted by K.Yu. Peter (2024), which analyses the potential of intellectual property law instruments during wartime. The study by A. Hasani *et al.* (2024) raised the issue of intellectual rights in the context of the growing use of deepfake technologies and justifies the need for an interdisciplinary approach to ensuring the representativeness of individuals, including legal, ethical and cybernetic components.

A review of published works indicates that despite growing attention to information threats, mechanisms for countering them are primarily considered through the lens of public law, media and communication studies, and political science. However, analysis of this phenomenon in the context of private law, particularly intellectual property law, remains fragmented. The potential of an interdisciplinary approach to the formation of asymmetric strategies for protecting information sovereignty and creating the advantage of truthful strategic narratives in the context of external information threats remains undeveloped, both in the domestic academic environment and in the European scientific tradition. In the context of researching various aspects of security, scholars practically do not consider intellectual property law instruments as a proactive means of legal protection of narratives that are embodied in various forms of expression and may be subject to intellectual property protection. In practice, this means the possibility of strategic commercialisation of meanings through intellectual property rights, ranging from copyright on information content to commercial names with geographical references. At the same time, it should be noted that the practical sphere itself is already generating demand for such a strategic approach. In particular, the head of the Ukrainian National Office of Intellectual Property and Innovation, O. Orliuk (2025), emphasises the need for comprehensive law enforcement. The study highlighted that "proof of registration will

not only help with financial transactions involving the relevant intangible asset, but will also save a lot of resources in case of IP rights violations". This approach directly correlates with the determination of information threats, which, as evidenced by the analysis of academic literature, constitute one of the key dimensions of contemporary challenges to national security.

The study aimed to identify the potential of intellectual property rights as a tool for asymmetric response to information threats, which consists of ensuring semiotic control, as well as to create conditions for the dominance of authentic meanings and the formation of strategic advantages in the narrative field for national narratives embodied in various forms of expression.

Materials and Methods

The study was based on an interdisciplinary approach that combined several conceptual frameworks, including the theory of strategic narratives in international relations by A. Miskimmon *et al.* (2012), which proposes a notion of the key semiotic form of "narrative" not simply as a communicative tool, but as a mechanism for exerting influence; the concept of information warfare as a component of hybrid conflict by G. Pocheptsov (2015); the paradigm of civil law, in particular, the institution of intellectual property law, including developments in the field of intellectual property law in wartime (Peter, 2024), which addressed IP instruments as part of a broader national security system. The classic work by L. Freedman (2006) emphasises the growing role of information and narrative components in modern conflicts. Although the study does not consider the legal mechanisms for protecting narratives, his analysis of the strategic environment confirms the relevance of approach used in the present study. This combination provides an interdisciplinary approach in which intellectual property is understood not only as a mechanism for protecting the results of creative activity, but also as a proactive mechanism for ensuring the superiority of the national strategic narrative in the context of information (cognitive) warfare.

The methodological basis of the study included several levels. At the primary level, using the dogmatic method, the regulatory and legal framework of Ukraine was examined, in particular, the Constitution of Ukraine[1], the Civil Code of Ukraine[2], the Law of Ukraine "On Copyright and Related Rights"[3], the Criminal Code of Ukraine (2001, as amended in 2025)[4]; international treaties, in particular the Paris Convention[5], the Berne Convention[6], the UNESCO Convention for the Safeguarding of the Intangible Cultural Heritage[7], and EU Regulation No. 1151/2012[8], which made it possible to systematise the existing regulatory provisions. At a further level, a systemic-structural analysis was applied to classify narratives at the macro, meso and micro levels (Doichyk & Hanzin, 2025) and to determine their potential as objects of legal protection. The conceptual method revealed the possibility of integrating the theory of strategic narratives with the provisions of intellectual property law and analysing the potential of IP tools as a functional mechanism capable of ensuring semiotic control in the specified conditions.

Results

Strategic advantages in the information space. Countering information interventions, as evidenced by Ukrainian and European experience, mainly takes place in the form of countering disinformation, external information interference and manipulation (FIMI), as well as efforts by various media literacy, fact-checking and other programmes. Despite the significant achievements of each of these approaches to the definition of information confrontation and cognitive warfare, none of them is a predictive tool that provides a stable system of sustainable regulation and long-term counterbalance. In Ukraine, as in most jurisdictions, there are no direct legal mechanisms for holding people accountable for spreading disinformation if it is not related to hate speech, the overthrow of the constitutional order, or direct calls for violence. Moreover, mechanisms for protecting the information environment remain limited: in particular, there is liability for the dissemination of inaccurate (unverified) information and mechanism s for refuting such information at the request of a person about whom information has been disseminated that violates their right to honour, dignity or business reputation. At the same time, any state intervention motivated by information security can easily be classified as censorship. This situation is actively exploited by Russia in the context of its aggression against Ukraine and by

[1] Constitution of Ukraine. (1996, June). Retrieved from https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text.
[2] Civil Code of Ukraine. (2003, January). Retrieved from https://zakon.rada.gov.ua/laws/show/435-15#Text.
[3] Law of Ukraine No. 3792-XII "On Copyright and Related Rights". (1993, December). Retrieved from https://zakon.rada.gov.ua/laws/show/3792-12#Text.
[4] Criminal Code of Ukraine. (2001, April). Retrieved from https://zakon.rada.gov.ua/laws/show/2341-14#Text.
[5] Paris Convention for the Protection of Industrial Property. (1883, March). Retrieved from https://zakon.rada.gov.ua/laws/show/995_123#Text.
[6] Berne Convention for the Protection of Literary and Artistic Works. (1886, September). Retrieved from https://zakon.rada.gov.ua/laws/show/995_051#Text.
[7] UNESCO Convention for the Safeguarding of the Intangible Cultural Heritage. (2003, October). Retrieved from https://zakon.rada.gov.ua/laws/show/995_d69#Text.
[8] Regulation of the European Parliament and of the Council No. 1151/2012 "On Quality Schemes for Agricultural Products and Foodstuffs". (2012, November). Retrieved from https://eur-lex.europa.eu/eli/reg/2012/1151/oj/eng.

other authoritarian regimes, which effectively creates unlimited opportunities to legitimise their presence in the information space of liberal democracies under the guise of "alternative opinion", while engaging in hybrid interference through the systematic exploitation of vulnerabilities in democratic systems.

The idea of creating strategic advantages in the information space is not new and is conceptually reflected in works analysing the information dimension of war as a component of hybrid conflict. In this context, intellectual property law can be seen as a legal tool that helps create a bunch of advantages for intellectual products, especially those that shape and reinforce counter-narratives in the narrative field of information warfare. Thanks to the timely legal protection of relevant objects by means of intellectual property, it becomes impossible for hostile information interventions (propaganda, disinformation, etc.) to parasitise on protected counter-products. This creates the possibility of applying civil liability mechanisms for violations of established rights without resorting to censorship or administrative blocking of information. In other words, a propagandist who illegally uses a protected counter-narrative or its elements may be held liable not for the content of the statements themselves, but for violating the owner's rights to the relevant product, which reduces the risk of accusations of censorship and restriction of freedom of speech and also brings the issue of countering information threats to the civil law level, which in turn complements the state's efforts in this counteraction.

The proposed strategy envisages expanding the scope of intellectual property rights instruments in the context of responding to information threats. Intellectual property is not only an instrument for protecting the results of creative activity, but also as a legal mechanism for identifying, legitimising and protecting strategically relevant products of symbolic production that shape, fill and concretise the strategic discourse of the state in the context of a highly intense information war aimed to delegitimise and culturally erode Ukrainian identity.

Narrative and narrative warfare. The concept of "narration" in different disciplines may have interpretations that differ slightly from one another. However, in the context of military conflict, its meaning takes on a semantic form that can be reproduced in various informational (virtual) and material formats and genres that influence society. As O. Kyrylyuk (2021) notes, "by changing narratives, it is possible to change the system of mentality and build a new system of social action". Narratives as semantic constructions can be differentiated by the scale of the idea they convey. The most complex is the strategic narrative, which is a semantic framework that formulates comprehensive explanations of the state's positions in the international arena, determines the nature of inter-state relations, and influences public opinion within the country regarding these positions: "If the ideas actualised in such narratives are substantial for the existence of the state, they are called strategic narratives" (Kyrylyuk, 2023). Therefore, strategic narratives are the focus of most research in the fields of political science, international relations and communications. At the same time, the process of narrative articulation also occurs at other levels, and as follows from the structure of narrative warfare proposed by O. Doichyk & V. Hanzin (2025), which, according to the authors, occurs at the macro, meso, and micro levels, the typology of narratives can also be reproduced in this hierarchy. Accordingly, there are macro-narratives, meso-narratives, and micro-narratives. According to the logic of confrontation, each of these narratives performs a specific function in the structure of semantic aggression or counter-strategy to counter it.

In particular, the macro-narrative covers ideological or civilisational frameworks, meso-narratives form regional, historical-cultural or socially significant plots, and micro-narratives form localised images, events, personalities or narratives that have a specialised purpose (mission). Thus, the narrative field is formed as a multi-level structure in which each type of narrative performs a separate function in legitimising or delegitimising meanings that compete in the narrative field. The concept of a "narrative field" refers to a space of competing stories and meanings in which there is a struggle to interpret the past and define the values of the present. Defending this space is a component of information sovereignty as an element of national security (Lipkan, 2022). In the context of hybrid warfare analysis, the concept of V.P. Horbulin (2017) of the multidimensionality of modern conflicts emphasises that the information component is one of the key ones, which is consistent with the need for a comprehensive approach to protecting the narrative field, where IP tools act as one of the components of the overall strategy.

Therefore, the "narrative field" is a kind of battlefield where different interpretations, meanings, values, etc., compete. Thus, in an information war, the aggressor seeks a narrative that will convey and legitimise its interpretation, adjusting people's perceptions of a particular event in accordance with its goal, which is generally subjugation.

The most well-known manifestations of narrative confrontation or information warfare are propaganda, disinformation, external information campaigns, and manipulation (FIMI, foreign information manipulation and interference). These forms of narrative warfare are not only conducted in the information environment, where they are most visible, but are also present in cultural, political, scientific, and educational spaces. The penetration of hostile narratives occurs through the creation and dissemination of content in various formats or through the organisation of events that reproduce, broadcast or legitimise certain ideas that constitute the content of the strategic narrative. In the case of Russia,

such narrative aggression is mostly associated with the distortion, appropriation and misrepresentation of the opponent's narratives, in particular the Ukrainian strategic narrative, to influence the general discourse and the information and cultural dominance. In this context, any format, as a means of representing meaning or ideas that has been subject to such interference or exploitation for propaganda purposes, can be considered as an object in respect of which Ukrainian intellectual property rights holders have the potential to exercise legal protection. This approach not only contributes to the protection of the results of intellectual and creative activity but also creates conditions for strengthening the position of the Ukrainian strategic narrative, which is based on a set of authentic intellectual products that are legally protected.

Practices for countering propaganda and disinformation. Many jurisdictions lack a direct mechanism for holding individuals accountable for disinformation as a form of hybrid warfare, with the exception (as in the case of Ukraine) of situations where such information campaigns are not linked to the spread of hate speech, which in most cases is one of the signs of a violation of Article 161 of the Criminal Code of Ukraine[1] (Kryzhanovskyi & Kryzhanovskyi, 2025) or public calls against the constitutional order, in particular, its overthrow or violent change, which are signs of a violation of Article 109 of the Criminal Code of Ukraine[2]. Moreover, any restriction on freedom of expression can easily be interpreted as censorship (Huyvan, 2020), especially when it comes to enemy content in times of war or hybrid conflict. This is actively exploited by aggressor states, which legitimise their presence in the information space of liberal democracies under the guise of "alternative opinion".

Scientific literature noted that Russia skilfully constructs narratives to legitimise its actions, including the legitimisation of a full-scale invasion (Zavershinskaia & Spera, 2024), which is a manifestation of a strategic narrative, given the inter-state context of the semantic meaning of the event. Such "strategic narratives" can take the form of short slogans or clichés, and be simplified and concretised at lower levels. Such narratives, especially strategic ones, formulate ideas that fill the "narrative field", for example: "Russia is the older brother", "Ukraine is a failed state", "The rights of Russian speakers are being violated everywhere", etc. (Romanyshyn *et al*., 2023). However, the implementation of these narratives exceeds the scope of information campaigns or media content. They can be embodied through books, pseudo-historical lectures, public events, as well as through the appropriation and incorporation of Ukrainian meanings as derivatives of Russian culture. This involves the distortion of historical memory, the devaluation of Ukrainian cultural, scientific and political figures, and the belittling of their role in shaping the national strategic discourse, both in terms of cultural heritage and in the context of information resistance.

Protection of intellectual property rights in Ukraine. The Constitution of Ukraine guarantees every citizen the right to the results of their intellectual and creative activity. This is enshrined in Article 54 of the Constitution. The Basic Law also guarantees freedom of literary, artistic, scientific and technical creativity and the protection of intellectual property and copyright, and censorship of creativity is expressly prohibited[3]. According to Articles 14 and 15 of the Law of Ukraine "On Copyright and Related Rights"[4], the rights of the author are divided into personal non-property rights and property rights, and among non-property rights. According to Article 14 of this Law, the author has personal non-property rights, in particular: to demand recognition of his authorship (proper attribution) or to remain anonymous; to choose a pseudonym; to demand the preservation of the integrity of the work and to oppose any distortion or misrepresentation of the work that may harm the honour and reputation of the author. The property rights of the author (or other person who has copyright) include, for example, the exclusive right to use the work, to authorise or prohibit the use of the work by other persons, etc.

The Civil Code of Ukraine (Article 420)[5] defines a wide range of intellectual property rights. These include traditional creative works such as literary and artistic works, computer programs, as well as objects that are directly relevant to the formation of narrative policy: data compilations (databases), folklore expressions, plant varieties, geographical indications, commercial (brand) names, trademarks (signs for goods and services), and trade secrets. Such objects differ in the way they are created, their legal nature and protection mechanisms, which can be used in the selection of a protection tool addressing the nature of the counterproduct itself. Article 5 of the Law of Ukraine "On Copyright and Related Rights"[6] provides an open list of copyright objects, which includes works of science, literature, art, information products, compilations of knowledge, conceptual models, cultural codes, etc. This

[1] Criminal Code of Ukraine. (2001, April). Retrieved from https://zakon.rada.gov.ua/laws/show/2341-14#Text.
[2] Ibidem, 2001.
[3] Constitution of Ukraine. (1996, June). Retrieved from https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text.
[4] Law of Ukraine No. 3792-XII "On Copyright and Related Rights". (1993, December). Retrieved from https://zakon.rada.gov.ua/laws/show/3792-12#Text.
[5] Civil Code of Ukraine. (2003, January). Retrieved from https://zakon.rada.gov.ua/laws/show/435-15#Text.
[6] Law of Ukraine No. 3792-XII "On Copyright and Related Rights". (1993, December). Retrieved from https://zakon.rada.gov.ua/laws/show/3792-12#Text.

list is not complete: the legislator emphasises that life brings new forms of creative activity, and all of them can be protected by law. At the same time, it should be noted that it is the form of expression of the work that is protected, not the ideas or facts themselves. In other words, legal protection extends only to the form of the work and does not extend to any ideas, theories, methods, or concepts, even if they are described or illustrated in the work. Accordingly, a propagandist who parasitises on the structure or terms of a counter-narrative protected in this way is liable not for the content of what is expressed, but for infringement of property rights, which also reduces the risk of accusations of censorship and restriction of freedom of speech.

At the national level, in the event of intellectual property rights infringement, Article 431 of the Civil Code of Ukraine[1] establishes a general rule that any infringement of intellectual property rights (including non-recognition of such rights or encroachment upon them) entails liability as provided for by the Code, other laws or contracts. Article 432 of the Civil Code specifies the types of judicial protection, including: immediate cessation of the infringement and preservation of evidence; suspension of customs clearance of infringing goods; seizure and destruction of infringing products; seizure of means and materials used primarily for infringement; application of a one-time monetary penalty (alternative to compensation for damages); publication of information about the infringement in the media.

Therefore, Russian illegal exploitation of intellectual property, including for propaganda purposes, which is protected by the above-mentioned mechanisms of national legislation, can be considered not only as a basis for response at the level of strategic communications (i.e. at the semantic level), but also as a legal basis for civil law protection of the rights of a specific author or copyright holder of the relevant intellectual or creative product, especially in cases where such a product is of strategic importance for Ukrainian national discourse.

International mechanisms for the protection of intellectual property rights. Ukrainian participation in international treaties on intellectual property rights also creates several prerequisites that could significantly improve its position in the narrative war through the protection of intellectual rights. These include the Paris Convention for the Protection of Industrial Property[2], the Berne Convention for the Protection of Literary and Artistic Works[3], the Universal Copyright Convention[4], the UNESCO Convention for the Safeguarding of the Intangible Cultural Heritage[5,6] and others. All these conventions operate within the framework of the World Intellectual Property Organisation (WIPO), of which both Ukraine and Russia are members. Accordingly, and based on the provisions of the Berne and Universal Conventions, as well as Ukrainian copyright law, texts, analytical materials, speeches, podcasts, videos, visual materials, etc. that embody the author's vision or interpretation of a strategic narrative are subject to protection. Violations, in particular the distortion or appropriation of such materials, give grounds for filing a lawsuit or contacting online platforms to have them removed or blocked. Visual elements of counter-narrative campaigns can be protected as trademarks or industrial designs under the Paris Convention[7]. Furthermore, following Article 10bis of the Paris Convention, in cases where imitated or similar designations are used that may mislead the audience or discredit the original message, legal mechanisms to counter unfair competition apply.

For elements of narrative warfare related to cultural memory and identity, the mechanism of protecting intangible cultural heritage through national registers and subsequent international recognition is also effective. An example of this is UNESCO's inclusion of elements of Ukrainian heritage (such as the culture of borscht preparation) in its relevant list, which provides legal and political grounds for challenging attempts by Russia to appropriate the narrative. Such examples demonstrate that individual or collective intellectual actions can develop into legally significant processes at the international level. In cases of cross-border violations, especially in the digital environment, WIPO alternative dispute resolution tools can be applied, the WIPO Arbitration and Mediation Centre, which offers mechanisms for resolving disputes over domain names (Uniform Domain Name Dispute Resolution Policy, UDRP) and other intellectual property objects in the online environment (WIPO, 2024).

The list of forms of expression of intellectual property objects subject to protection under copyright and related rights, which is determined by Ukrainian legislation, is not exhaustive. Therefore, not only traditional intellectual property objects (works of science, literature

[1] Civil Code of Ukraine. (2003, January). Retrieved from https://zakon.rada.gov.ua/laws/show/435-15#Text.
[2] Paris Convention for the Protection of Industrial Property. (1883, March). Retrieved from https://zakon.rada.gov.ua/laws/show/995_123#Text.
[3] Berne Convention for the Protection of Literary and Artistic Works. (1886, September). Retrieved from https://zakon.rada.gov.ua/laws/show/995_051#Text.
[4] Brussels Convention Relating to the Distribution of Programme-Carrying Signals Transmitted by Satellite. (1974, May). Retrieved from https://zakon.rada.gov.ua/laws/show/995_052#Text.
[5] Universal Copyright Convention. (1952, September). Retrieved from https://zakon.rada.gov.ua/laws/show/995_052#Text.
[6] UNESCO Convention for the Safeguarding of the Intangible Cultural Heritage. (2003, October). Retrieved from https://zakon.rada.gov.ua/laws/show/995_d69#Text.
[7] Paris Convention for the Protection of Industrial Property. (1883, March). Retrieved from https://zakon.rada.gov.ua/laws/show/995_123#Text.

or art, conceptual models, databases, etc.) can be recognised as objects of legal protection, but also modern forms of information products, cultural codes, creative performances, etc. Accordingly, the list of legal instruments for their protection is not exhaustive, which creates room for flexible application of civil and international law in new areas, particularly in the context of information warfare as a component of hybrid threats.

In this regard, the category of unfair competition, which is considered both in national doctrine and in international legal acts (in particular, in Article 10bis of the Paris Convention[1]), is of particular importance. Its main feature remains the misleading of consumers, discrediting or imitation, which in turn completely reproduces the logic of information confrontation, when the opponent (aggressor) aims to undermine trust in authentic sources, substitute content or intercept the opponent's semantic positions (to establish semantic control). Thus, mechanisms to counter unfair competition can be applied as a legal framework for responding to information attacks, which are conducted mainly through distortion, discrediting and parasitising on other people's narratives. Therefore, strategic responses in the civil law sphere should focus not only on achieving the broader goal of creating legal advantages for key elements of the national brand and consolidating the state's strategic narrative in the international information field by restoring the violated rights of a specific entity.

Discussion

The results of the study redefined the role of intellectual property rights in the context of modern information threats and proposed a new conceptual approach to protecting the narrative field. The conclusions of V. Petrenko (2025) regarding intellectual capital as a component of a state's humanitarian security are valid, but the author primarily addressed the commercialisation of IP in the military-industrial sector. In contrast, the proposed study reveals the potential of IP tools directly for the protection of the semiotic space and strategic discourse of the state. The reason for the discrepancy is that V. Petrenko (2025) considers intellectual property as an economic asset, while our approach integrates IP into the context of information warfare, where meanings and narratives expressed in specific results of intellectual activity become objects of protection.

The assertions of S. Mazurenko (2025) regarding the legal vacuum in the media space appear to be valid, especially in terms of focusing exclusively on reactive responses. The proposed approach provides for proactive protection against post facto violations, and IP tools can become a proactive mechanism through the prior establishment of rights to key elements of the national narrative. The study by M. Vedeniapina & M. Pidvysotska (2024), which analyses protective mechanisms against IP violations, can be viewed from another perspective: IP as an offensive tool for actively shaping strategic advantages in the narrative field.

K.Yu. Peter (2024) considers IP in the context of war through the prism of protecting existing rights and restoring them in the post-conflict period. However, the proposed approach involves the proactive use of IP tools during the active phase of the conflict. The reason for the discrepancy lies in different conceptual frameworks. K.Yu. Peter (2024) addressed IP as an object of protection, while the present study considers it as an instrument of active counteraction. The study by O.L. Kyrylyuk (2023) on the discourse of information warfare is fundamental to the research of the semantic mechanisms of conflict. The present study correlates with the conclusion about the possibility of changing the system of mentality through narratives but adds a legal dimension by demonstrating specific IP mechanisms of control over narratives at the level of civil-legal participation of intellectual property rights holders. The concept of G. Pocheptsov (2015; 2019) creates a theoretical framework, but the assertion about the limitations of legal mechanisms seems debatable: the IP approach demonstrates that civil law mechanisms can effectively complement traditional security instruments without resorting to censorship. The study by O.M. Bykov (2023) emphasised the relevance of balancing the protection of the information space with democratic freedoms, which is consistent with the conclusion that the IP approach emphasises the form of expression rather than the content, shifting the issue from the public law sphere to the civil law sphere. O. Spesyvtseva (2023) emphasises the reputational risks of unverified information, but IP tools create legally significant barriers due to the possibility of civil liability. The analysis by P. Horbulin (2017) and Ye. Mahda (2023) confirms that the information component is a key element of hybrid warfare, which justifies the relevance of the IP approach as an additional mechanism of national security.

The theory of strategic narratives by A. Miskimmon *et al.* (2012, 2014) provides a conceptual framework for definition of narratives as instruments of communicative power. The proposed study develops this theory by adding a legal dimension to consolidate strategic narratives through IP instruments, which translates communication strategies into specific legal actions and strengthens the soft power of the state through the legitimisation of narratives.

C. Bjola & J. Pamment (2019) and C. Bjola & R. Zaiotti (2023) highlight technological and diplomatic strategies to counter propaganda. However, IP legal mechanisms can be equally effective in the long term by creating durable legal barriers. A systematic review by

[1] Paris Convention for the Protection of Industrial Property. (1883, March). Retrieved from https://zakon.rada.gov.ua/laws/show/995_123#Text.

J. Pamment *et al.* (2018) catalogues existing approaches to countering information influence but does not consider the potential of intellectual property law, making this study complementary. The concept of "truth decay" by J. Kavanagh & M.D. Rich (2018) describes the systematic decline of the role of facts in public discourse. The proposed approach offers a legal mechanism for countering this by establishing the priority of authentic sources through IP, creating legal liability for parasitising on verified narratives. The study by P. Bernal (2020) emphasises the need for legal regulation of the digital space. The claim that a new legal framework is needed seems debatable: existing IP mechanisms, adapted to new challenges, can work effectively without creating new legal institutions, which accelerates practical implementation. The study by L. Lixinski (2013) on intangible cultural heritage provides a theoretical basis for the protection of cultural practices through the UNESCO system. An example is the inclusion of Ukrainian borscht in the UNESCO list (2022), which set a legal precedent against Russian attempts at cultural appropriation. K. Carpenter *et al.* (2009) demonstrate that IP can protect collective cultural practices, which is relevant to Ukrainian national narratives. The analysis by R. Chesney & D. Citron (2019) and P. Nemitz (2018) on deepfakes and artificial intelligence confirms the relevance of the IP approach to protect against technological manipulation, maintaining a balance between innovation and democratic values. Detailed analysis by G.B. Dinwoodie & M.D. Janis (2022) and D.J. Gervais (2021) provide a legal basis for protecting visual elements and cross-border IP mechanisms in the digital space. L. Freedman (2006) confirms the historical evolution when narratives became an independent object of conflict. O. Orliuk (2025) notes that the practical sphere shapes the demand for comprehensive IP enforcement, confirming the readiness of the approach for implementation. O. Doichyk & V. Hanzin (2025) propose a typology of narratives at the macro, meso and micro levels, which is consistent with the multi-level structure of the narrative field.

The limitations of the proposed approach should also be acknowledged. First, its effectiveness depends on the willingness of the judicial system to recognise narrative constructs as objects of legal protection. Second, the cross-border nature of threats requires international coordination, which is not always possible with aggressor states. Third, the speed of the legal system's response may be slower than the pace of disinformation. Fourth, IP protection requires prior fixation and registration of objects. The novelty of the research lies in the synthesis of three previously isolated areas: strategic narrative theory, intellectual property law, and information security studies. This interdisciplinary approach can be used to define intellectual property law as a strategic element of ensuring national information sovereignty.

Conclusions

For centuries, Ukraine was deprived of the right to write and tell its history, and only today is it regaining the opportunity to formulate "stories about itself", offering the world a domestic view of the past and present. The "soft" legal instruments, the non-application of which does not entail restrictions on freedom of speech and the introduction of censorship, can become a promising tool for establishing Ukrainian strategic discourse through the recognition, protection and popularisation of intellectual property. The intellectual property mechanisms discussed in this Article are precisely such tools. They do not force people to believe in one story or another by force of law, but at the same time create a legal framework in which authentic narratives are given priority status and protection from exploitation.

The study identified several key generalisations that are both theoretically and practically significant for determination of the potential of intellectual property law in countering contemporary information threats. First, intellectual property law should be viewed not only as a tool for protecting the creative output of individual authors or organisations, but also as a broader protective mechanism capable of providing a strategic advantage in the narrative field. This involves creating a legal framework in which authentic national meanings receive official recognition and legitimisation, which significantly reduces the risks of their distortion, appropriation or exploitation by an aggressor.

Secondly, intellectual property rights instruments create opportunities for asymmetric responses to information interference. Instead of direct censorship or administrative bans, which are often interpreted as restrictions on freedom of speech, a civil law approach is applied. This can be used to classify illegal use or parasitism on counter-narratives as a violation of copyright or related rights, which moves the fight into the realm of legitimate legal procedures. This approach is more stable in democratic societies and creates extra opportunities for international advocacy and defending Ukraine's position.

Thirdly, an analysis of current Ukrainian legislation and international conventions has shown that the legal framework already has significant potential for protecting the narrative field. At the same time, a further challenge is to institutionalise practices aimed to register, protect and commercialise national intellectual products, including symbols, cultural codes, creative formats and information materials. Such steps will make it possible to create a comprehensive system of semiotic control, which is key in modern cognitive warfare.

Therefore, intellectual property rights should be considered a promising element of a national security strategy aimed to consolidate Ukrainian information sovereignty. The use of its instruments in combination with other measures to counter propaganda creates the basis for the formation of a stable narrative environment in which authentic meanings dominate and become the

foundation of the state's strategic discourse. Intellectual property law, although not designed for information warfare, offers an arsenal of protective tools suitable for this purpose. It is necessary to view it not in isolation, but in the context of the overall strategy of cultural and information policy and national security strategy.

Promising areas for further study include the application of intellectual property rights as an element of national security to protect Ukraine's information sovereignty, through the institutionalisation of practices for the registration, protection and commercialisation of national intellectual products, as well as the use of a civil law approach as an asymmetric response to information interference.

Acknowledgements

With gratitude to my academic supervisor, Professor Florin Țurcanu of the University of Bucharest, for his valuable guidance and support, and to my alma mater, the National Academy of Internal Affairs, for laying the foundations for my professional and academic development.

Funding

The Article is provided within the ATHENA, Horizon-funded project (Grant Agreement 101132686 ATHENA HORIZON-CL2-2023-DEMOCRACY-01) alongside the ISSP project partner. ATHENA is the project that aims at the early detection of FIMI campaigns and a better understanding of the behavioral and societal effects of their manifestation, aswell as the efficiency of countermeasures before and during malignantinformation campaigns.

Conflict of Interest

None.

References

[1] Bernal, P. (2020). *The road to digital unfreedom: How artificial intelligence is reshaping our lives*. Cambridge: Cambridge University Press. doi: 10.1017/9781108877534.

[2] Bjola, C., & Pamment, J. (Eds.). (2019). *Countering online propaganda and extremism: The dark side of digital diplomacy*. London: Routledge. doi: 10.4324/9781351588409.

[3] Bjola, C., & Zaiotti, R. (Eds.). (2023). *Digital diplomacy and international organisations: Autonomy, legitimacy and contestation*. London: Routledge. doi: 10.4324/9781003032724.

[4] Bykov, O.M. (2023). Information security: Legal and cultural dimensions. *Scientific Bulletin of Uzhhorod National University. Series: Law*, 78, 396-402. doi: 10.24144/2788-6018.2024.02.67.

[5] Carpenter, K., Katyal, S.K., & Riley, A. (2009). In defense of property. *Yale Law Journal*, 118(6), 1022-1125.

[6] Chesney, R., & Citron, D. (2019). Deep fakes: A looming challenge for privacy, democracy, and national security. *California Law Review*, 107(6), 1753-1820. doi: 10.15779/Z38RV0D15J.

[7] Diatlova, I., Kondratyuk-Antonova, T., & Tsykhuliak, I. (2025). Philosophical aspects of information warfare: Truth, manipulation, and critical thinking. *Philosophy and Governance*, 3(7). doi: 10.70651/3041-248X/2025.3.07.

[8] Dinwoodie, G.B., & Janis, M.D. (2022). *Trade dress and design law (2nd ed.)*. Alphen aan den Rijn: Wolters Kluwer.

[9] Doichyk, O.Ya., & Hanzin, V.V. (2025). War narrative: Definition and structure (Context of modern armed conflicts). *Kryvyi Rih State Pedagogical University Scientific Bulletin. Philological Sciences*, 1(2), 9-15. doi: 10.32999/ksu2663-3426/2025-1-2.

[10] Freedman, L. (2006). *The transformation of strategic affairs*. London: Routledge for the International Institute for Strategic Studies. doi: 10.4324/9780203820001.

[11] Gervais, D.J. (Ed.). (2021). *International intellectual property: A handbook of contemporary research*. Cheltenham: Edward Elgar Publishing. doi: 10.4337/9781788975551.

[12] Hasani, A., Rasheed, J., Alsubai, S., & Luma Osmani, S. (2024). Personal rights and intellectual properties in the upcoming era: The rise of deepfake technologies. In J. Rasheed, A.M. Abu Mahfouz & M. Fahim (Eds.), *Forthcoming networks and sustainability in the AIoT Era* (pp. 379-391). Geneva: Springer Nature Switzerland AG. doi: 10.1007/978-3-031-62881-8_32.

[13] Horbulin, V.P. (2017). *World hybrid war: Ukrainian front*. Kharkiv: Folio.

[14] Huyvan, P.D. (2020). Civilizational foundations of freedom of speech and legitimacy of its restriction. *Actual Problems of State and Law*, 86, 56-61. doi: 10.32837/apdp.v0i86.2404.

[15] Kavanagh, J., & Rich, M.D. (2018). *Truth decay: An initial exploration of the diminishing role of facts and analysis in American public life*. Santa Monica: RAND Corporation. doi: 10.7249/RR2314.

[16] Kryzhanovskyi, O.M., & Kryzhanovskyi, P.O. (2025). Prevention of criminal offenses under Article 161 of the Criminal Code of Ukraine. *Scientific Notes of the Lviv University of Business and Law. Economic Series. Legal Series*, 40. doi: 10.5281/zenodo.15185445.

[17] Kyrylyuk, O.L. (2021). Narrativity of information warfare. In *Modern pedagogue and pedagogical theory, philological disputes, and language science* (pp. 106-108). Vinnytsia: European Scientific Platform. doi: 10.36074/mcnd-19.02.2021.ped philol.

[18] Kyrylyuk, O.L. (2023). *Discourse of information warfare: Linguocognitive and psycholinguistic aspects*. (Doctoral dissertation, Ivan Franko State Pedagogical University of Drohobych, Drohobych, Ukraine).
[19] Lipkan, V.A. (2022). Narrative analysis of destructive geopolitical concepts. *Politykus: Scientific Journal*, 4, 47-55. doi: 10.24195/2414-9616.2022-4.7.
[20] Lixinski, L. (2013). *Intangible cultural heritage in international law*. Oxford: Oxford University Press. doi: 10.1093/acprof:oso/9780199668533.001.0001.
[21] Mahda, Ye. (2023). *Russia's hybrid aggression: Lessons for Europe*. Kyiv: Friedrich Ebert Foundation.
[22] Mazurenko, S. (2025). Infringement of copyright in the media space during martial law. *Legal Bulletin of Odesa Law Academy*, 3, 59-65. doi: 10.32782/yuv.v3.2025.7.
[23] Miskimmon, A., O'Loughlin, B., & Roselle, L. (2012). *Strategic narratives: Communication power and the new world order*. New York: Routledge. doi: 10.4324/9781315871264.
[24] Nemitz, P. (2018). Constitutional democracy and technology in the age of artificial intelligence. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 376(2133). doi: 10.1098/rsta.2018.0089.
[25] Orliuk, O. (2025). *Copyright on guard for national security: Why this is no exaggeration*. Retrieved from https://www.pravda.com.ua/columns/2025/07/30/7524038/.
[26] Pamment, J., Nothhaft, H., Agardh-Twetman, H., & Fjallhed, A. (2018). *Countering information influence activities: The state of the art*. Lund: Lund University, Department of Strategic Communication.
[27] Peter, K.Yu. (2024). War and IP. *Brigham Young University Law Review*, 49(3), 823-882.
[28] Petrenko, V. (2025). Protection of intellectual property rights in the context of intellectual security of an enterprise. In *Creation, protection, defense and commercialization of intellectual property rights objects: Proceedings of the VIII all-Ukrainian scientific and practical conference with international participation dedicated to the World Intellectual Property Day*. Kyiv: National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute".
[29] Pocheptsov, G. (2015). *Hybrid war: Information component*. Retrieved from https://www.academia.edu/17274555/Гібридна_війна_інформаційна_складова.
[30] Pocheptsov, G. (2019). *Modern information wars*. Kyiv: Kyiv-Mohyla Academy Publishing House.
[31] Romanyshyn, A.M., *et al*. (2023). *100 false Russian narratives about the RussianUkrainian war*. Kyiv: SKIF Publishing House.
[32] Spesyvtseva, O. (2023). *Consequences of spreading unverified information: Advice for media*. Kyiv: Center for Democracy and Rule of Law (CEDEM).
[33] UNESCO. (2022). *Culture of Ukrainian borscht cooking inscribed on the List of Intangible Cultural Heritage in Need of Urgent Safeguarding*. Retrieved from https://www.unesco.org/ru/articles/kultura-prigotovleniya-ukrainskogo-borscha-vnesena-v-spisok-nematerialnogo-kulturnogo-naslediya.
[34] Vedeniapina, M., & Pidvysotska, M. (2024). Problems of protection of intellectual property rights during the war. In *VIII international scientific and practical conference "Actual problems of intellectual property in Ukraine and the European Union"* (56-59). Budapest: Institute of Educational and Professional Development.
[35] WIPO. (2024). *WIPO Arbitration and Mediation Center*. Retrieved from https://www.wipo.int/amc/en/center/background.html.
[36] Zavershinskaia, P., & Spera, F. (2024). A change of paradigm? How the Russian invasion of Ukraine influenced Italian memory laws. *Contemporary Italian Politics*. doi: 10.1080/23248823.2024.2439175.

Інструменти інтелектуального права як проактивні засоби захисту наративного поля в контексті інформаційної війни та боротьби з пропагандою

Маріанна Присяжнюк
Аспірант
Бухарестський університет
050663, вул. Пандурі, 90, м. Бухарест, Румунія
https://orcid.org/0000-0001-6636-7620

Анотація
Досвід російсько-української війни засвідчує, що інформаційний, а також когнітивний простір є критичним виміром протистояння та агресії. Натомість стратегічні наративи є як ресурсом, так і об'єктом для атак. Стаття мала на меті виявити можливості права інтелектуальної власності як засобу асиметричної протидії інформаційним загрозам шляхом семіотичного контролю, утвердження автентичних смислів і забезпечення домінування національних наративів у наративному полі. Дослідження проведено з використанням методології, яка ґрунтується на догматичному аналізі нормативно-правових актів України та міжнародних конвенцій, системно-структурного та концептуального підходів до типології наративів, а також елементів міждисциплінарного аналізу у сфері безпеки й комунікацій та аналізу конкретних кейсів. За результатами дослідження запропоновано висновки щодо наративного поля, що є багаторівневою структурою стратегічних, регіональних і локальних наративів, кожен з яких може стати об'єктом захисту в правовому полі. Такий підхід може посилити традиційні інструменти протидії пропаганді (фактчекінг, стратегічні комунікації, санкції), які не можуть забезпечити політико-правову перевагу, водночас застосування механізмів інтелектуального права дає змогу легітимізувати національні контрнаративи й унеможливити в такий спосіб їх експлуатацію агресором. Проаналізовано національне законодавство й міжнародні механізми, які створюють підґрунтя для юридичного захисту автентичних смислів. Сформульовано висновок, що такий підхід має переваги відповідно до демократичних стандартів, оскільки IP-підхід не обмежує свободу слова, не фокусується на цензурі, натомість пропонує форми захисту для форми вираження змісту і прав автора. Відповідно інструменти інтелектуального права можуть бути застосовані як проактивний інструмент у контексті посилення інформаційної безпеки, адже посилюють стратегічний дискурс держави. Запропонований підхід у перспективі може стати основою формування політики захисту національних наративів і зміцнення інформаційного суверенітету

Ключові слова:
стратегічний дискурс; стратегічний наратив; наративне поле; правова охорона смислів; нематеріальні активи; правова легітимація; семіотичний контроль

UDC 343.1+343.337.4+343.98
DOI: 10.63341/naia-chasopis/3.2025.70

Circumstances subject to determination in proceedings concerning violations of the laws and customs of war

Nataliia Rubanenko*
Postgraduate Student
National Academy of Internal Affairs
03035, 1 Solomianska Sq., Kyiv, Ukraine
https://orcid.org/0009-0001-2958-4228

Anna Myrovska
PhD in Law, Professor
National Academy of Internal Affairs
03035, 1 Solomianska Sq., Kyiv, Ukraine
https://orcid.org/0000-0001-5714-1873

Abstract
The research relevance is determined by the need to improve the methodology of proof in criminal proceedings on the fact of violation of the laws and customs of war. The study addressed the disposition of Article 438 of the Criminal Code of Ukraine, according to which the norms of international humanitarian and criminal law should be applied. The study aimed to determine the structure of the subject matter of proof in war crimes cases, to identify its features in view of the principle of complementarity, and to develop a forensic classification and characterisation of the relevant acts. The methodological toolkit included systemic and structural, comparative legal, and formal legal methods, content analysis of case law, and inductive analysis, which formulated theoretical generalisations based on the study of specific criminal proceedings. The practical basis of the study was determined by the analysis of decisions of national courts of first instance and appellate courts in cases involving war crimes on the territory of Ukraine. The study established that the process of proof has a dual nature. It covers, on the one hand, the circumstances stipulated by criminal procedural law, and, on the other hand, the facts that are key to qualifying acts as international crimes committed within the framework of an armed conflict and having a direct connection with it. In this context, the investigation of war crimes is characterised by an increased level of complexity, which can be conditionally differentiated into two groups. The first group includes circumstances of an objective nature that cannot be influenced by the pre-trial investigation authorities. The second group is formed by negative factors that can be influenced within criminal proceedings to minimise their consequences. In this aspect, typical elements to be established during the investigation of violations of the laws or customs of war were identified. The study substantiated the expediency of supplementing Article 438 of the Criminal Code of Ukraine with qualifying circumstances which specify its content. The scientific and practical significance of the results obtained includes the development of a unified approach to the analysis, verification and evaluation of evidence in war crimes cases, as well as to

Article's History:
Received: 24.05.2025
Revised: 26.08.2025
Accepted: 29.09.2025

Suggest Citation:
Rubanenko, N., & Myrovska, A. (2025). Circumstances subject to determination in proceedings concerning violations of the laws and customs of war. *Law Journal of the National Academy of Internal Affairs*, 15(3), 70-81. doi: 10.63341/naia-chasopis/3.2025.70.

*Corresponding author

develop a forensic classification and forensic characteristics of such offences to form a unified methodology for investigating violations of the laws and customs of war

Keywords:
war crimes; subject matter and limits of proof; contextual circumstances; armed conflict; international humanitarian law; international criminal law; forensic characterisation; forensic classification

Introduction

The complexity of the process of proving in criminal proceedings for violations of the laws and customs of war is due to the blanket nature of the disposition of Article 438 of the CC of Ukraine[1], which requires additional specification through international legal norms and case law of international tribunals. This circumstance indicates the complementary nature of international and national law as complementary systems. Accordingly, pre-trial investigation bodies are obliged to conduct criminal proceedings in accordance with international standards for the protection of human rights and freedoms, as well as the key provisions of the Rome Statute[2], which is a fundamental but not the only instrument of international criminal justice.

In this context, when investigating violations of the laws and customs of war, authorised participants in criminal proceedings should be guided not only by the norms of national legislation, but also incorporate the material, procedural and penal aspects of war crimes investigation (Caianiello, 2022). This was addressed by O. Kravchuk & M. Bondarenko (2022), noting that the investigation of violations of the laws and customs of war acquires specific features due to the peculiarities of the subject of proof, its objective and subjective characteristics that determine the participants in the offence and their motives, ways of implementing criminal intentions, the nature and scale of socially dangerous consequences, as well as circumstances that may indicate the systematic or massive nature of unlawful acts and their connection with political or military plans, strategies and/or structures.

In this regard, O. Agarkova (2024) noted that during the identification and recording of violations of the laws and customs of war, law enforcement activities should focus on establishing both the general elements of proof defined by criminal procedural law[3] and the individual (specific) circumstances of a particular unlawful act, which can define the features of the objective side of a war crime and conduct its criminal law qualification. In fact, this position is consistent with the provisions of Articles 214-216 of the CPC of Ukraine[4] and Article 19 of the Basic Law[5].

According to S. Sichko (2019), the correct and timely determination of jurisdictional competence in criminal proceedings for violations of the laws and customs of war is a substantial prerequisite for the effective implementation of law enforcement activities and the efficient fulfilment of criminal justice tasks. That is, failure to comply with the requirements for qualification of the criminal offences under investigation and their procedural jurisdiction may cause significant complications in the process of proof and lead to the incorrect application of the methodology for collecting and analysing the evidence base, which, according to Yu. Tan & S. Yang (2023), negatively affect the quality of criminal proceedings and the legality of the results obtained.

According to the analysis of court practice, these violations impede the effective interaction of pre-trial investigation bodies with other participants in criminal proceedings, as well as lead to the loss of relevant evidence and distortion of its assessment, which complicates the administration of justice and increases the risk of erroneous decisions[6]. In this regard, in some criminal proceedings, there is an insufficient analysis of the circumstances that establish the nature of the armed conflict, which negatively affects the validity of the qualifying features of war crimes and may lead to an erroneous assessment of their composition[7]. In some cases, despite the established link between the unlawful act and the armed conflict, the key circumstances that determine the legal nature of the conflict, the status of its parties, the place and time of the crime, the nature of the accused's activities, role in the conflict, and the victims' affiliation with persons not involved in the armed conflict are not properly detailed.

In addition, the circumstances related to the period of illegal detention of victims, the fact of their forced labour, the type and nature of work performed, etc., are insufficiently investigated[8]. In several cases, the only sources of evidence establishing a link between the

[1] Criminal Code of Ukraine. (2001, May). Retrieved from https://zakon.rada.gov.ua/laws/show/2001-05#Text.
[2] Rome Statute of the International Criminal Court. (1998, July). Retrieved from https://zakon.rada.gov.ua/laws/show/995_588#Text.
[3] Criminal Code of Ukraine. (2001, May). Retrieved from https://zakon.rada.gov.ua/laws/show/2001-05#Text.
[4] Criminal Procedure Code of Ukraine. (2012, April). Retrieved from https://zakon.rada.gov.ua/laws/show/4651-17#Text.
[5] Constitution of Ukraine. (1996, June). Retrieved from https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text.
[6] Verdict of the Kelmenetsky District Court of Chernivtsi Region in Court Proceedings No. 1-кп/717/1/18. (2018, October). Retrieved from http://www.reyestr.court.gov.ua/Review/77098737.
[7] Ruling of the Luhansk Court of Appeal No. 415/2182/20. (2020, October). Retrieved from https://reyestr.court.gov.ua/Review/92065176.
[8] Ruling of the Cassation Criminal Court of the Supreme Court No. 415/2182/20. (2022, February). Retrieved from https://reyestr.court.gov.ua/Review/103466917.

armed conflict and the act committed are testimonies, which are not always sufficient to fully and comprehensively establish all the circumstances of the case, as no testimony can be considered in isolation without corroboration by other relevant and admissible evidence[1].

Therefore, as noted by A. Szalai & V. Ahmeti (2025), the quality of the evidence process in criminal proceedings for violations of the laws and customs of war is affected by a wide range of negative factors. Taken together, they require comprehensive research and careful assessment. As a result, it is necessary to develop new approaches to law enforcement, improve interagency cooperation, enhance the education and training of relevant specialists in the investigation of international crimes, and integrate international experience to improve international law enforcement mechanisms in national legislation.

As noted by A. Shulzhenko (2022), the investigation of war crimes mostly encounters difficulties due to the complexity of establishing objective features of a particular offence, the peculiarities of its criminal law qualification, as well as the uncertainty of the subjects of the offence and the victims of its commission. There are also problems with assessing physical, moral, material and/or property damage, as well as the mechanisms for its compensation. An additional complicating factor is the lack of unified methods for investigating violations of the laws and customs of war. This necessitates a comprehensive scientific study of the material, procedural and forensic aspects of war crimes investigations. A significant condition in this process is to ensure proper coordination between national and international law enforcement and justice agencies to create a single mechanism capable of responding immediately to global challenges and needs arising in the context of international criminal justice.

In this aspect, the study aimed to determine the circumstances to be established in criminal proceedings on the fact of violation of the laws and customs of war, accounting for their significance for further development of the criminalistics classification and criminalistics characteristics of war crimes. In this regard, the main objectives of the study are, firstly, to outline, based on a systematic analysis of scientific literature, investigative and judicial practice, the range of factual circumstances to be established in the process of proving violations of the laws and customs of war. Secondly, following the identified circumstances, to determine those which are essential for the investigation of war crimes and should be reflected in the structure of their forensic classification and characterisation.

Materials and Methods

The regulatory framework of the study is based on national and international legislation, which regulates the material and procedural aspects of war crimes investigation. These are the provisions of the criminal law of Ukraine[2], the criminal procedure law of Ukraine[3], the Rome Statute of the International Criminal Court[4], the Geneva Conventions of 1949[5] and their Additional Protocols[6], which define serious violations of international humanitarian law. In addition, the study covered the provisions of other international legal acts establishing general standards in the field of protection of human rights and freedoms, which are analysed through the prism of their legal nature and significance for the qualification and investigation of violations of the laws and customs of war.

The practical basis of the study is the analysis of court decisions of the first instance[7,8,9] and higher courts[10,11] in criminal proceedings on war crimes committed on the territory of Ukraine. This traced the peculiarities of the legal qualification of the acts under study, procedural approaches to recording and evaluating evidence, and identified several problems related to the interpretation of international humanitarian law within the framework of national law enforcement. The collected data provided an empirical basis for substantiating the conclusions and recommendations of the study.

Thus, the methodological basis of the study is a set of general scientific and special legal methods which ensured the comprehensiveness and scientific validity of the results obtained. In particular, the systemic-structural method was used to identify the internal

[1] Verdict of the Slavyanskyi City Court of Donetsk Region in case No. 243/6186/20. (2021, December). Retrieved from https://reyestr.court.gov.ua/Review/99929812.
[2] Criminal Code of Ukraine. (2001, May). Retrieved from https://zakon.rada.gov.ua/laws/show/2001-05#Text.
[3] Criminal Procedure Code of Ukraine. (2012, April). Retrieved from https://zakon.rada.gov.ua/laws/show/4651-17#Text.
[4] Rome Statute of the International Criminal Court. (1998, July). Retrieved from https://zakon.rada.gov.ua/laws/show/995_588#Text.
[5] Geneva Convention relative to the Protection of Civilian Persons in Time of War. (1949, August). Retrieved from https://zakon.rada.gov.ua/laws/show/995_154.
[6] Protocol Additional to the Geneva Conventions of August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I). (1977, October). Retrieved from https://zakon.rada.gov.ua/laws/show/995_199.
[7] Verdict of the Kelmenetsky District Court of Chernivtsi Region in Court Proceedings No. 1-кп/717/1/18. (2018, October). Retrieved from http://www.reyestr.court.gov.ua/Review/77098737.
[8] Verdict of the Slavyanskyi City Court of Donetsk Region in Case No. 243/6186/20. (2021, December). Retrieved from https://reyestr.court.gov.ua/Review/99929812.
[9] Decision of the Kherson City Court No. 98716623. (2022, July). Retrieved from https://reyestr.court.gov.ua/Review/98716623.
[10] Ruling of the Luhansk Court of Appeal No. 415/2182/20. (2020, October). Retrieved from https://reyestr.court.gov.ua/Review/92065176.
[11] Ruling of the Cassation Criminal Court of the Supreme Court No. 415/2182/20. (2022, February). Retrieved from https://reyestr.court.gov.ua/Review/103466917.

links between the elements of legal regulation of war crimes investigation. The comparative legal method was used to compare national and international norms governing criminal liability for violations of the laws and customs of war. Formal legal method for analysing legal acts and interpretations of legal concepts within the scope of the study. The method of contextual analysis was used to study the content of court decisions and the scientific base to identify typical approaches to the qualification and investigation of war crimes. The method of inductive analysis was used to draw general conclusions based on specific empirical data and the results of legal analysis.

Results and Discussion

Before proceeding to the identification of facts to be established in proceedings for violations of the laws and customs of war, it is first necessary to outline the negative factors that affect the process of proof in cases of this category. Such an approach is determined by several reasons and is methodologically justified in the context of the issues under study. Firstly, any process of proof in criminal proceedings is not an isolated phenomenon. It is an integral part of criminal proceedings, which functions as a complex system in which legal, social, psychological, ethical and organisational aspects interact. Evidence processing is always conducted within a specific criminal situation, characterised by a set of circumstances that can both facilitate and hinder the investigation.

Secondly, timely identification of such factors at the initial stage of the pre-trial investigation can be used for an objective assessment of the real conditions and potential possibilities of the evidence process, an outline of the range of circumstances to be established, identification of those complicated by the influence of external and/or internal factors, and timely determination of the need to apply alternative approaches to collecting evidence. This, in turn, ensures systematic and consistent forensic analysis that considers the specifics of both the commission of war crimes and their evidence.

Thus, a systematic analysis of the scientific literature, methodological recommendations and materials of investigative and judicial practice can be used to classify the negative factors affecting the process of proof in criminal proceedings for violations of the laws and customs of war into two main groups. The first one covers conditions on which the authorised pre-trial investigation bodies have no real influence, since they exist regardless of the will or procedural activity of the participants in criminal proceedings. Under these conditions, it is only appropriate to partially adjust or adapt the tactics and methods of pre-trial investigation to the specifics of the situation within which the process of proof is carried out.

This group includes the dynamics of the development of hostilities, characterised by high variability, intensity and rapid change of the operational and tactical situation in the armed conflict zone (Shulzhenko, 2022). This significantly complicates the timely and complete implementation of procedural actions necessary for the collection, verification and legal assessment of evidence. At the same time, the systematic movement and change of deployment of military units can lead to the loss or distortion of primary information, in particular, that which records signs of a crime, and its identification and research are a prerequisite for a full and comprehensive investigation (Hryha & Burnos, 2024). It is also worth paying attention to the complete or partial destruction of the crime scene as a result of hostilities (Batiuk & Dmytriv, 2021), which significantly complicates the process of identifying, recording and investigating the circumstances of the crime at the scene.

This group also includes the death, injury, capture or repatriation of potential participants in criminal proceedings (Yankovyi, 2023), which complicates the possibility of obtaining testimony that is essential to establish the circumstances of a criminal offence and form a sufficient evidence base. The process of proof is also complicated by the excessive burden on the authorised pre-trial investigation bodies due to the large number of criminal offences committed in the combat zone. In addition, another reason that complicates the process of investigating violations of the laws and customs of war is the limited access to certain types of information, including information related to state and/or military secrets, which is necessary for the process of proof but cannot be provided within the framework of the proceedings (Fig. 1).

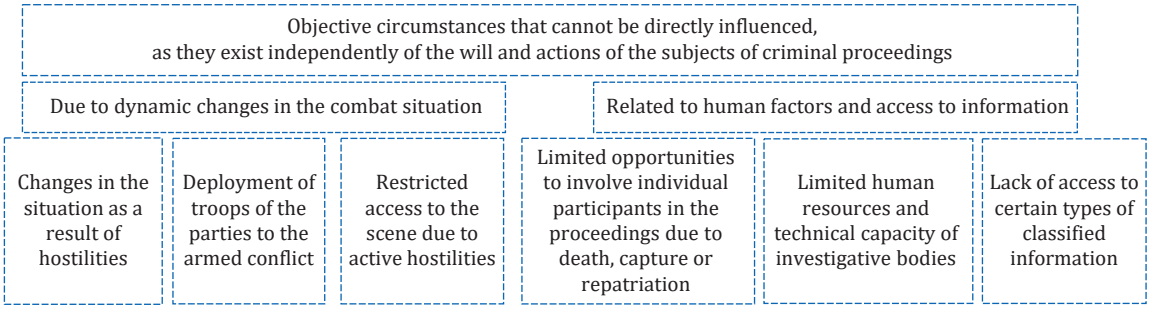

Figure 1. Objective negative factors that complicate the process of proof in the investigation of war crimes
Source: compiled by the authors

The second group consists of factors that authorised participants in criminal proceedings can influence to minimise their negative consequences. These circumstances include legal uncertainty and insufficient clarity of the regulatory provisions governing the procedural aspects of war crimes investigation (Kozmenko *et al.*, 2023). This can lead to misinterpretation of legislation, difficulties in the legal qualification of an act, as well as ambiguous application of criminal law provisions in terms of legal assessment of serious violations of international humanitarian law. This group also includes the insufficient level of legal awareness of authorised participants in criminal proceedings regarding the mechanisms of interaction with international institutions, in particular, specialised institutions of international criminal justice (Khavroniuk, 2022; Lebeniuk & Osypenko, 2024). This reduces the effectiveness of coordination of procedural actions in cases with an international context, and contributes to the emergence of legal conflicts and slows down the establishment of the contextual circumstances of war crimes in accordance with international standards of justice.

Within the above reasons, it is worth highlighting the lack of clearly formulated, scientifically based and practically oriented methodological approaches to determining the subject matter and limits of proof in war crimes cases (Kovalenko, 2022; Antoniuk, 2023). This problem is exacerbated by the influence of contextual circumstances that cause difficulties with the legal interpretation of the relevant rules and the sequence of the evidence process. An equally significant problem is the limited staffing capacity of pre-trial investigation bodies due to the shortage of qualified professionals with the necessary theoretical knowledge and practical experience (skills) in investigating international crimes. Lack of proper professional training or retraining of employees involved in the investigation of war crimes directly affects the quality and effectiveness of the evidence process.

It is also worth noting the insufficient level of interagency cooperation between pre-trial investigation bodies, prosecutors, military formations, as well as other state institutions and local governments, including military administrations, which consequently complicates the effective cooperation of these bodies in solving the tasks of criminal proceedings (Kornev, 2022). In addition, the insufficient level of development of relevant forensic methods for investigating war crimes aimed to collect, analyse and procedurally use evidence in cases of this category (Hryha & Burnos, 2024), equally significantly reduces the effectiveness of the investigation and complicates the provision of an evidence base that would meet both national and international legal requirements (standards) (Fig. 2).

Figure 2. Controllable (subjective) factors that complicate the investigation of war crimes
Source: compiled by the authors

In view of the above, a priority area for addressing the problems referred to in the second group is a comprehensive analysis of the characteristics inherent in war crimes, with an emphasis on the methods of their commission. This approach will ensure a more accurate interpretation of the disposition of Article 438 of the Criminal Code of Ukraine[1], which currently only fragmentarily defines the objective circumstances of serious violations of international humanitarian law. Accordingly, there is a need to systematise and structure the elements of the act under investigation, which can be utilised as a structured approach to analysis of the subject matter and limits of proof in cases involving violations of the laws and customs of war.

This thesis is confirmed by several court decisions. In their context, it is worth analysing the ruling of the Kherson City Court of 30 July 2021 in case No. 766/12962/21[2] on the election of a preventive measure in the form of detention for committing a crime under Part 5 of Article 27 and Part 1 of Article 438 of the Criminal Code of Ukraine[3]. According to this decision, security investigators served a notice of

[1] Criminal Code of Ukraine. (2001, May). Retrieved from https://zakon.rada.gov.ua/laws/show/2001-05#Text.
[2] Decision of the Kherson City Court No. 98716623. (2022, July). Retrieved from https://reyestr.court.gov.ua/Review/98716623.
[3] Criminal Code of Ukraine. (2001, May). Retrieved from https://zakon.rada.gov.ua/laws/show/2001-05#Text.

suspicion of committing acts in violation of the laws and customs of war to a Ukrainian citizen for entering into a contract with a military state institution of federal significance in March 2017, while permanently residing with the family in the occupied Crimea and being a business entity, relevant business agreements on the provision of services for the transportation of persons of military age from the military commissariats of the Autonomous Republic of Crimea to the recruitment points, which, according to the investigation, violated the laws and customs of war in the form of aiding and abetting, consisting in providing means for committing war crimes by transporting persons protected by international humanitarian law.

The legal position of the prosecution in the criminal proceedings under investigation is believed to be insufficiently substantiated, as it does not fully comply with the contextual and legal features or elements that characterise the commission of war crimes. In this context, V. Repetskyi & V. Lysyk (2009) distinguished at least four general contextual features that are characteristic of all war crimes. The latter includes, firstly, actions that form the objective side of war crimes, which are committed exclusively during armed conflict or are directly related to it. In other words, war crimes can only be committed within the framework of an armed conflict or have a direct connection with it. Otherwise, as V. Novrotskyi (2022), these acts should be qualified under general, special and/or casualty grounds of criminal offences against peace, national security, life and health, human security or international law and order.

This feature is highlighted by I. Hlovyuk & H. Teteryatnyk (2022), noting that war crimes can be committed exclusively in the context of an armed conflict of an international or non-international nature, provided that the perpetrators of these offences are aware of the factual circumstances confirming the existence of such a conflict. This indicates the existence of a causal link between the act and the armed conflict.

Accordingly, not all offences committed during an armed conflict can be classified as war crimes. For example, criminal offences with material elements that are not directly related to the armed conflict occurring in any part of the territory controlled by the parties to the conflict cannot be considered war crimes. In fact, this position is supported by T. Yefimenko (2024), illustrating the opinion with the Basic Investigative Standards for International Crimes Investigation (Compliance with global rights, 2016), developed by an international non-profit human rights organisation specialising in legal protection, human rights and justice in the context of international crimes.

Secondly, acts committed by war crimes perpetrators must infringe upon the fundamental principles (foundations) of international humanitarian law, which define the limits of acceptable behaviour of participants (parties) to an armed conflict. Violation of these fundamentals gives war crimes the status of serious violations of international humanitarian law, which fundamentally distinguishes them from other socially dangerous acts by the nature of the offence, the legal context and international legal responsibility. Some researchers include the following principles of international humanitarian law: protection of persons not directly involved in an armed conflict, which implies the obligation of the parties to the conflict to refrain from attacks on civilians and persons not involved in hostilities; distinction, which requires a clear separation of civilians and infrastructure from military objectives by the parties to the conflict; selectivity and proportionality, which relates to the reasonable choice of the object of attack; limitation of means and methods of warfare, which

Thirdly, war crimes are usually committed by combatants or other persons with the authority to give orders in an armed conflict. This means that only persons authorised by a party to the conflict to take part in hostilities, endowed with the relevant rights and obligations, and acting within the framework of an armed conflict, on behalf of a party to the conflict, a subject of international legal relations (state, union, coalition, or other recognised entity) can be the subjects of violations of the laws and customs of war. Combatants and the military and political leadership of the country have a direct obligation to comply with international humanitarian law, as they are the only ones with the relevant authority to conduct armed struggle and issue military and political orders within the framework of military resistance.

Fourthly, the object of war crimes are persons, their rights, freedoms and property protected by international humanitarian law, as well as other benefits, subjects and objects protected by its norms, including authorised representatives of international organisations whose activities are governed by relevant conventions and institutional norms of international law (authorised representatives of the Red Cross, IAEA, OSCE, etc.), cultural property and World Heritage sites, the natural environment, etc. (Rubanenko, 2024a).

A similar opinion is shared by O. Pchelina & V. Pchelin (2022), adding that the complexity and specificity of war crimes investigations are due not only to the need to amend national legislation to harmonise or unify it with international legal standards, but also to the development of scientifically sound approaches to the tactics and methods of investigating these crimes. In other words, scholars substantiate the expediency of forming a forensic methodology for investigating war crimes. In this context, based on legal regulation and case law on documenting the acts under investigation, it is proposed to develop a forensic classification of these crimes in scientific circles, with due regard for their forensic characterisation.

The relevance of developing a methodology for investigating war crimes, as well as determining the

subject matter and limits of their proof, is confirmed by court practice, which reflects the application of national legislation, considering the implementation of international criminal law in criminal proceedings. In this regard, it is worth paying attention to the verdict of the Solomianskyi District Court of Kyiv of 23 May 2022 in case No. 760/5257/22[1]. According to this decision, a Russian serviceman was charged with a war crime, namely the intentional killing of a civilian in the execution of a criminal order. The criminal proceedings established that the convict, being in the combat zone, mistakenly perceived the civilian as a threat because of the telephone conversation, assuming that the civilian could pass on information about the location and number of Russian troops. Executing a criminal order from a military superior, the perpetrator used a firearm, intentionally causing the victim's death, which is a violation of the laws and customs of war under international humanitarian law.

However, the analysis of scientific discussions on the legal assessment of this situation suggests that some researchers have a well-founded position on the erroneous criminal law qualification of this act. When analysing the event under study, scholars note that not every fact of killing a civilian during an armed conflict by the relevant participants is a violation of the laws and customs of war. According to I. Hlovyuk & G. Teteryatnyk (2022), this is explained by several aspects, where one approach to assessing the situation is to analyse the legal status of a civilian in the context of possible participation in hostilities.

Firstly, if a civilian is viewed as a subject who transmits information about the location of enemy armed forces, status as a noncombatant may be lost, as such actions may be regarded as direct participation in an armed conflict. This may lead to the loss of legal immunity guaranteed to subjects of civilian legal relations under international humanitarian law.

At the same time, it is worth noting that when assessing any situation, military personnel had to be certain that there were signs that the telephone conversation did indeed concern the transmission of information of military significance. This means that the question of direct intent and full awareness of the violation of international humanitarian law requires separate proof. If the above circumstances cannot be properly proven, in accordance with the presumption of innocence, any doubts regarding the commission of a war crime should be interpreted in favour of the accused. However, this does not eliminate legal responsibility for the act of taking a life, since even if there is suspicion of a person's possible participation in hostilities, the principles of distinction, proportionality and necessity enshrined in international humanitarian law must be observed (Rubanenko, 2024b).

This fact is confirmed by several international legal acts. According to Article 3 of the Universal Declaration of Human Rights, everyone is guaranteed the right to life, liberty and security of person[2]. Article 6, paragraph 1, of the International Covenant on Civil and Political Rights defines life as an inalienable right of everyone protected by law and prohibits arbitrary deprivation of this right[3]. Article 2(1) of the European Convention on Human Rights enshrines the right to life of everyone, while providing for exceptions in cases of execution of a death sentence, protection of others, prevention of escape from custody, and the lawful use of force to suppress riots or uprisings[4].

Similar provisions are contained in the Geneva Conventions and their Additional Protocols regulating the protection of civilians in armed conflicts. Articles 27 and 32 of the IV Convention prohibit any acts of violence against the civilian population, including those involving intentional killing[5]. Article 51(2) of Additional Protocol I prohibits attacks directed against civilians. The same applies to attacks on civilian infrastructure (Article 52)[6]. In this context, according to Article 57 of the Protocol, the parties to the conflict have an obligation to exercise due care for the protection of the civilian population, civilians and civilian objects at all times, and to take the necessary measures to distinguish between military objectives and objects of special protection to prevent their destruction. In addition, the parties to the conflict are obliged to use all possible means and methods of warfare that do not cause unnecessary civilian casualties, including incidental deaths.

Therefore, in the process of investigating war crimes, it is of particular importance to establish contextual and legal elements (circumstances) that determine the specifics of the subject matter of proof in criminal proceedings for violations of the laws and customs of war. At the same time, the circumstances are to be established in accordance with Article 91 of the CPC of Ukraine[7] must be causally related to the contextual characteristics of the offence. That is why, as noted by I. Hlovyuk & H. Teteryatnyk (2022), the structure of the

[1] Verdict of the Solomyanskyi City Court of Kyiv No. 760/5257/22. (2022, May). Retrieved from https://reyestr.court.gov.ua/Review/104432094.
[2] Universal Declaration of Human Rights. (1948, December). Retrieved from https://zakon.rada.gov.ua/laws/show/995_015#Text.
[3] International Covenant on Civil and Political Rights. (1966, February). Retrieved from https://zakon.rada.gov.ua/laws/show/995_043#Text.
[4] European Convention on Human Rights. (1950, November). Retrieved from https://zakon.rada.gov.ua/laws/show/995_004#Text.
[5] Geneva Convention relative to the Protection of Civilian Persons in Time of War. (1949, August). Retrieved from https://zakon.rada.gov.ua/laws/show/995_154.
[6] Protocol Additional to the Geneva Conventions of August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I). (1977, October). Retrieved from https://zakon.rada.gov.ua/laws/show/995_199.
[7] Criminal Procedure Code of Ukraine. (2012, April). Retrieved from https://zakon.rada.gov.ua/laws/show/4651-17#Text.

subject matter of war crimes evidence has a two-element characteristic.

The first element is general and includes circumstances stipulated by the rules of procedural law and individual facts that depend on the specific case of a criminal offence and the specifics of its investigation. The second element, in turn, is contextual or special legal in nature, due to the specifics of objective and subjective factors defined by international law. A substantial aspect is the assessment of the objective and subjective features of the act under investigation and their relationship to the armed conflict. In other words, when investigating war crimes, it is necessary to first establish a causal link between a particular act and the armed conflict in which it was committed (Fig. 3).

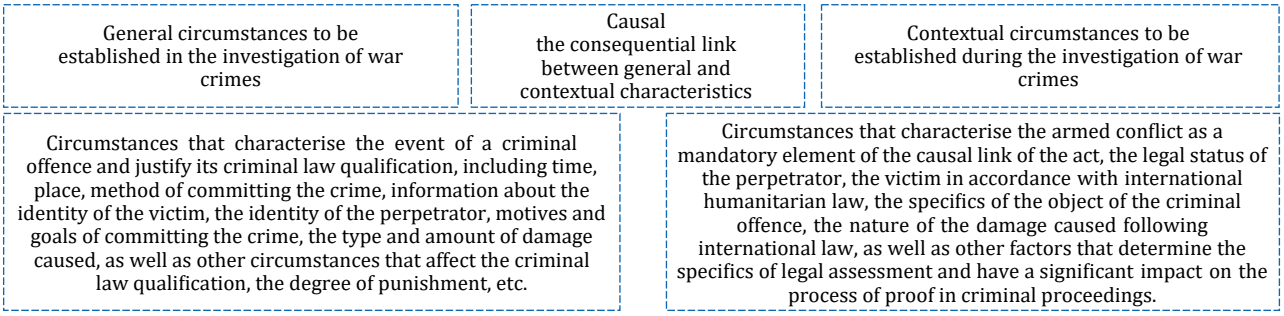

Figure 3. Two-element structure of the subject matter of proof in war crimes cases
Source: compiled by the authors

Other researchers have also drawn attention to this feature. Thus, analysing the process of proof in war crimes cases, D. Lazareva (2025) emphasises the obligation to establish contextual elements that must have a causal relationship with other circumstances to be proved in accordance with Article 91 of the CPC of Ukraine. As the author notes, this affects the specifics of criminal procedure and the peculiarities of investigative actions. According to M. Yankovyi (2023), the general characteristics of criminal offences committed by military personnel in armed conflict have a three-tiered structure, consisting of generic, group and species aspects of their commission. The study proposed to consider the differences between these groups through a set of features inherent in the respective genus, group or specific type of criminal offence. According to the author, generic features are inherent in all unlawful acts committed by military personnel in the context of armed conflict.

Group features relate to certain types of criminally similar offences determined by the circumstances of hostilities and the conditions of their commission during international or internal conflicts. Specific features, in turn, are inherent in certain types of criminal offences that are directly related to the conduct of hostilities and their course in a combat situation. From this perspective, the formation of circumstances to be established in the investigation of war crimes is determined by both the subject of proof and the criminal law and forensic assessment of a particular criminal offence. In this context, researchers rightly emphasise that the subject of proof in war crimes proceedings covers not only the general circumstances provided for in Article 91 of the CPC of Ukraine[1], but also special or contextual elements that reflect the specifics of the category of crimes under investigation.

Developing this position, D. Lazareva (2025) addressed the close relationship between the subject matter of proof and the circumstances to be established in war crimes cases. The study noted that the determination of such circumstances directly affects the subject matter of proof, which integrates both criminal law and forensic components of a particular offence. In this context, K. Shevchyshyna (2024) identified an indicative list of circumstances to be proved in the investigation of war crimes. These include information that characterises the event of the war crime itself, the circumstances that determine its criminal law qualification, information on the time, place, manner and means of committing the unlawful acts, data on the traces of the crime, information on the victim, witnesses, eyewitnesses and complainants, characteristics of the offender, circumstances related to the intent, motives and purpose of the unlawful act, other information and/or data relating to the specific event and its consequences.

O. Taran (2022) employed a more specific approach. Analysing the issues of legal regulation and law enforcement in the process of investigating violations of the laws and customs of war, the study proposed that the circumstances to be proved in war crimes cases (the subject of proof) include the circumstances of the crime, which covers the totality of conditions under which the war crime was committed. In this regard, the author divides these circumstances by physical and legal features. The

[1] Criminal Procedure Code of Ukraine. (2012, April). Retrieved from https://zakon.rada.gov.ua/laws/show/4651-17#Text.

researcher refers to the physical ones as the very fact of committing a crime and its consequences, and to the legal ones as the correlation of this fact and consequences with the norms of national and international law.

In addition, the study highlighted the methods of committing a crime that result from the wording of international law, in particular those contained in the Rome Statute, the Geneva Conventions, their protocols, as well as other international instruments of treaty value, the provisions of which cover the relevant area of legal regulation. In this context, the study identified specific methods of ill-treatment of prisoners of war, expulsion of civilians for forced labour, looting of national property in the occupied territories, use of means of warfare prohibited by international treaties and other violations of the laws and customs of war, as well as ordering them to be committed.

Equally relevant is the connection of the offender's unlawful actions with the conditions of martial law. That is, the offender's awareness of the fact that unlawful acts are committed within the framework and in pursuance of the military and political plan, policy and strategy of the state, where a participant is involved in an armed confrontation of international or non-international significance, and actions are or may be part of the functions, tasks, orders or correspond to their context. It is not necessary for a person to be aware of all the details of a military-political nature. A cognitive awareness and perception of the situation as part of the military-political context is sufficient to determine the purpose, motives and circumstances of the unlawful actions.

The existence of an order, its execution, as well as the duties of military commanders and superiors who are authorised to issue orders to subordinate military personnel, deserve special attention. The issuance and execution of an order must include subjective and substantive components to prevent violations of the laws and customs of war. Any order should incorporate the requirements of international humanitarian law and not violate them, and should be aimed to ensure compliance with the rules governing the behaviour of participants in armed conflict.

This feature is also highlighted in the provisions of Article 87 of Additional Protocol I, entitled "Duties of commanders"[1]. In fact, this provision emphasises the importance of the legality of orders in the context of armed conflict and establishes the responsibility of commanders for non-compliance with international humanitarian law. That is, commanders are responsible for the orders they give to their subordinates. They are obliged to take measures to ensure that their subordinates do not violate international humanitarian law and execute orders only within the limits of permitted actions. They must ensure that organisational and preventive measures are in place to prevent their subordinates from conducting orders that are clearly criminal or from committing unlawful acts in violation of international humanitarian law.

In general, these circumstances form two main purposes of proof, which form the evidence base within the investigation. The first relates to evidence of the event of the criminal offence (time, place, manner, circumstances of commission, mechanism of development of unlawful acts, their consequences, connection between the event, circumstances and consequences, etc.) The second is evidence of involvement (who, with whom, how, in what manner, on whose orders, plan committed the crime, its purpose, motives, etc.). It is the evidence of involvement that creates the basis for proving the causal link between the act committed and the military and political structures involved in and managing the military conflict (Compliance with global rights, 2016).

As I. Hlovyuk & H. Teteryatnyk (2022) noted, without establishing the contextual elements and their causal relationship with the unlawful act, it is impossible to make a proper criminal law assessment of the act and determine the subject matter of its proof. The existence of a special subject matter in war crimes cases is due to the peculiarity of their criminal law qualification in accordance with international criminal law, as well as the need to establish a causal link between the contextual (special) and general (mandatory) elements of the subject matter of proof.

According to O. Agarkova (2024), the evidence should contain facts and circumstances that make it possible to establish individual signs of a specific event of a criminal offence and clearly outline the form of the objective side of the violation of the laws and customs of war. Therefore, when investigating war crimes, the analysis of the methods of their commission is of particular importance, which is assessed in the light of international law governing the relevant area of legal relations.

In this context, war crimes can be classified into acts that encroach on: life and health of a person, honour and dignity, inviolability and security; property rights; special international immunity of the relevant subjects of international legal relations and their activities as defined by international law; functioning of vital infrastructure to ensure the basic needs of the population and the stability of the state; established rules and methods of warfare.

This affects the choice of methods and means for collecting and analysing information about the criminal offence, the object of the offence, the victim, the place of commission, as well as the socially dangerous consequences and their causal relationship with the perpetrator's actions (Pchelina & Pchelin, 2022). These elements are substantial for establishment for relevant

[1] Protocol Additional to the Geneva Conventions of August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I). (1977, October). Retrieved from https://zakon.rada.gov.ua/laws/show/995_199.

circumstances of the act, which is necessary for its proper legal assessment, as well as for the formation and construction of the evidence base in a particular criminal proceeding.

Conclusions

The process of proving in criminal proceedings for violation of the laws and customs of war is characterised by high legal and evidentiary complexity. This is due to the blanket nature of the disposition of Article 438 of the Criminal Code of Ukraine, which provides for liability for war crimes. In this regard, pre-trial investigation bodies are obliged to implement the principle of complementarity, which requires reference not only to the provisions of national legislation, but also to the provisions of international humanitarian law and the case law of international criminal tribunals integrated into the domestic legal system. This approach ensures the unity and consistency of the evidentiary procedure in cases of this category, in conditions when international standards complement national jurisdiction.

In this regard, pre-trial investigations should be conducted with due regard to the need to achieve an appropriate balance between domestic law and the requirements of international criminal justice. The harmonisation of these two legal systems concerns both substantive and procedural aspects. Therefore, pre-trial investigation bodies should have the appropriate level of legal training to properly apply international law in the process of proving war crimes at the national level.

In this context, the subject matter of proof in criminal proceedings for violations of the laws and customs of war is of a dual nature. On the one hand, it covers the establishment of general circumstances to be proved in accordance with the provisions of the criminal procedure legislation, including the factual data that characterise the event of a criminal offence. On the other hand, it involves establishing contextual and legal features defined by international humanitarian and criminal law, as well as proving their connection to the unlawful acts, their consequences and the armed conflict itself. In this context, the key is not only to prove the existence of an armed conflict, but also to determine its legal nature, classification, and establish the fact that prohibited acts were committed by participants in the armed conflict within its borders.

Clarifying these circumstances is key to the process of proving violations of the laws and customs of war, as they form the basis for applying international legal approaches and recommendations developed in the practice of war crimes investigation. Their establishment contributes to the formation of a holistic view of unlawful acts committed in armed conflict and ensures the analytical capacity of pre-trial investigation bodies in the complex legal and factual structure of international crimes.

The limits of the subject matter of proof in cases of violations of the laws and customs of war are closely related to the theoretical foundations of forensic classification and forensic characterisation of war crimes. This connection is due to the fact that these scientific tools make it possible to identify typical elements of a criminal event, identify its characteristic features and formulate a unified approach to the analysis of this category of offences, considering their division into relevant groups, types and subtypes. In turn, these elements are components of the subject matter of proof, as they reflect both the circumstances that characterise the methods of committing war crimes and the peculiarities of their detection, recording and investigation within a particular event.

The special qualifying circumstances of war crimes are notable. This refers to cases when authorised participants in an armed conflict who are vested with power (military and political leadership, commanders, military chiefs) give orders to their subordinates to commit acts contrary to the laws and customs of war. This is because such situations not only complicate the mechanism of qualification of an act but are also of fundamental importance for establishing individual responsibility within the collective execution of a criminal order. In this aspect, the main criterion for assessing the commission of a war crime within the process of proof is to establish the role of the relevant official in making a criminal decision that violates the laws and customs of war, the degree of participation of both this person and other participants in the armed conflict in their implementation, as well as the ability of law enforcement agencies to provide an adequate and admissible evidence base.

In further research, it is advisable to outline the forensic aspects of war crimes investigation. First, it is necessary to form a holistic forensic classification and forensic characterisation of violations of the laws and customs of war, which will ensure a unified approach to the collection, verification and evaluation of evidence during their investigation.

Acknowledgements

None.

Funding

The study was not funded.

Conflict of Interest

None.

References

[1] Agarkova, O. (2024). Detection and recording of violations of the laws and customs of war a direction of activity of law enforcement agencies. *Scientific Bulletin of the International Humanitarian University*, 68, 78-82. doi: 10.32782/2307-1745.2024.68.16.

[2] Antoniuk, N. (2023). Contextual element of war crimes: Content and necessity of establishment. *Law of Ukraine*, 5, 30-38. doi: 10.33498/louu-2023-05-030.
[3] Batiuk, O., & Dmytriv, S. (2021). On the issues of organizing investigations of war crimes. *Social and Legal Studies*, 4(3), 77-87. doi: 10.32518/2617-4162-2021-3-77-87.
[4] Caianiello, M. (2022). The role of the EU in the investigation of serious international crimes committed in Ukraine. Towards a new model of cooperation? *European Journal of Crime, Criminal Law and Criminal Justice*, 30(3-4), 219-237. doi: 10.1163/15718174-30030002.
[5] Compliance with global rights. (2016). *Basic standards of investigation for employees of the rapid response service in the investigation of international crimes*. Retrieved from https://surl.li/bjuxnp.
[6] Hlovyuk, I., & Teteryatnyk, G. (2022). Contextual elements in war crimes proceedings: A sui generis subject of proof. *Legal Scientific Electronic Journal*, 6, 394-398. doi: 10.32782/2524-0374/2022-6/87.
[7] Hryha, M., & Burnos, O. (2024). Documenting the ill-treatment of prisoners of war and civilians: Complications and challenges. *Bulletin of the Luhansk State University of Internal Affairs named after E. Didorenko*, 1(105), 266-275. doi: 10.33766/2786-9156.105.266-279.
[8] Khavroniuk, M. (2022). Criminal law norms designed for application in wartime conditions, in force before the start of open Russian aggression against Ukraine: Achievements and miscalculations of Ukrainian legislation and law enforcement practice. In *Ukrainian criminal justice in wartime conditions: Materials of the VIII (XXI) Lviv Criminal Justice Forum* (pp. 246-257). Lviv: Lviv State University of Internal Affairs.
[9] Kornev, O. (2022). Problematic issues of ensuring the investigation of war crimes against civilians during the armed aggression of the Russian Federation against Ukraine. In *Issues of documentation, determination of damage and compensation for losses caused to Ukraine and its citizens as a result of the armed aggression of the Russian Federation: Proceedings of the scientific and practical conference* (pp. 76-79). Kharkiv: New Law University named after Ya. Mudry.
[10] Kovalenko, A. (2022). Some legal and organizational problems of collecting, researching and using evidence during the investigation of criminal offenses under martial law. In *Issues of documentation, determination of damage and compensation for losses caused to Ukraine and its citizens as a result of armed aggression of the Russian Federation: Proceedings of the scientific and practical conference* (pp. 114-117). Kharkiv: New Law University named after Ya. Mudry.
[11] Kozmenko, A., Lebid, V., & Krapyvin, E. (2023). *International crimes in Ukraine: A review of national investigation and judicial practice*. Kyiv: Ukrainian Helsinki Human Rights Union.
[12] Kravchuk, O., & Bondarenko, M. (2022). *Pre-trial investigation of war crimes*. Retrieved from https://ela.kpi.ua/handle/123456789/46805.
[13] Lazareva, D. (2025). Evidence in criminal proceedings regarding war crimes. *Legal Scientific Electronic Journal*, 1, 483-486. doi: 10.32782/2524-0374/2025-1/111.
[14] Lebeniuk, A., & Osypenko, I. (2024). Pre-trial investigation of war crimes in Ukraine: Standards, risks to personal life and health. *Scientific Bulletin of Uzhhorod National University*, 86(5). 95-100. doi: 10.24144/2307-3322.2024.86.5.13.
[15] Novrotskyi, V. (2022). General, special and casuistic components of criminal offenses against the foundations of national security of Ukraine. *Law of Ukraine*, 11, 12-23. doi: 10.33498/louu-2022-11-012.
[16] Pchelina, O., & Pchelin, V. (2022). Forensic classification of war crimes. In *Modern trends in the development of forensics and criminal process in martial law: Proceedings of the scientific and practical conference* (pp. 334-338). Kharkiv: KhNUVS.
[17] Repetskyi, V., & Lysyk, V. (2009). Concepts and signs of war crimes. *Almanac of International Law*, 1, 120-125.
[18] Rubanenko, N. (2024a). Concept, typology and characteristics of international crimes: Systematic analysis. *Forum of Law*, 79(2), 84-95. doi: 10.5281/zenodo.10933562.
[19] Rubanenko, N. (2024b). Conceptual foundations of international judicial proceedings. *Scientific Bulletin of the Kharkiv National University of Internal Affairs*, 2(105), 160-175. doi: 10.32631/v.2024.2.38.
[20] Shevchyshyna, K. (2024). *Investigation of war crimes in Ukraine*. (PhD Dissertation, Research Institute of Public Law, Kyiv, Ukraine).
[21] Shulzhenko, A. (2022). Problems of proving the objective side in crimes of violation of the laws and customs of war. *Bulletin of the Luhansk State University of Internal Affairs named after E.O. Didorenko*, 2(98), 261-270. doi: 10.33766/2524-0323.98.261-270.
[22] Sichko, S. (2019). Current issues of criminal investigation. *South Ukrainian Legal Journal*, 1, 32-35. doi: 10.32850/sulj.2019.1-8.
[23] Szalai, A., & Blerta, A. (2025). The intersection of justice and European Union integration: War crimes adjudication in Kosovo. *Balkans Legal, Economic and Social Studies (BLESS)*, 2(1), 36-49. doi: 10.14232/bless.2025.1.36-49.
[24] Tan, Yu., & Yang, S. (2023). The Joint Investigation Team in Ukraine: An opportunity for the International Criminal Court? *Chinese Journal of International Law*, 1(22), 103-119. doi: 10.1093/chinesejil/jmad005.

[25] Taran, O. (2022). Circumstances subject to proof during the investigation of violations of the laws and customs of war. *Legal Scientific Electronic Journal*, 7, 413-416. doi: 10.32782/2524-0374/2022-7/100.

[26] Yankovyi, M. (2023). Investigation of criminal offenses committed by military personnel during an armed conflict: Problem statement. *Academic Visions*, 18. doi: 10.5281/zenodo.7795218.

[27] Yefimenko, T. (2024). Peculiarities of proof in criminal proceedings concerning war crimes. *Bulletin of the Criminological Association of Ukraine*, 3(33), 284-294. doi: 10.32631/vca.2024.3.25.

Обставини, що підлягають встановленню в провадженнях за фактом порушення законів і звичаїв війни

Наталія Рубаненко

Аспірант
Національна академія внутрішніх справ
03035, пл. Солом'янська, 1, м. Київ, Україна
https://orcid.org/0009-0001-2958-4228

Анна Мировська

Кандидат юридичних наук, професор
Національна академія внутрішніх справ
03035, пл. Солом'янська, 1, м. Київ, Україна
https://orcid.org/0000-0001-5714-1873

Анотація

Актуальність дослідження зумовлена необхідністю вдосконалення методології доказування в кримінальних провадженнях за фактом порушення законів і звичаїв війни. Увагу зосереджено на диспозиції ст. 438 Кримінального кодексу України, відповідно до якої слід звертатися до норм міжнародного гуманітарного і кримінального права. Метою дослідження було визначення структури предмета доказування у справах про воєнні злочини, виявлення його особливостей з огляду на принцип компліментарності, а також розроблення криміналістичної класифікації та характеристики відповідних діянь. Методологічний інструментарій охоплював системно-структурний, порівняльно-правовий, формально-юридичний методи, контент-аналіз судової практики й індуктивний аналіз, який дав змогу сформулювати теоретичні узагальнення на основі вивчення конкретних кримінальних проваджень. Практичну основу дослідження становив аналіз рішень національних судів першої та апеляційної інстанцій у справах, що стосуються вчинення воєнних злочинів на території України. Встановлено, що процес доказування має подвійну природу. Він охоплює, з одного боку, обставини, передбачені кримінальним процесуальним законодавством, а з іншого – факти, які є ключовими для кваліфікації діянь як міжнародних злочинів, учинених у межах збройного конфлікту та які мають прямий зв'язок з ним. У цьому контексті розслідування воєнних злочинів характеризується підвищеним рівнем складності, яку умовно можна диференціювати на дві групи. Першу групу становлять обставини об'єктивного характеру, що не підлягають впливу з боку органів досудового розслідування. Другу групу формують негативні чинники, на які можна вплинути в межах кримінального провадження для мінімізації їх наслідків. У цьому аспекті виявлено типові елементи, що підлягають встановленню під час розслідування порушень законів і звичаїв війни. Обґрунтовано доцільність доповнення ст. 438 Кримінального кодексу України кваліфікуючими обставинами, що конкретизують її зміст. Наукова і практична значущість одержаних результатів полягає у формуванні уніфікованого підходу до аналізу, перевірки й оцінки доказової інформації у справах про воєнні злочини, а також розробленні криміналістичної класифікації та криміналістичної характеристики таких правопорушень задля формування уніфікованої методики розслідування порушень законів і звичаїв війни

Ключові слова:

воєнні злочини; предмет і межі доказування; контекстуальні обставини; збройний конфлікт; міжнародне гуманітарне право; міжнародне кримінальне право; криміналістична характеристика; криміналістична класифікація

UDC 343.3+343.9(594)
DOI: 10.63341/naia-chasopis/3.2025.82

From retribution to humanity: Adapting the "rarest of the rare" doctrine in Indonesian criminal law

Erwin Susilo*
Doctoral Student
Syiah Kuala University
24415, 1 Tgk. Hasan Krueng Kalee Str., Banda Aceh, Republic of Indonesia
https://orcid.org/0009-0000-9990-8112

Abstract
This study examined the legal relevance and urgency of applying the Rarest of the Rare doctrine within the Indonesian criminal justice system as a limiting principle on judges' authority to impose the death penalty. Law No. 1 of 2023 brings fundamental changes by no longer categorising the death penalty as a primary punishment but rather as an alternative special punishment subject to strict substantive and procedural requirements. This research employed a normative legal research method through statutory, conceptual, and comparative approaches and refers to several jurisprudences of the Supreme Court of India, such as in the case of Bachan Singh v. State of Punjab. This doctrine requires that the death penalty be imposed only in extremely exceptional cases with a high level of brutality, demonstrating moral depravity, and when the rehabilitation of the perpetrator is deemed impossible. This research recommended the establishment of judicial guidelines in Indonesia to limit judicial discretion, ensure accountability of decisions, and align penal practices with the values of Pancasila and the theory of dignified justice. This doctrine was proposed as a filtering mechanism so that the death penalty is applied only as an *ultimum remedium* in a proportional, cautious, and humane manner to protect the right to life and reflect a more just and humane direction in criminal law policy

Keywords:
death penalty; rarest of the rare; judge; dignified justice; Pancasila

Introduction

The death penalty is one of the heaviest types of punishment regulated in the Indonesian legal system. In the constitutional system, judges hold a strategic role as independent and autonomous actors of the judiciary in upholding law and justice, as emphasised in Article 24 paragraph (1) of the 1945 Constitution of the Republic of Indonesia (Indonesian Constitution)[1]. Based on this constitutional mandate, judges have the discretion to impose sentences on defendants who are proven by law and convincingly to have committed a crime. However, the Indonesian Constitution also guarantees a very fundamental right for every citizen, namely the right to live. This is reflected in Article 28A, which states that everyone has the right to live and to defend their life and livelihood. Furthermore, Article 28H paragraph (1) emphasises the right to a prosperous life and a satisfactory living environment, while Article 28I paragraph (1) mentions that the right to live is a human

[1] Constitution of the Republic of Indonesia. (1945, August). Retrieved from https://www.dpr.go.id/jdih/uu1945.

Article's History:
Received: 12.04.2025
Revised: 04.09.2025
Accepted: 29.09.2025

Suggest Citation:
Susilo, E. (2025). From retribution to humanity: Adapting the "rarest of the rare" doctrine in Indonesian criminal law. *Law Journal of the National Academy of Internal Affairs*, 15(3), 82-91. doi: 10.63341/naia-chasopis/3.2025.82.

*Corresponding author

right that cannot be reduced under any circumstances. In the old Indonesian Penal Code[1] (IPC), the death penalty was established as the primary punishment and occupied the first position in the list of types of punishments, as stated in Article 10. However, in the new IPC[2] based on Law of the Republic of Indonesia No. 1 of 2023, which will come into effect in 2026, the death penalty is no longer categorised as a primary punishment but rather as a special punishment, as regulated in Article 67.

Various previous studies have shown that the death penalty is a complex and controversial legal issue in relation to human rights and Indonesia's social dynamics. Law No. 1 of 2023[3] introduces a death penalty scheme with a 10-year probation period, during which the sentence can be converted to imprisonment if the convicted person demonstrates good behaviour. The legislation reflects a compromise position that seeks to bridge the debate between pro and contra groups while aligning with the values of human rights and Islamic law (Tongat, 2024). Islamic law, in this case, is considered to have a significant influence on the formulation of the death penalty policy in Indonesia because it prioritises the principle of balanced justice and deterrence against serious criminals. One of the issues that has sparked sharp controversy is the application of the death penalty to drug offenders. This practice often receives criticism, for example in study S. Suyatno & H. Yusuf (2023), because it is considered to violate the right to life and is deemed cruel. Nevertheless, some circles still view the death penalty as legitimate to apply to safeguard public interest, as long as it is carried out in accordance with legal provisions. In comparative research with China I.K. Duan & M.D. Susilawati (2023) showed that, although both countries still retain the death penalty in their legal systems, Indonesia has positioned it as a special punishment within the framework of Law No. 1 of 2023. On the other hand, there is an urgent need to reform the penal system so that Indonesia's legal system aligns with the dynamics of social values and the development of international law. One form of this reform is the introduction of the concept of the conditional death penalty as a compromise between the retributive and rehabilitative approaches. На думку J. Cahyono & F. Santiago (2023), in this framework the death penalty is no longer regarded as the primary punishment but rather as a last resort when rehabilitation is no longer possible. As indicated in the study by P. Riyadi (2023), the debate between guaranteeing the right to life in the constitution and the continued existence of the death penalty persists, further complicated by execution-related issues that generate legal uncertainty and conflicts among law enforcement institutions (Sidabukke, 2023). According to D.R. Dewanto & R. Susanti (2023), although Law No. 1 of 2023 embodies a spirit of reform, the death penalty remains a significant subject of reflection within the context of human rights and the nation's fundamental ethical values.

However, among all the studies, none have explicitly examined and compared the application of the death penalty in Indonesia with the "rarest of the rare" doctrine used in criminal law in India. The "rarest of the rare" doctrine in India is a principle of very strict limitation on the use of the death penalty, which can only be imposed under the most extraordinary conditions, when the crime committed reaches a level of brutality or moral repugnance that is extremely high and rehabilitation, as stated M. Deshpande & S. Gurpur (2023), is deemed impossible. This doctrine serves as an important guideline for judges in India in determining the proportional and cautious imposition of the death penalty (Phulwary, 2018).

Judges, as the last bastion of justice, hold a moral and constitutional responsibility in deciding someone's life (Widijowati & Adji, 2020). Therefore, clear, careful, and justice-oriented guidelines are needed in imposing the death penalty. In this context, it is important to build a relevant concept for judges in Indonesia by adopting best practices from India through the "rarest of the rare" doctrine. This research aims to address two issues: first, the regulation and application of the "rarest of the rare" doctrine within the Indian legal system; and second, how this doctrine can be normatively and practically adapted for use by judges in Indonesia. Thus, the aim of this research lied in the effort to build a more measured and cautious framework for the death penalty in Indonesia by drawing lessons from practices in India that have developed mechanisms to limit the death penalty through the Rarest of the Rare doctrine. This approach has not been comprehensively discussed in previous studies, and it is expected to contribute to the formulation of a more just criminal law policy in line with Pancasila as the philosophy of the Indonesian nation.

Materials and Methods

This study employed a normative legal research method using three complementary approaches: statutory, conceptual, and comparative. The statutory approach was used to examine the formulation and positioning of the death penalty under Indonesian criminal law, particularly the transformation under Law of the Republic

[1] Penal Code of Indonesian. (1915, May). Retrieved from https://peraturan.bpk.go.id/Details/44289/kuhp.
[2] Law of the Republic of Indonesia No. 1 "On Criminal Code". (2023, January). Retrieved from https://peraturan.bpk.go.id/Details/226204/uu-no-1-tahun-2023.
[3] Ibidem, 2023.

of Indonesia Number 1 of 2023[1]. This included analysis of relevant provisions such as Articles 64, 65, 67, 98, and 100, which reclassify the death penalty as a special and conditional punishment. The statutory analysis served as a foundation to identify the legal status and constraints of the death penalty in the Indonesian criminal code reform.

The conceptual approach was employed to examine the underlying philosophical and normative principles that govern the imposition of the death penalty. This included an in-depth analysis of the "Theory of dignified justice" developed by T. Prasetyo (2019), which positions human dignity as the core of legal reasoning, balancing legal certainty, justice, and utility. This approach was crucial for assessing whether Indonesia's evolving penal policy aligns with Pancasila values and international human rights standards. Key concepts such as *ultimum remedium*, individualisation of punishment, and restorative justice are critically explored within this framework.

The comparative approach was utilised to examine the Indian "rarest of the rare" doctrine through case law analysis and jurisprudence from the Supreme Court of India. Seminal cases such as Bachan Singh v. State of Punjab[2], Santosh Kumar Bariyar v. State of Maharashtra[3], and Manoj v. State of Madhya Pradesh[4] are scrutinised to extract applicable criteria and judicial reasoning that could inform Indonesian legal practice. The aim was to assess the feasibility of adopting such a doctrine to limit judicial discretion and ensure proportional sentencing. The research methodology followed a systematic sequence. First, identified the doctrinal shift in Indonesian criminal law. Second, was analysed the philosophical justifications and normative values that underpin death penalty reforms. Third, was compared these findings with the Indian jurisprudential model. Finally, it offered normative recommendations for adapting the "rarest of the rare" doctrine in Indonesia. The uniqueness of the source base lied in the integration of two national legal systems (Indonesia and India), linked through shared constitutional commitments to the right to life but differentiated in their doctrinal and jurisprudential approaches to capital punishment. The inclusion of philosophical concepts such as dignified justice and restorative justice allowed this research to move beyond textual analysis and propose a transformative model of judicial sentencing.

Results

Regulation and implementation of the rarest of the rare doctrine in India. The term "rarest of rare" does not have an official definition in Indian legislation. Its meaning has evolved through the jurisprudence of the Supreme Court and is determined based on the facts and circumstances of each case, including the degree of brutality of the act, the character of the accused, their criminal history, and the possibility of rehabilitation (Rajkumari & Singh, 2022). Although normatively India limits the death penalty to extraordinary cases classified as "rarest of rare", court practices show that the death penalty is still imposed quite frequently, especially by first-instance courts. This phenomenon raises concerns about the consistency in the application of the doctrine. Since 1962, the Indian Law Commission has been discussing this issue. At that time, it was concluded that India was not yet ready to abolish the death penalty. However, in 2015, the Commission recommended abolishing the death penalty for general crimes while retaining it only for acts of terrorism and treason. One of the reasons underlying the recommendation is that the death penalty is final, irreversible, and highly susceptible to judicial errors (Rao & Sharma, 2022).

In India, judicial discretion plays a central role in imposing the death penalty because, prior to the existence of clear guidelines, verdicts heavily depended on the individual judgment of each judge. This has the potential to create inconsistencies that threaten the principle of justice. Through the ruling in Bachan Singh v. State of Punjab[5], the Supreme Court of India established that the death penalty can only be imposed in truly extreme situations and when there are no adequate alternative punishments. The "rarest of rare" doctrine was born to limit the judge's excessive discretion and reduce the chances of deviation (Jain, 2025).

The Court then reaffirmed this principle in Santosh Kumar Bariyar v. State of Maharashtra[6], stating that the death penalty is only an exception to the general principle of life imprisonment. The provision of Article 21 of the Indian Constitution[7], which guarantees the right

[1] Law of the Republic of Indonesia No. 1 "On Criminal Code". (2023, January). Retrieved from https://peraturan.bpk.go.id/Details/226204/uu-no-1-tahun-2023.
[2] Judgement of the Supreme Court of India in Case No. 273 "Bachan Singh v. State of Punjab". (1980, May). Retrieved from https://indiankanoon.org/doc/1235094/.
[3] Judgement of the Supreme Court of India in Case No. 1478 "Santosh Kumar Satishbhushan Bariyar v. State of Maharashtra". (2009, May). Retrieved from https://indiankanoon.org/doc/1312651/.
[4] Judgement of the Madhya Pradesh High Court in Case No. 4069 "Manoj v. The State Of Madhya Pradesh". (2025, May). Retrieved from https://indiankanoon.org/doc/113383276/.
[5] Judgement of the Supreme Court of Undia in Case No. 273 "Bachan Singh v. State of Punjab". (1980, May). Retrieved from https://indiankanoon.org/doc/1766147/.
[6] Judgement of the Supreme Court of India in Case No. 1478 "Santosh Kumar Satishbhushan Bariyar v. State of Maharashtra". (2009, May). Retrieved from https://indiankanoon.org/doc/1312651/.
[7] Constitution of India. (1950, January). Retrieved from https://legislative.gov.in/sites/default/files/COI_1.pdf.

to life, necessitates a highly selective and proportional application of the death penalty, considering its irrevocable nature (Jain, 2025). Problems arise when the application of that doctrine is not always consistent. In the Death Penalty India Report, it was found that many death sentences were given discriminatorily against marginalised groups – those who are poor, have low education, or come from minority communities (Rao & Sharma, 2022). During the investigation process, death row inmates often experience torture and do not receive timely legal assistance; additionally, their families become victims of pressure from the authorities (Rao & Sharma, 2022).

The Supreme Court of India reinforced caution in death penalty cases through the ruling in Mohd. Arif v. Registrar[1], which stipulated that petitions for review of the death penalty must be heard in open court, rather than merely through file examination. This decision is based on the principle that the death penalty is irreversible and has a direct implication on a person's right to life (Chaturvedi, 2023). An example of the application of this doctrine can be seen in the case of Ishwari Lal Yadav v. State of Chhattisgarh[2], where the perpetrator kidnapped and sacrificed a child in a mystical ritual. Because his crime was classified as extremely heinous and inhumane, the Court imposed the death penalty. On the other hand, in State of UP v. MK Anthony[3], the Court did not impose the death penalty because the perpetrator's actions were influenced by economic pressure and medical disturbances, resulting in a life imprisonment sentence. The Supreme Court of India has also classified crimes that can be categorised as the rarest of the rare into five groups:

- extreme cruelty that shocks the public conscience;
- the motive for the crime that indicates the moral depravity of the perpetrator;
- widespread social impact, such as genocide;
- large-scale criminal acts;
- the characteristics of the victims, such as children or the elderly.

Nevertheless, there are still many rulings that deviate from that principle. After Bachan Singh[4], many judges have used penological arguments such as deterrence and public morality as the main justification for imposing the death penalty. These arguments should only be used in the general discourse on the death penalty's existence, not as concrete reasons in case-by-case situations. This approach leads to a crime-centric penal system and neglects the principle of individualisation in punishment upheld by Bachan Singh.

The issue of inequality also arises in the context of gender, where it is found that domestic crimes or honour-based violence are often considered momentary deviations and forgiven, while crimes in public spaces are more quickly categorised as deserving of the death penalty. This reflects that a normatively neutral legal system actually reinforces structural inequalities if it does not take into account the vulnerabilities of certain groups (Chandra, 2012). In the case of Manoj v. State of Madhya Pradesh[5], the Court began to consider the potential for rehabilitating the offender before imposing the death penalty. Now, the task of evaluating the possibility of reform is entrusted to probation officers in accordance with the Probation of Offenders Act of 1958[6]. This step is considered an important reform in the practice of capital punishment, making it more humane and based on procedural justice (Bhaskar, 2023).

Historically, the implementation of the death penalty in India has deep roots. Since ancient times in India, the death penalty has been carried out to eliminate dangerous elements from society. During the British colonial period, although there were ideas about abolishing the death penalty, the colonial government continued to uphold it. After independence, Godse was sentenced to death for killing Mahatma Gandhi, and since then the death penalty has been strictly regulated in the Indian Penal Code[7] and the Code of Criminal Procedure[8].

The judges face a major dilemma when deciding on the death penalty. A wrong decision will have fatal consequences and cannot be corrected. Therefore, the Indian legal system provides various legal remedies such as appeals, review petitions, curative petitions, and clemency to the President or Governor. Many cases where the trial court imposed the death penalty have been overturned or commuted by the Supreme Court (Pattnaik & Shahi, 2024). However, a survey of Supreme Court decisions between 2000 and 2011, as examined by Deva,

[1] Judgement of the Supreme Court of India in Case No. 77 "Mohd. Arif Ashfaq v. The Reg. Supreme Court of India & Ors". (2014, September). Retrieved from https://indiankanoon.org/doc/80457116/.
[2] Judgement of the Supreme Court of India in Case No. 1095 "Ishwari Lal Yadav v. State of Chhattisgarh". (1978, January). Retrieved from https://indiankanoon.org/doc/51591697/.
[3] Judgement of the Delhi District Court in Case "State of U.P. v. M.K. Anthony". (1984, November). Retrieved from https://indiankanoon.org/doc/1381651/.
[4] Judgement of the Supreme Court of India in Case No. 273 "Bachan Singh v. State of Punjab". (1980, May). Retrieved from https://indiankanoon.org/doc/1766147/.
[5] Judgement of the Madhya Pradesh High Court in Case No. 4069 "Manoj v. The State Of Madhya Pradesh". (2025, May). Retrieved from https://indiankanoon.org/doc/113383276/.
[6] Law of India No. 20 "The Probation of Offenders Act". (1958, May). Retrieved from https://www.indiacode.nic.in/bitstream/123456789/15408/1/the_probation_of_offenders_act%2C_1958.pdf.
[7] Penal Code of India. (1860, October). Retrieved from https://www.indiacode.nic.in/repealedfileopen?rfilename=A1860-45.pdf.
[8] Code of Criminal Procedure (Amendment) Act of India. (2005, June). Retrieved from https://www.mha.gov.in/sites/default/files/2022-09/TheCCP%28Amendment%29Act%2C2005%5B1%5D.pdf.

shows that there is not always a consistent standard in imposing or rejecting the death penalty, thereby opening up excessive discretionary space. This shows that although the Supreme Court is viewed as progressive in Bachan Singh, in practice, there are still interpretative gaps (Deva, 2014). J. Diwakar's (2022) research proposes detailed criteria for applying this doctrine:

1) it should be applied only to extremely extraordinary crimes with extreme culpability;

2) the death penalty must be considered an exception, not the rule;

3) it should be imposed only if no other alternatives exist;

4) each case must be assessed individually and contextually;

5) there must be a balance between aggravating and mitigating factors;

6) the interpretation of mitigating factors should be broad, including potential for rehabilitation;

7) it is insufficient that the crime is rare; it must also exhibit extreme brutality.

Several other cases also demonstrate the flexibility of this doctrine. In Shankar Kisanrao Khade v. State of Maharashtra[1], the Court deemed that the severity of the crime did not meet the threshold of the rarest of rare, despite its cruelty. Conversely, in Deepak Rai v. State of Bihar[2] and Md. Mannan Abdul Mannan v. State of Bihar[3], the Court imposed the death penalty because there were no other alternatives and because the crime was truly heinous and deeply undermined human values.

Thus, the "rarest of the rare" doctrine in India has developed as a limiting principle rooted in jurisprudence and is used to ensure that the death penalty is imposed only in truly extreme conditions, when no other punishment is adequate. Through a series of important rulings, the Supreme Court of India emphasised the importance of a selective, proportional approach based on a thorough evaluation of the offender's character, the level of brutality of the crime, and the possibility of rehabilitation. This doctrine reflects the judges' prudence in imposing sentences and demonstrates the transformation of punishment toward a more humane and just approach.

The concept of the "rarest of the rare" doctrine is relevant for judges when imposing the death penalty in Indonesia. In the old Indonesian criminal justice system, the death penalty occupied the highest position as the main type of punishment, as stated in Article 10, letter a, of the IPC[4], a remnant of Dutch colonialism (Lumbanraja, 2023). This model of punishment assumes that the death penalty can be imposed on certain types of crimes normatively, without first undergoing a contextual assessment of proportionality elements, the background of the perpetrator, or rehabilitation opportunities. The pattern of punishment reflects a classical retributive approach that prioritises retribution for criminal acts (Clemens Dion, 2023).

However, this paradigm underwent a fundamental change with the enactment of Law No. 1 of 2023[5], which is the result of national codification based on the spirit of criminal law reform (Susilo, 2025). Law No. 1 of 2023 no longer categorises the death penalty as a primary punishment. Article 65, paragraph (1), of Law No. 1 of 2023 explicitly mentions five types of primary punishments, namely "imprisonment, confinement, supervision, fines, and community service". Meanwhile, the death penalty is classified as a special alternative punishment, as stated in Article 64, Letter C, and Article 67. This systematic change indicates a shift in orientation from retributive punishment to a more humanistic and corrective approach, which makes substantive justice and the protection of human rights the main pillars (Tri Setiawan & Kurnianingsih, 2023; Zulkipli, 2023). The placement of the death penalty as a conditional sanction – not a normative obligation – implies that its execution can only be carried out after a comprehensive evaluation of the perpetrator's circumstances and the impact of their crime.

Furthermore, Law No. 1 of 2023[6] introduces an important mechanism in the form of a probation period for the death penalty through Article 100 (Fitriani, 2023). This provision allows judges to impose the death penalty with a ten-year probation period in cases where there are mitigating circumstances such as the defendant's remorse, a non-dominant role in the crime, or the potential for rehabilitation. If during the probation period the convict shows exemplary behaviour, the death penalty can be commuted to life imprisonment through a Presidential Decree with consideration from the Supreme Court. Law No. 1 of 2023 also regulates the postponement of the death penalty execution under special conditions as stipulated in Articles 98 to 102, such as when the convict is pregnant, suffers from a mental disorder, or is applying for clemency. The execution of the death penalty must also not be carried out in public.

[1] Judgement of the Supreme Court of India in Case No. 362-363 "Shankar Kisanrao Khade v. State of Maharashtra". (2013, April). Retrieved from https://indiankanoon.org/doc/79577238/.
[2] Judgement of the Supreme Court of India in Case No. 249-250 "Deepak Rai v. State of Bihar". (2013, September). Retrieved from https://indiankanoon.org/doc/178668154/.
[3] Judgement of the Supreme Court of India in Case No. 308 "Md. Mannan Abdul Mannan v. State of Bihar". (2019, February). Retrieved from https://indiankanoon.org/doc/125632384/.
[4] Penal Code of Indonesian. (1915, May). Retrieved from https://peraturan.bpk.go.id/Details/44289/kuhp.
[5] Law of the Republic of Indonesia No. 1 "On Criminal Code". (2023, January). Retrieved from https://peraturan.bpk.go.id/Details/226204/uu-no-1-tahun-2023.
[6] Ibidem, 2023.

This normative framework aligns with the "rarest of the rare" doctrine developed by the Supreme Court of India in the case of Bachan Singh v. State of Punjab[1] (1980), which emphasises that the death penalty can only be imposed in cases that reach an extraordinary level of brutality and cruelty and when there are no adequate alternative punishments to fulfil the objectives of sentencing (Bharadwaj, 2021). This doctrine serves as a judicial filter to prevent the excessive and disproportionate use of the death penalty. It demands caution and a restrictive approach, which is consistent with the spirit of the 2023 Penal Code[2] in placing the death penalty as an *ultimum remedium* (Sulistiani & Fakhriah, 2023). Related to Indonesia, the application of the death penalty must be accompanied by a strict filtering mechanism to ensure that the judge's decision truly reflects justice. Therefore, the adoption of the "rarest of the rare" doctrine becomes relevant, both as a limiting principle in criminal justice practice and as a guideline for judges in drafting their decisions.

The Supreme Court needs to issue judicial guidelines or Supreme Court Regulations to ensure that the implementation of this doctrine has normative power and is operationalised consistently, providing judges with a practical basis for its application. In the guidelines, it must be emphasised that the death penalty can only be imposed if three cumulative conditions are met, namely: the crime committed has a very high degree of cruelty and shakes the collective conscience of society; the perpetrator shows no potential for rehabilitation, either socially or psychologically, based on an objective and scientific assessment; all other forms of punishment are deemed incapable of achieving the goals of justice, security, and protection for society.

Practically, the application of this doctrine requires the use of a multifactorial assessment approach by judges (Gunawardena *et al*., 2017), which includes analysis of (a) the personal character of the perpetrator, including age, psychological condition, and socio-economic background; (b) the characteristics of the crime, including modus operandi, escalation of violence, and impact on victims and society; and (c) the vulnerability of the victim related to power relations, age, or physical condition. All these elements must be analysed based on objectively testable data, not just the judge's opinion.

In the procedural dimension, it is very important to form a rehabilitative assessment team consisting of community supervisors, forensic psychologists, and criminal law experts. This team is tasked with preparing a pre-sentencing report, which is an instrument that must be considered by the judge when imposing the death penalty. Judges must publicly state, based on the report, that all other forms of punishment have been considered but deemed insufficient to achieve substantive justice. To ensure judicial accountability and public control, every death penalty ruling must include detailed, argumentative, and evidence-based legal reasoning that explicitly explains why the case falls into the "rarest of the rare" category.

The above concept is in line with the Indonesian nation, which cannot be separated from the values of Pancasila and the living legal character in society (Wijayanto, 2022). Therefore, appreciation for community-based conflict resolution mechanisms such as forgiveness from the victim's family or customary-based penal mediation can be considered as long as they do not contradict public interest and the principle of justice. This approach reflects the importance of considering sociocultural aspects in sentencing without diminishing the authority of national law. Thus, the "rarest of the rare" doctrine can serve as a substantive standard in assessing the appropriateness of the death penalty and as an embodiment of the principle of dignified justice. It prioritises life above all else, allowing it to be sacrificed only in extreme situations. Law No. 1 of 2023 changes the position of the death penalty to conditional and special penalties, reflecting the transformation of Indonesian legal values towards a more just direction (Andriawan, 2022). In this case, the role of judges becomes very central as protectors of the fundamental values of Pancasila, especially the first principle about the One and Only God (Syahlin *et al*., 2024) and the second principle regarding Just and Civilised Humanity (Prasetyo & Wartoyo, 2021). The law should not merely be a formalistic instrument but must be able to honour humans as legal subjects (Prasetyo, 2019). Therefore, the death penalty must truly be an *ultimum remedium* imposed only in extreme cases that tear apart the sense of collective justice.

In this case, the "Theory of dignified justice" developed by T. Prasetyo (2019) provides a strong philosophical foundation. This theory, as elaborated in his book and further examined in collaborative studies such as E. Sukardi *et al*. (2021), emphasises that law must balance legal certainty, justice, and utility by placing the human person at its centre. T. Prasetyo (2019) rejects the rigid positivistic paradigm that relies solely on normative texts and instead promotes a legal framework that integrates the moral, ethical, and spiritual values inherent in Indonesian society. In penal practice, particularly regarding the death penalty, this theory urges judges to go beyond formal legality by considering broader humanistic and spiritual dimensions. Applying the "rarest of the rare" doctrine in the spirit of the Theory transforms the death penalty from a mechanistic form of punishment into a reflection of judicial

[1] Judgement of the Supreme Court of India in Case No. 273 "Bachan Singh v. State of Punjab". (1980, May). Retrieved from https://indiankanoon.org/doc/1766147/.
[2] Law of the Republic of Indonesia No. 1 "On Criminal Code". (2023, January). Retrieved from https://peraturan.bpk.go.id/Details/226204/uu-no-1-tahun-2023.

prudence, social responsiveness, and respect for human dignity, which aligns with the Pancasila-based Indonesian legal system. Judges who embody these considerations are thus expected to deliver decisions that uphold justice as a profoundly humanistic ideal.

Discussion

This study demonstrates the relevance and urgency of adopting the "rarest of the rare" doctrine as a guiding principle in the application of the death penalty in Indonesia. The transformation initiated by Law of the Republic of Indonesia Number 1 of 2023 on the Criminal Code[1] marks a substantial shift in the legal policy regarding capital punishment, wherein the death penalty is no longer considered a primary punishment but is repositioned as a special and conditional sanction. In contrast to Indonesia's statutory approach, the doctrine in India emerged from jurisprudential development, particularly through the seminal case of Bachan Singh v. State of Punjab[2], which restricted the death penalty to cases of extreme brutality and irredeemable offenders. This judicially created filter was later reaffirmed in other cases such as Santosh Kumar Bariyar v. State of Maharashtra[3] and Manoj v. State of Madhya Pradesh[4], stressing the exceptional nature of the death penalty and the need for individualised sentencing assessments. However, empirical studies such as the Death Penalty India Report revealed inconsistent applications and discriminatory tendencies, especially against marginalised groups (Rao & Sharma, 2022). Unlike India, where judicial discretion historically dominated sentencing in capital cases, Indonesia now has the opportunity to codify a coherent filtering mechanism through Articles 64, 65, and 100 of Law No. 1 of 2023[5]. The law introduces a 10-year probation period for death row convicts, allowing sentence conversion to life imprisonment upon demonstration of good behaviour. This structure inherently reflects the values of justice, humanity, and legal proportionality, aligning with A. Bharadwaj's (2021) interpretation of Bachan Singh as a framework of restraint, not vengeance.

The Indonesian approach is also philosophically grounded in the "Theory of dignified justice" developed by T. Prasetyo (2019), which centres legal decision-making on human dignity, moral responsibility, and the balance of justice, certainty, and utility. This differs from India's secular jurisprudence, where proportionality is viewed primarily through a liberal-legalist lens. The author's claims in the Indian context seem to be debatable because they often ignore spiritual and cultural elements that are essential in Indonesian legal philosophy. In implementing this doctrine, the creation of a rehabilitative assessment team is essential. Judges should not rely solely on their perception of remorse or potential for rehabilitation. As practiced in India following Manoj v. State of Madhya Pradesh[6], evaluation must be conducted by trained professionals under the Probation of Offenders Act, 1958[7]. In Indonesia, the introduction of similar mechanisms would improve the credibility of pre-sentencing reports and minimize judicial arbitrariness. S.A. Gunawardena *et al*. (2017) similarly argue for a multidisciplinary approach, incorporating forensic, social, and psychological evaluations.

Nonetheless, caution is necessary. In India, the misuse of penological justifications – such as deterrence and public morality – has often overshadowed individualised assessments (Surendranath *et al*., 2019). This is not consistent with the results of this study because the Indonesian model, based on Law No. 1 of 2023[8] and dignified justice, explicitly discourages automatic or mechanistic reasoning. The reason for the different interpretations may lie in the greater normative clarity offered by statutory reform compared to India's fragmented jurisprudence. Furthermore, this study supports A. Chandra's (2012) findings on the gender bias in Indian capital sentencing. Crimes against women in domestic contexts were frequently trivialised, while public crimes were deemed more deserving of the death penalty. In Indonesia, this highlights the need to incorporate sociological vulnerability assessments into the guidelines. The conclusions drawn by the researcher are quite appropriate, because, as the results of this study show, neutrality in law must not ignore structural inequalities. To operationalise the doctrine effectively, the Indonesian Supreme Court should issue a Supreme Court Regulation defining strict, cumulative criteria for death penalty cases: (1) the crime must involve extreme cruelty shocking the public conscience, (2) the

[1] Law of the Republic of Indonesia No. 1 "On Criminal Code". (2023, January). Retrieved from https://peraturan.bpk.go.id/Details/226204/uu-no-1-tahun-2023.
[2] Judgement of the Supreme Court of India in Case No. 273 "Bachan Singh v. State of Punjab". (1980, May). Retrieved from https://indiankanoon.org/doc/1766147/.
[3] Ibidem, 1980.
[4] Judgement of the Madhya Pradesh High Court in Case No. 4069 "Manoj v. The State Of Madhya Pradesh". (2025, May). Retrieved from https://indiankanoon.org/doc/113383276/.
[5] Law of the Republic of Indonesia No. 1 "On Criminal Code". (2023, January). Retrieved from https://peraturan.bpk.go.id/Details/226204/uu-no-1-tahun-2023.
[6] Judgement of the Madhya Pradesh High Court in Case No. 4069 "Manoj v. The State Of Madhya Pradesh". (2025, May). Retrieved from https://indiankanoon.org/doc/113383276/.
[7] Law of India No. 20 "The Probation of Offenders Act". (1958, May). Retrieved from https://www.indiacode.nic.in/bitstream/123456789/15408/1/the_probation_of_offenders_act%2C_1958.pdf.
[8] Law of the Republic of Indonesia No. 1 "On Criminal Code". (2023, January). Retrieved from https://peraturan.bpk.go.id/Details/226204/uu-no-1-tahun-2023.

perpetrator must demonstrate no potential for rehabilitation, and (3) no other punishment must be adequate to achieve justice and social protection. These criteria reflect J. Diwakar's (2022) proposal for a structured and contextualised application of capital punishment.

All of this is consistent with the philosophy of Pancasila and the Indonesian legal tradition that integrates community values and local wisdom. Incorporating elements such as forgiveness by the victim's family, customary reconciliation, and restorative measures would enhance legitimacy without weakening state authority (Wijayanto, 2022). Such hybridisation of justice reflects a broader humanistic commitment, similar to th e intention behind Article 10 of the Indonesian Penal Code[1] in the past, albeit now reformulated under Law No. 1 of 2023[2]. In sum, the Indonesian legal system is currently positioned to adopt a more structured and principled application of the death penalty. The adoption of the "rarest of the rare" doctrine – adjusted for Indonesia's normative landscape – can serve as both a judicial filter and a moral compass. This convergence of comparative jurisprudence and indigenous legal philosophy signifies a shift from punitive retribution to justice that humanises.

Conclusions

This Article focused on the relevance and possible adaptation of the rarest of the rare doctrine from India into the Indonesian criminal justice system, particularly in the context of imposing the death penalty. The study aimed to evaluate whether such a doctrine could serve as a limiting principle aligned with the recent penal reforms in Indonesia as stipulated in Law No. 1 of 2023. Through a normative and comparative legal analysis, the Article explored how the Indian model – especially as articulated in the Bachan Singh v. State of Punjab case – constructs a highly restrictive framework for the death penalty based on three critical criteria: the brutality of the act, the character of the offender, and the prospects of rehabilitation.

At each stage, the study examined the philosophical, doctrinal, and judicial underpinnings of the rarest of the rare doctrine in India, then contrasted them with the Indonesian penal structure, which is currently undergoing transformation toward a more humane and rehabilitative approach. This included an assessment of Indonesia's evolving legislative intent and judicial trends, which increasingly emphasise the dignity of the accused and the proportionality of punishment. It was found that the Indian doctrine offers a structured method for ensuring that capital punishment is not imposed arbitrarily but only in exceptionally extreme circumstances, thus aligning with the goals of penal moderation and human rights. The findings suggested that the conceptual core of the "rarest of the rare" doctrine – namely, restricting judicial discretion through objective criteria – provides significant insights for Indonesian judges navigating capital cases under the new Criminal Code. The analysis deepens the understanding of how comparative legal doctrines can be selectively adapted to strengthen safeguards against disproportionate sentencing and to promote a justice system grounded in humanity and restraint.

Future research could explore the practical integration of this doctrine into Indonesian jurisprudence, especially through judicial training and guideline development. It is also necessary to examine how this adaptation would interact with Indonesia's cultural, legal, and political context, including its constitutional provisions and human rights commitments. A limitation of this study is the absence of comprehensive empirical data on judicial attitudes toward the death penalty in Indonesia, as well as the restricted access to certain unpublished case decisions that might have enriched the comparative dimension of the analysis.

Acknowledgements

None.

Funding

The study was not funded.

Conflict of Interest

None.

References

[1] Andriawan, W. (2022). Pancasila perspective on the development of legal philosophy: Relation of justice and progressive law. *Volksgeist: Jurnal Ilmu Hukum Dan Konstitusi*, 5(1). doi: 10.24090/VOLKSGEIST.V5I1.6361.

[2] Bhaskar, A. (2023). Chances of reform as a mitigating factor in death penalty cases in India: Issues and challenges. *Indian Journal of Law and Justice*, 14(2).

[3] Cahyani, G.T., Bilkis Sholehah, S., Salsabillah, D.N., Ramadhana, M.A., Pratama, R.A., & Antoni, H. (2023). Analysis of the death penalty in Indonesia from a human rights perspective and alternative legal enforcement. *Jurnal Universitas Muhammadiyah Jakarta*, 7(1), 167-184.

[4] Cahyono, J., & Santiago, F. (2023). Reconstruction of conditional death penalty norms in the perspective of renewing Indonesian criminal law. *Edunity: Kajian Ilmu Sosial Dan Pendidikan*, 2(1), 47-55. doi: 10.57096/edunity.v1i05.35.

[1] Penal Code of Indonesian. (1915, May). Retrieved from https://peraturan.bpk.go.id/Details/44289/kuhp.
[2] Law of the Republic of Indonesia No. 1 "On Criminal Code". (2023, January). Retrieved from https://peraturan.bpk.go.id/Details/226204/uu-no-1-tahun-2023.

[5] Chandra, A. (2012). Gender dimensions of the death penalty in India. *SSRN Electronic Journal*. doi: 10.2139/ssrn.1617603.
[6] Chaturvedi, A. (2023). *The rarest of the rare*. Retrieved from https://pure.jgu.edu.in/id/eprint/6184/1/Delhi---The-Statesman-06-04-2023-page-11.pdf.
[7] Clemens Dion, Y.T. (2023). An appreciation of the amendment to the death penalty provisions. *Diskursus – Jurnal Filsafat Dan Teologi STF Driyarkara*, 19(2), 234-256. doi: 10.36383/diskursus.v19i2.376.
[8] Deshpande, M., & Gurpur, S. (2023). Connecting the dots in "rarest of rare": Is judicial discretion the perfection of reason? Tracking judicial discretion in death penalty cases in India. *Cardiometry*, 360-365. doi: 10.18137/cardiometry.2022.25.360367.
[9] Deva, S. (2014). Death penalty in the "rarest of rare" cases: A critique of judicial choice-making. In *Confronting capital punishment in Asia* (pp. 238-286). Oxford: Oxford Academic Press. doi: 10.1093/acprof:oso/9780199685776.003.0014.
[10] Dewanto, D.R., & Susanti, R. (2023). The death penalty under Law No. 1 of 2023 on the Indonesian Criminal Code: A human rights perspective. *Wijayakusuma Law Review*, 5(1), 64-70. doi: 10.51921/wlr.v5i1.239.
[11] Diwakar, J. (2022). The court of bigotry: Contested sexuality of dalit and non-dalit women. *Contemporary Voice of Dalit*, 14(2), 199-211. doi: 10.1177/2455328X221106537.
[12] Duan, I.K., & Susilawati, M.D. (2023). The death penalty for corruption offenders in China and Indonesia (a comparative study). *International Journal of Social Science and Human Research*, 6(11), 6791-6797. doi: 10.47191/ijsshr/v6-i11-30.
[13] Fitriani, F. (2023). The imposition of the death penalty on criminal offenders under Law No. 1 of 2023 on the Indonesian Criminal Code. *SENTRI: Jurnal Riset Ilmiah*, 2(8), 3016-3024. doi: 10.55681/sentri.v2i8.1327.
[14] Gunawardena, S.A., Liyanage, U.A., Weeratna, J.B., Mendis, N.D.N.A., Perera, H.J.M., Jayasekara, R.W., & Fernando, R. (2017). Forensic age estimation in anti-piracy trials in Seychelles: Experiences and challenges faced. *Forensic Science International*, 270, 278.e1-278.e7. doi: 10.1016/j.forsciint.2016.11.010.
[15] Jain, Y. (2025). *Life or death: Capital punishment in India*. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5283267.
[16] Lumbanraja, B. (2023). A holistic analysis of moral offenses punishable by death in Indonesia from the perspective of human rights, Pancasila, and the moral ethics of Saint Thomas Aquinas. *Fiat Iustitia: Jurnal Hukum*, 3(2), 177-188. doi: 10.54367/fiat.v3i2.2533.
[17] Pattnaik, A., & Shahi, S.K. (2024). Death penalty in India: A review with sample cases. In *Sustainability and equity: Economic democracy and social empowerment*. New York: Nova Science Publisher. doi: 10.52305/NHGZ0466.
[18] Phulwary, D. (2018). Criminological study of death penalty and ways to remove discrimination in death award. *SSRN Electronic Journal*. doi: 10.2139/ssrn.2481602.
[19] Prasetyo, T. (2019). *Dignified justice from a legal theory perspective*. Bandung: Nusamedia.
[20] Prasetyo, T., & Wartoyo, F. X. (2021). Understanding Indonesian electronic data law through dignified justice theory. *Journal of Legal, Ethical and Regulatory Issues*, 24(1).
[21] Rajkumari, & Singh, R.D.P. (2022). "The doctrine of rarest of rare": A critical analysis. *Indian Journal of Integrated Research in Law*, 2(4), 676-683. doi: IJIRL/V2-I4/A64.
[22] Rao, R.V., & Sharma, P. (2022). *Death sentence in India: Is it rare yet arbitrary?* Retrieved from https://www.project39a.com/dpir.
[23] Riyadi, P. (2023). Construction of death penalty legal arrangements in Indonesia. *Journal of Political and Legal Sovereignty*, 1(1), 5-14. doi: 10.38142/jpls.v1i1.32.
[24] Sidabukke, S.M. (2023). Double punishment in the waiting time for death penalty: A study of human rights protection in Indonesia. *Lex Prospicit*, 1(1). doi: 10.19166/lp.v1i1.6634.
[25] Sukardi, E., Pasaribu, D., & Kwang, V.C. (2021). Efforts to address domestic violence triggered by COVID-19: A perspective from the dignified justice theory. *Jurnal Lemhannas RI*, 9(1), 11-24. doi: 10.55960/jlri.v9i1.373.
[26] Sulistiani, L., & Fakhriah, E.L. (2023). The effect of extra judicial settlement in criminal cases based on the principle of ultimum remedium. *Padjadjaran Jurnal Ilmu Hukum*, 10(3), 300-320. doi: 10.22304/pjih.v10n3.a1.
[27] Surendranath, A., Vishwanath, N., & Dash, P.P. (2019). Penological justifications as sentencing factors in death penalty sentencing. *Journal of National Law University Delhi*, 6(2), 107-125. doi: 10.1177/2277401720972852.
[28] Susilo, E. (2025). An analysis of the concept of the principle of legality in the New Indonesian Criminal Code: A legal certainty perspective. In B. Sujatmiko (Ed.), *Anthology of judicial studies* (pp. 1-19). Yogyakarta: CV. PUSTAKA HUKUM.

[29] Suyatno, S., & Yusuf, H. (2023). Death penalty for criminal actions in Indonesia in a legal perspective and human rights. *Journal of Social Research*, 2(9), 2925-2933. doi: 10.55324/josr.v2i9.1338.
[30] Syahlin, F.U., Andini, F.A., Lubis, M.A., & Usiono, U. (2024). Understanding the relationship between religion and the state. *IJEDR: Indonesian Journal of Education and Development Research*, 2(1), 515-518. doi: 10.57235/ijedr.v2i1.1822.
[31] Tongat. (2024). Death penalty in Indonesia: Between criminal law and Islamic law perspectives. *Legality: Jurnal Ilmiah Hukum*, 32(1), 90-104. doi: 10.22219/ljih.v32i1.32335.
[32] Tri Setiawan, W., & Kurnianingsih, M. (2023). Assessing community service sentences as a new paradigm of corruption punishment based on cultural determinism. *Justisi*, 9(2), 116-132. doi: 10.33506/jurnaljustisi.v9i2.2328.
[33] Widijowati, D., & Adji, R.P. (2020). Legal psychology of judges to determine the defendant's ability to commit a crime. *International Conference on Law, Economics and Health*, 140, 60-63. doi: 10.2991/aebmr.k.200513.012.
[34] Wijayanto, E. (2022). Autonomy, Sharia regional regulations, and living law in the Pancasila-based rule of law state. *Wicarana*, 1(2), 150-160. doi: 10.57123/wicarana.v1i2.24.
[35] Zulkipli, M.W.A. (2023). The application of the lex fravo reo principle in the criminal justice system in Indonesia. *Mandub: Jurnal Politik, Sosial, Hukum Dan Humaniora*, 2(1), 199-208. doi: 10.59059/mandub.v2i1.895.

Від відплати до людяності: адаптація доктрини крайнього засобу в індонезійському кримінальному праві

Ервін Сусіло
Докторант
Університет Сія Куала
24415, вул. Хасан Круенг Калі, 1, м. Банда-Ачех, Республіка Індонезія
https://orcid.org/0009-0000-9990-8112

Анотація
У цьому дослідженні розглянуто правову актуальність і потенційну можливість застосування доктрини крайнього засобу в індонезійській системі кримінального правосуддя як обмежувального принципу щодо повноважень суддів призначати смертну кару. Закон № 1 від 2023 року вніс фундаментальні зміни, оскільки більше не класифікує смертну кару як основне покарання, а радше як альтернативне спеціальне покарання, що підлягає суворим матеріальним і процесуальним вимогам. У цьому дослідженні використано нормативно-правовий метод у межах законодавчого, концептуального та порівняльного підходів, і посилання на кілька судових рішень Верховного суду Індії, таких як справа Бачана Сінгха проти штату Пенджаб. Доктрина крайнього засобу вимагає, щоб смертну кару призначали лише в надзвичайно виняткових випадках з високим рівнем жорстокості, що демонструють крайню аморальність, і коли реабілітацію злочинця вважають неможливою. У дослідженні рекомендовано встановити в Індонезії керівні принципи для обмеження судових повноважень, забезпечення підзвітності рішень й узгодження кримінальної практики із цінностями Панкасіли й теорією гідного правосуддя. Цю доктрину запропоновано як механізм фільтрації, завдяки якому смертну кару застосовують лише як *ultimum remedium* пропорційно, обережно та гуманно, щоб захистити право на життя та відобразити справедливіший і гуманніший напрям у політиці кримінального правосуддя

Ключові слова:
смертна кара; крайній засіб; суддя; гідне правосуддя; Панкасіла

UDC 34.041.3:004
DOI: 10.63341/naia-chasopis/3.2025.92

Digital objects as a new type of civil rights objects: Theoretical aspects and classification criteria

Bohdan Shuliaka*
Postgraduate Student
European University
03187, 42 Akademik Glushkov Ave., Kyiv, Ukraine
https://orcid.org/0009-0006-2895-705X

Abstract
The study aimed to provide a comprehensive analysis of the legal nature of digital objects as a new type of civil rights object and to develop the theoretical framework for their effective legal regulation in the context of the digital transformation of society. The methodological basis of the study was the comparative legal method for analysing approaches to the regulation of digital objects in the legal systems of China, Switzerland, Germany, Japan, Singapore and the USA, the formal legal method for studying current Ukrainian legislation, and the systemic analysis for studying digital objects as a complex phenomenon. The study established that digital objects are a unique legal phenomenon which does not fully fit into classical civil law constructs and requires a special legal regime. The study revealed the fragmented and contradictory nature of Ukrainian legal regulation, in particular, systemic conflicts between the general property regime of a digital object in the Civil Code of Ukraine and the special regime of a virtual asset in the relevant law. The study proved the problematic nature of applying the legal fiction of extending property rights to intangible objects, which creates legal uncertainty and complicates law enforcement. An analysis of court practice has revealed practical difficulties in applying the current legislation, in particular when seizing cryptocurrencies as material evidence in criminal proceedings. The study substantiated the need to revise the approach by abandoning the fiction of a digital object and creating an independent category of digital assets with a special legal regime. The practical value of the study is determined by the creation of a theoretical basis for improving the legal regulation of digital objects and the possibility of using the results in lawmaking, law enforcement practice and further research

Keywords:
custody services; virtual asset; tokens; blockchain; transactions

Introduction

The research relevance is determined by the legal nature of digital objects, due to fundamental changes in economic relations caused by the digital transformation of society, which generates fundamentally new forms of value without analogues in the traditional legal system. The rapid growth in the volume of transactions with cryptocurrencies, non-fungible tokens and other digital assets amid the exponential development of the global digital asset market, the spread of tokenisation of property rights, the development of

Article's History:
Received: 10.06.2025
Revised: 01.09.2025
Accepted: 29.09.2025

Suggest Citation:
Shuliaka, B. (2025). Digital objects as a new type of civil rights objects: Theoretical aspects and classification criteria. *Law Journal of the National Academy of Internal Affairs*, 15(3), 92-107. doi: 10.63341/naia-chasopis/3.2025.92.

*Corresponding author

blockchain technologies and the emergence of decentralised autonomous organisations creates a critical need for effective legal regulation to protect participants in civil turnover and ensure the stability of economic relations. At the same time, the problem is that legal systems are unprepared to regulate objects that exist exclusively in the virtual space and have unique properties not inherent in traditional goods, which, combined with the lack of unified international approaches to the regulation of digital objects, requires a different approach to the basic categories of civil law and the development of scientifically sound theoretical foundations for the legal qualification of digital objects and the determination of adequate legal regimes.

The problem of tokenisation of property rights turned out to be much more complicated than the simple transfer of traditional legal structures to the digital environment, as proved by R.M. Garcia-Teruel & H. Simón-Moreno (2021) in the comparative study of European and American practices analysed the peculiarities of legal regulation of digital assets in different jurisdictions and identified specific challenges associated with adapting existing legal frameworks to new technological realities. The researchers examined the correlation between traditional legal institutions and innovative forms of digital assets, focusing on the need for more flexible approaches to legal regulation. The issue of the legal qualification of tokens as objects of civil rights was studied by J.M. Moringiello & C.K. Odinet (2022) in an analysis of the difficulties of applying traditional legal categories to digital assets. The study considered the problem of determining the legal nature of tokens in the context of existing legal systems and drew attention to the need to rethink approaches to the regulation of digital objects. The study highlights the importance of adapting legal mechanisms to the specific characteristics of digital assets to ensure effective legal protection of the interests of owners. The conclusions regarding the inadequacy of blockchain technology regulation exclusively through the prism of securities law were confirmed by M. Kiskis (2024). The study proved that current attempts to regulate blockchain, which consider crypto tokens and digital assets only as securities, currencies or their derivatives, have a fundamental limitation – they are unable to incorporate the various legal rights, obligations and assets that blockchain technology can virtually reproduce. The researcher emphasised that a regulatory approach focused exclusively on public law ignores the full potential of blockchain technology and risks stifling innovation and practical applications.

In the Ukrainian scientific discourse, the terminological ambiguity between virtual and digital assets has long remained a source of legal confusion until the publication of a study by O. Dmytryk (2021). The study not only identified the roots of the problem in the imperfection of legislative definitions but also developed criteria for distinguishing between these concepts based on technological properties and economic functions. The issue of the legal nature of digital assets was studied by I.Yu. Guleykov (2025). The study defined digital assets as atypical objects of civil law, the legal nature of which still lacks unity of approach in legal doctrine. The finding that Ukraine currently lacks clear legal regulation of relations relating to digital assets, which naturally creates legal uncertainty in the course of concluding and performing transactions with digital assets, is notable. The study has developed a comprehensive classification of digital assets according to five criteria: property, axiological, functional, technological and depending on their use in civil circulation. E. Michurin (2022) studied the trends in the legal regulation of digital technology objects, identifying three main approaches to their study: technocratic, comprehensive and special legal. The study analysed in detail the special legal approach, which includes public law and private law, as well as the study of digital technologies as objects of intellectual property rights. Legal terminology, in particular, the correlation of the concepts of "virtual assets", "virtual goods", "digital objects" and "objects of digital technologies", was emphasised, and the study substantiates the expediency of using the term "virtual good" in private law instead of the economic term "virtual asset". The study proved that the concept of property rights can be applied to the legal regulation of digital technology objects, suggesting that the actual owner of a digital technology object is a person who has the right to access it through authentication and verification.

At the same time, despite a considerable amount of research, the issues of systematisation of digital objects (things) and determination of the most effective approaches to their legal regulation in the current environment remain insufficiently studied. In particular, the aspects of the correlation between different legal regimes of digital objects, the mechanisms of their integration into the traditional system of civil rights objects, and the peculiarities of applying classical civil law constructs to intangible goods require in-depth analysis. In addition, additional research is required to determine the legal nature of digital objects as a special type of civil rights objects, to develop criteria for their classification with due regard for technical and economic features, to analyse the effectiveness of different approaches to legal regulation based on a comparative study, and to justify the need to create a special legal regime for digital objects instead of extending traditional legal constructs to them.

The study aimed to form a scientific basis for optimising the legal regime of digital objects. To achieve this goal, the following tasks were set: to analyse the views on the legal nature and criteria for classification of digital objects; to analyse the current legislative regulation of digital objects in Ukraine; to substantiate the need for a special legal regime for digital objects.

Materials and Methods

A primary method of research was the comparative legal method, which was used to analyse approaches to the regulation of digital objects in different legal systems of the world, in particular in China, Switzerland, Germany, Japan, Singapore and the United States. This method was used to identify common trends and differences in legal regulation, as well as to assess the effectiveness of various regulatory models for their potential adaptation in the Ukrainian legal environment. The formal legal method was used for a detailed analysis of the current Ukrainian legislation, including the provisions of the Civil Code of Ukraine[1] and Law of Ukraine No. 2074-IX "On Virtual Assets"[2]. The provisions of Law of Ukraine No. 3321-IX "On Digital Content and Digital Services"[3] and Law of Ukraine No. 361-IX "On Prevention and Counteraction to Legalisation (Laundering) of Criminal Proceedings, Terrorist Financing and Financing of Proliferation of Weapons of Mass Destruction"[4] were also studied. This method identified systemic conflicts and gaps in legal regulation, as well as analysed internal contradictions between different legal acts.

The system analysis was used to study digital objects as a complex legal phenomenon that requires consideration of technical, economic and legal aspects of their functioning. This approach was used to develop a multidimensional classification of digital objects and identify the interrelationships between different legal regimes applied to them in Ukrainian legislation. The legal framework of the study was based on national and international legal acts regulating relations in the field of digital technologies, in particular Regulation of the European Parliament and of the Council No. 2024/1624 "On the Prevention of the Use of the Financial System for the Purposes of Money Laundering or Terrorist Financing (Text with EEA relevance)"[5], Federal Act of Switzerland "On the Adaptation of Federal Law to Developments in Distributed Electronic Register Technology"[6]. The study also analysed US regulations, including the Commodity Futures Trading Commission orders (CFTC, 2015) and the Securities Act of 1933[7].

The empirical basis of the study was the case law, including the decisions of Ukrainian courts in cases related to digital assets. In particular, the Decision in case No. 991/1512/23[8], the Judgement of the Shepetivka City District Court of Khmelnytskyi Region in Case No. 688/3758/23[9] and the Decision on the seizure of property in Case No. 752/7557/22[10] were analysed. The provisions of the Civil Procedure Code of Ukraine[11] are additionally considered. The analysis of court practice has revealed practical problems of application of the current legislation and demonstrated the consequences of theoretical contradictions in the legal regulation of digital objects.

Results

Conceptual framework and conceptual foundations of digital objects. The first and most obvious sign of the crisis in the legal regulation of relations in the digital sphere is the lack of a unified and consistent terminology. Both scientific doctrine and legislation use a large number of different, often synonymous or partially overlapping terms to refer to objects existing in the digital environment. Among them are such terms as "digital objects", "virtual assets", "digital assets", "cryptoassets", "virtual goods", "digital objects", etc. Such terminological diversity is not a purely linguistic problem; it is a direct consequence of the lack of a unified concept and a coherent approach to research of the legal nature of these phenomena. Each term carries a certain conceptual charge, reflecting the attempt of a legislator or scholar to fit a new phenomenon into a certain, already known legal framework, which, as will be shown below, is not always successful.

The "digital object" is a concept introduced by Law of Ukraine No. 3320-IX[12]. According to the new Article

[1] Civil Code of Ukraine. (2003, January). Retrieved from https://zakon.rada.gov.ua/laws/show/435-15.
[2] Law of Ukraine No. 2074-IX "On Virtual Assets". (2022, February). Retrieved from https://zakon.rada.gov.ua/laws/show/2074-20.
[3] Law of Ukraine No. 3321-IX "On Digital Content and Digital Services". (2023, August). Retrieved from https://zakon.rada.gov.ua/laws/show/3321-20#Text.
[4] Law of Ukraine No. 361-IX "On Prevention and Counteraction to Legalisation (Laundering) of Criminal Proceeds, Terrorist Financing and Financing of Proliferation of Weapons of Mass Destruction". (2019, December). Retrieved from https://zakon.rada.gov.ua/laws/show/en/361-20.
[5] Regulation of the European Parliament and of the Council No. 2024/1624 "On the Prevention of the Use of the Financial System for the Purposes of Money Laundering or Terrorist Financing (Text with EEA relevance)". (2024, May). Retrieved from https://eur-lex.europa.eu/eli/reg/2024/1624/oj.
[6] Federal Act of Switzerland "On the Adaptation of Federal Law to Developments in Distributed Electronic Register Technology". (2021, February). Retrieved from https://www.bk.admin.ch/ch/d/pore/rf/cr/2019/20192205.html.
[7] Securities Act of the USA. (1933). Retrieved from https://www.govinfo.gov/content/pkg/COMPS-1884/pdf/COMPS-1884.pdf.
[8] Judgement of the High Anti-Corruption Court of Ukraine in Case No. 991/1512/23. (2023, June). Retrieved from https://reyestr.court.gov.ua/Review/111590400.
[9] Judgement of the Shepetivka City District Court of Khmelnytskyi Region in Case No. 688/3758/23. (2023, December). Retrieved from https://reyestr.court.gov.ua/Review/115427588.
[10] Judgement of the Holosiivskyi District Court of Kyiv in Case No. 752/7557/22. (2022, November). Retrieved from https://reyestr.court.gov.ua/Review/107216946.
[11] Civil Procedural Code of Ukraine. (2004, March). Retrieved from https://zakon.rada.gov.ua/laws/show/en/1618-15#Text.
[12] Law of Ukraine No. 3320-IX "On Amendments to the Civil Code of Ukraine Regarding the Expansion of the Scope of Civil Rights". (2023, August). Retrieved from https://zakon.rada.gov.ua/laws/show/3320-%D0%86%D0%A5#Text.

179-1 of the Civil Code of Ukraine[1], a digital object is "a good that is created and exists exclusively in the digital environment and has property value"[2]. This category is generic, as part 2 of the same Article explicitly states that a digital object is a virtual asset, digital content and other goods (Neskorodzhena *et al.*, 2024; Zozulyak & Maksymiv, 2024). The key and most controversial aspect of this novelty is the extension to digital objects of the legal regime of things "unless otherwise provided... by law or follows from the essence of the digital object". This approach, based on a legal fiction, has been the subject of fundamental criticism by a large part of the legal community (Slipchenko & Slipchenko, 2024a).

The "virtual asset" is the central concept of the special Law of Ukraine No. 2074-IX[3]. According to Article 1 of this Law, a virtual asset is an "intangible good that is an object of civil rights, has a value and is expressed by a set of data in electronic form". At the same time, a different definition is contained in Law of Ukraine No. 361-IX, where a virtual asset is defined as "a digital expression of value that can be traded in a digital format or transferred and can be used for payment or investment purposes". This ambiguity creates a direct conflict, as Law of Ukraine No. 2074-IX in Article 4 explicitly prohibits the use of virtual assets as a means of payment in Ukraine (Pochynok, 2023).

The "digital content" is a concept defined in Law of Ukraine No. 3321-IX[4]. According to this act, digital content is "data created and provided in digital form", which includes computer programs, applications, video files, audio files, music files, digital games and e-books. The classification of digital content as "digital objects" in the Civil Code of Ukraine[5] is controversial, as most of such objects are the results of intellectual and creative activity and are protected by copyright, which provides for a completely different legal regime than property law (Trofymenko & Fedorenko, 2022).

The debate on the correlation of these concepts in the scientific doctrine also has no common denominator. The scientific literature lacks a unified approach to the correlation between the terms "digital assets" and "virtual assets". O. Dmytryk (2021) proposes to distinguish between them, considering "digital assets" as a broader concept that covers any benefits in digital form that have a real financial value, while "virtual assets" exist mainly in the virtual world (for example, game items) and may not have a direct link to real value. The legislative construction of the Civil Code of Ukraine, where "digital object" is a generic term for "virtual asset", adds another layer of complexity to this terminological confusion.

For further analysis, it is necessary to consider specific types of digital objects that have already become an integral part of the digital economy. Cryptocurrencies (e.g., Bitcoin, Ethereum) are decentralised, fungible tokens that operate on a distributed ledger technology (blockchain). Their legal nature is one of the most difficult to qualify. On the one hand, they are not money or currency values within the meaning of Ukrainian law. On the other hand, they de facto perform some of the functions of money, in particular, as a means of exchange and accumulation of value. The prevailing approach in legal doctrine and court practice is to qualify them as a specific type of property (goods) that can be the subject of sale and exchange agreements.

Tokens are accounts in a distributed ledger that can represent a variety of rights and values. Their legal nature is determined by the function they perform. Payment tokens are similar in purpose to cryptocurrencies and are used as a means of payment between users (Lawrange, n.d.). Security/Investment tokens certify rights similar to those arising from traditional securities, for example, the right to receive a portion of the profit, the right to participate in the management of the company. Ukrainian legislation does not yet contain clear criteria for such qualification. Service/Utility tokens give their holder the right to access a specific product or service within a particular digital platform or ecosystem (Shapovalova, 2024). Governance tokens give the right to vote in decision-making on the development of a decentralised project, protocol, or decentralised autonomous organisation (DAO). NFTs, or non-fungible tokens, are unique records in the blockchain that confirm the authenticity and right of control over a certain, usually digital, object (Klyan & Selivakin, 2023). The key legal issue related to NFTs is the relationship between the rights to the token itself and the rights to the underlying object that it "tokenises" (e.g., a digital work of art, music file, game item). The acquisition of an NFT does not, by default, imply the transfer of copyright or any other exclusive rights to the underlying object, unless expressly provided for in the terms of the transaction.

Despite the diversity of digital objects, in the process of analysing them, several common, inherent features and properties can be identified that determine their specificity as objects of civil rights. First, it is worth noting the intangible nature of all digital objects, as they lack physical, corporeal substance and exist in the

[1] Civil Code of Ukraine. (2003, January). Retrieved from https://zakon.rada.gov.ua/laws/show/435-15.
[2] Law of Ukraine No. 361-IX "On Prevention and Counteraction to Legalisation (Laundering) of Criminal Proceeds, Terrorist Financing and Financing of Proliferation of Weapons of Mass Destruction". (2019, December). Retrieved from https://zakon.rada.gov.ua/laws/show/en/361-20.
[3] Law of Ukraine No. 2074-IX "On Virtual Assets". (2022, February). Retrieved from https://zakon.rada.gov.ua/laws/show/2074-20.
[4] Law of Ukraine No. 3321-IX "On Digital Content and Digital Services". (2023, August). Retrieved from https://zakon.rada.gov.ua/laws/show/3321-20#Text.
[5] Civil Code of Ukraine. (2003, January). Retrieved from https://zakon.rada.gov.ua/laws/show/435-15.

form of data or software code (Guleykov, 2025). Closely related to this feature is the property of existence in the digital environment, as such objects are created, exist, circulate and cease to exist exclusively within the digital environment, which is defined as a set of hardware, software and network connections. A substantial characteristic of digital objects is their property value, which is manifested in the ability to meet certain needs of participants in civil circulation (investment, consumer, gaming, etc.) and have a value equivalent, which is usually determined by market supply and demand (Michurin, 2022). This feature is directly correlated with the property of negotiability, due to which digital objects can be the subject of various civil law transactions: sale and purchase, exchange, gift, inheritance, etc. Finally, a characteristic feature of digital objects is their controllability, which is the ability to establish dominance over such an object, which is usually realised through the possession of a unique set of cryptographic data, a private key that provides access to the asset and the ability to dispose of it (Neskorodzhena *et al.*, 2024; Zozulyak & Maksymiv, 2024).

An analysis of the conceptual framework reveals a fundamental obstacle to the development of adequate legal regulation. Ukrainian legislation has simultaneously introduced two parallel and partially contradictory concepts: the broad category of "digital object" in the Civil Code of Ukraine[1] and the more specialised, but not fully correlate, concept of "virtual asset" in the relevant Law of Ukraine No. 2074-IX[2]. The Civil Code of Ukraine attempts to apply a universal, but outdated, property-law approach to all digital objects, extending the regime of objects to them. At the same time, the special Law of Ukraine No. 2074-IX creates a special regime, but it itself contains internal contradictions (for example, regarding the payment function, as noted by V.O. Yarotsky (2023)) and, most notable, is not effective due to the lack of tax regulation (Shapovalova, 2024). The consequences of such uncertainty exceed the scope of theoretical debates. They paralyse the development of the legal market, scare away investors, make adequate judicial protection impossible, and create a grey area conducive to fraud and money laundering. Thus, the problem lies not so much in the terminology as in the lack of a unified state policy and a coherent legal strategy for digital assets.

The legal nature of digital objects in the doctrine of civil law. The emergence and rapid proliferation of digital objects has raised a fundamental question for the civil law doctrine about their place in the traditional system of civil rights objects enshrined in Article 177 of the Civil Code of Ukraine[3]. This system, which includes things, property, property rights, results of intellectual and creative activity, information and other tangible and intangible goods, was not ready to integrate such atypical phenomena (Guleykov, 2025). The main academic debate has revolved around the dilemma of whether digital objects can be qualified within one of the existing categories, perhaps through an expansive interpretation or the use of legal fictions, or whether they are objects of a completely new, special kind (*sui generis*), requiring the creation of their own, unique legal regime.

The most widespread and, at the same time, most criticised in civil law is the proprietary concept, which proposes to extend the legal regime of things to digital objects, and, therefore, the key institution of property law – the right of ownership with its classical triad of powers (possession, use, disposal). E. Michurin (2025) substantiated the pragmatism of the proprietary approach, which mitigates the need to create a new complex system from scratch, instead employing the institutions of property law already developed over the centuries to regulate the circulation and, most notably, protect the rights to digital assets. The study also highlighted the economic similarity of digital objects to things: they have value, are individually identifiable (such as NFTs) or generic (such as cryptocurrencies), can be alienated and are under the exclusive control of one person.

At the same time, the criticism of the proprietary concept is much weightier and more systemic. The main counterargument lies in a fundamental conceptual contradiction: property rights as an absolute right are historically, doctrinally and inherently associated with material, corporeal objects over which physical domination is possible (Slipchenko & Slipchenko, 2024b). Calling an incorporeal good that is a collection of data an "object" means resorting to a legal fiction that creates terminological confusion and logical contradictions (Neskorodzhena *et al.*, 2024; Zozulyak & Maksymiv, 2024). The legal regime of an object does not consider the key specifics of digital objects: their intangibility, ease of copying, cross-border nature, impossibility of physical destruction or damage, and close connection with intellectual property law (Slipchenko & Slipchenko, 2024a). This creates practical legal uncertainty, in particular in the application of a vindication claim (reclamation of an object from someone else's illegal possession) to stolen cryptocurrency or a negator claim (removal of obstacles to use) to NFTs. The concept of intellectual property rights is most relevant to objects such as digital content and NFTs. It is based on the fact that the token or file itself is only a form of embodiment of the copyright object (work), and accordingly, the rights to it should be regulated not by the law of property, but by intellectual property law (Zerov, 2023).

[1] Civil Code of Ukraine. (2003, January). Retrieved from https://zakon.rada.gov.ua/laws/show/435-15.
[2] Law of Ukraine No. 2074-IX "On Virtual Assets". (2022, February). Retrieved from https://zakon.rada.gov.ua/laws/show/2074-20.
[3] Law of Ukraine No. 3320-IX "On Amendments to the Civil Code of Ukraine Regarding the Expansion of the Scope of Civil Rights". (2023, August). Retrieved from https://zakon.rada.gov.ua/laws/show/3320-%D0%86%D0%A5#Text.

The concept of *sui generis* appears as the most scientifically sound, as it recognises the uniqueness of digital objects as a legal phenomenon that cannot be fit into any of the existing categories without distortion. Therefore, they require the creation of a special, separate legal regime that would organically combine elements of property (exclusive control), obligatory (relations within the system) and exclusive rights (protection against unauthorised copying and use). Regardless of the chosen concept, digital objects are already integrated into civil circulation and interact with traditional legal institutions. Property rights in Ukraine are enforced through the fiction of a "digital object", with the key element of the ownership triad being associated not with physical dominance but with technical control over the private key to access the asset (Neskorodzhena *et al.*, 2024; Zozulyak & Maksymiv, 2024).

Inheritance is one of the most problematic areas, as the transfer of digital assets to inheritance is complicated by both technical (the need for heirs to have access to the testator's private keys) and legal (problems with the identification and valuation of assets by a notary, the lack of a clear procedure for their inclusion in the estate) aspects. The possibility of pledging digital assets remains controversial and directly depends on their legal qualification. If they are defined as property, then such a possibility exists, but the mechanisms for the implementation of the pledge (for example, foreclosure) are not developed (Klyan & Selivakin, 2023). The circulation of digital objects mainly takes place based on traditional contractual structures: sale and purchase, exchange, provision of services (for example, crypto-exchange services) (Guleykov, 2025). The doctrinal conflict that has arisen around the legal nature of digital objects goes beyond a purely academic dispute. The choice of the proprietary model ("digital object") has become a source of real and acute problems in law enforcement practice (Slipchenko & Slipchenko, 2024a). However, the Civil Procedure Code of Ukraine[1] defines material evidence as a tangible object that has retained traces of a crime.

Cryptocurrencies are intangible in nature and cannot meet this criterion in the classical sense, which creates an insoluble conflict. As a result, the courts are forced to either refuse to seize the assets, leaving the victims without any real protection, or resort to a "creative" interpretation of the law, as the High Anti-Corruption Court did, by seizing the assets not as material evidence but to secure future confiscation of property. This decision sets an significant precedent, but does not solve the systemic problem. This example demonstrates how a theoretically wrong choice (the use of an unsuccessful legal fiction) directly leads to the practical impossibility of effective and predictable justice.

Classification criteria and digital object system. The classification of digital objects determines approaches to their legal regulation and influences the formation of differentiated legal regimes. It is impossible to apply the same legal regime to the cryptocurrency Bitcoin, which serves as a medium of exchange, to an NFT that certifies the uniqueness of a work of art, and to a token that grants the right to vote in a decentralised autonomous organisation. An effective classification should be based on a system of criteria that considers not only the legal but also the technical and economic nature of these objects (Guleykov, 2025). This will avoid overgeneralisation and the development of a special legal regime for each significant group of digital goods. Table 1 demonstrates systematised main types of digital objects and analysis of their legal status in the Ukrainian jurisdiction.

Table 1. Classification of digital objects by legal nature

Object type	Subtype	Examples	Legal regime	Legislative framework
Crypto assets	Unsecured	Bitcoin, Ethereum	Virtual asset	Law of Ukraine No. 2074-IX[2] (not yet in effect)
	Secured	Asset tokens	Virtual asset	Law of Ukraine No. 2074-IX (not yet in effect)
Digital content	Entertainment	Video, music, games	Data/copyright	Civil Code of Ukraine[3] and Civil Procedural Code of Ukraine[4]
	Software	Software, applications	Data/copyright	Civil Code of Ukraine and Civil Procedural Code of Ukraine
NFT	Art	Digital paintings	Digital object	Civil Code of Ukraine
	Collectables	Cards, items	Digital object	Civil Code of Ukraine

Source: compiled by the author based on R.V. Popov (2024) and E. Michurin (2025)

[1] Civil Procedural Code of Ukraine. (2004, March). Retrieved from https://zakon.rada.gov.ua/laws/show/en/1618-15#Text.
[2] Law of Ukraine No. 2074-IX "On Virtual Assets". (2022, February). Retrieved from https://zakon.rada.gov.ua/laws/show/2074-20.
[3] Civil Code of Ukraine. (2003, January). Retrieved from https://zakon.rada.gov.ua/laws/show/435-15.
[4] Civil Procedural Code of Ukraine. (2004, March). Retrieved from https://zakon.rada.gov.ua/laws/show/en/1618-15#Text.

This classification reveals critical gaps in the legal regulation of digital objects in Ukraine. The most problematic is the situation with cryptoassets, the legal status of which remains uncertain due to the failure to enact a specialised law, which creates legal uncertainty in the areas of taxation, inheritance and criminal liability. Digital content is regulated mainly through the prism of copyright, which does not always adequately reflect the economic nature of such objects, especially in the context of their use as investment instruments or means of payment. NFTs represent a special category, as their legal qualification as "digital objects" under the Civil Code of Ukraine contradicts traditional civil law concepts of property law and creates difficulties in applying property, contractual and consumer protection rules. This inconsistency indicates the need for a comprehensive review of legislative approaches and the creation of a unified conceptual framework for the regulation of all types of digital assets, incorporating their technological features and economic function in the modern digital economy.

The current legislation of Ukraine, albeit fragmented, has already laid the foundations for the primary classification of digital objects based on their legal regime. At the highest level, in accordance with the Civil Code of Ukraine[1], they are all grouped under the generic category of "digital objects". The first group includes virtual assets, the legal regime of which should be determined by a special Law of Ukraine No. 2074-IX[2]. The second group covers digital content, which is regulated by special Law of Ukraine No. 3321-IX[3]. The third group is the category of other goods with an open list, which theoretically includes such objects as domain names, accounts in social networks and other online services that also exist in the digital environment and have property value. The VA Law offers a more detailed internal classification of virtual assets based on their economic substance and the existence of a connection with other civil rights objects. The first criterion is based on the availability of collateral, which distinguishes between unsecured virtual assets that do not certify any property or other rights of their owner against any third party. Their value is based solely on the trust of system participants and market demand, with cryptocurrencies such as Bitcoin being a classic example (Pochynok, 2023).

In contrast, secured virtual assets certify property rights, in particular, the rights of their owner to claim against the issuer or other obligated person in respect of another, basic object of civil rights (Zerov, 2023). The second criterion applied to secured VAs differentiates them depending on the type of collateral. Financial virtual assets constitute a specific category of secured VAs that certify rights to financial instruments and are divided into secured virtual assets collateralised by currency values (SVAs) and secured virtual assets collateralised by a security or derivative financial instrument (SVAs)[4]. Alongside them, there are non-financial virtual assets that are collateralised by other goods, such as real estate, goods or services.

International practice, in particular Regulation of the European Parliament and of the Council No. 2024/1624[5] and the approaches of the Swiss regulator, the Swiss Financial Market Supervisory Authority (FINMA), offer a classification based not on formal legal structures, but on the economic function performed by the token (FINMA, n.d.; FINMA publishes guidelines..., 2018). This approach is more flexible and adequate to the essence of the phenomenon, distinguishing payment tokens (Payment/E-money tokens), the main purpose of which is to function as a means of exchange and payment, including classic cryptocurrencies and stablecoins (Shapovalova, 2024; Kostyuchenko, 2021). Investment tokens or asset-referenced tokens are characterised by the fact that they are purchased for investment purposes, provide rights similar to those of securities (to profit, to a share in an asset), or their value is tied to a basket of other assets, such as currencies or commodities. Service or Utility tokens provide their holder with digital access to certain goods or services provided by the issuer on its platform (Shapovalova, 2024).

In a technical context, all tokens that exist based on blockchain technology can be differentiated into two broad groups depending on their fungibility. Fungible tokens are characterised by the fact that each unit is identical, indivisible and equivalent to any other unit of the same type, as in the case of Bitcoin, where one token is indistinguishable from another. Non-Fungible (NFT) tokens are the opposite in nature, as each one is unique, has individual characteristics recorded in its metadata, and cannot be replaced by another similar token. It is this uniqueness that determines their value in areas such as digital art, collectables, and gaming (Klyan & Selivakin, 2023).

The analysis of the criteria for classification of digital objects demonstrates the complexity and multidimensionality of this legal phenomenon, which requires an integrated approach to systematisation. The author establishes that an effective classification should be

[1] Civil Code of Ukraine. (2003, January). Retrieved from https://zakon.rada.gov.ua/laws/show/435-15.
[2] Law of Ukraine No. 2074-IX "On Virtual Assets". (2022, February). Retrieved from https://zakon.rada.gov.ua/laws/show/2074-20.
[3] Law of Ukraine No. 3321-IX "On Digital Content and Digital Services". (2023, August). Retrieved from https://zakon.rada.gov.ua/laws/show/3321-20#Text.
[4] Law of Ukraine No. 2074-IX "On Virtual Assets". (2022, February). Retrieved from https://zakon.rada.gov.ua/laws/show/2074-20.
[5] Regulation of the European Parliament and of the Council No. 2024/1624 "On the Prevention of the Use of the Financial System for the Purposes of Money Laundering or Terrorist Financing (Text with EEA relevance)". (2024, May). Retrieved from https://eur-lex.europa.eu/eli/reg/2024/1624/oj.

based on a combination of technical properties (interchangeability, decentralisation), economic functions (payment, investment, utilitarian) and legal regimes, rather than on formal legal constructs.

Digital objects in Ukrainian law: Regulatory analysis and issues. A key step in the attempt to integrate digital objects into Ukraine's legal system was the amendment to the Civil Code of Ukraine[1] in 2023, which supplemented Article 177 with a reference to "digital objects" alongside tangible objects and introduced a legal definition in a new Article 179-1. The most significant and at the same time problematic provision is part 2 of Article 179-1, which extends the legal regime of objects to digital objects on a residual basis. This decision is a legal fiction that equates intangible goods with tangible objects, ignoring the fundamental differences between them and creating logical obstacles to law enforcement, in particular in terms of the application of property rights remedies (Slipchenko & Slipchenko, 2024a).

Law of Ukraine No. 2074-IX[2], adopted in February 2022, was the first attempt to comprehensively regulate the virtual asset market in Ukraine, defining the legal status of virtual assets as intangible goods and objects of civil rights, introducing a classification into secured and unsecured assets, establishing the principles of service providers' activities, and defining the powers of state regulators (Hrytsay, 2022). However, the key problem is that the law has not yet entered into force due to the lack of adopted amendments to the Tax Code on taxation of transactions with virtual assets, which creates a paradoxical situation of "deferred regulation" (Shapovalova, 2024).

In addition to these basic acts, relations in the digital sphere are regulated by Law of Ukraine No. 3321-IX[3], which establishes rules for contractual relations regarding the provision of digital content to consumers based on European directives, emphasising the obligation aspects, which conflict with the property-based approach of the Civil Code of Ukraine, as well as Law of Ukraine No. 361-IX, which establishes the status of primary financial monitoring entities for virtual asset service providers and uses specific definition of a virtual asset, which differs from the relevant law.

The diversity of digital objects and the absence of a unified classification system necessitate the systematisation of the criteria for their legal qualification. To develop a comprehensive approach to regulation, it is advisable to identify the main classification criteria in Table 2 used in Ukrainian and international law.

Table 2. Classification criteria for digital objects

Classification criterion	The basis for the distinction	Legal significance	Source of regulation
Legal regime	Special vs general regulation	Identify applicable rules and procedures	Civil Code of Ukraine, special laws
Functional purpose	Purpose of use of the asset	Regulatory requirements and circulation regime	Regulation No. 2024/1624[4]
Technical replaceability	Interchangeability vs uniqueness	Peculiarities of transactions and valuation	Blockchain technical standards
Materiality	Physical vs digital form of existence	Application of law in rem vs law of obligations	Civil Code of Ukraine[5], p. 179-1
Issuer	Centralised versus decentralised production	Liability and control	Financial legislation
Territory of circulation	National versus cross-border circulation	Jurisdiction and applicable law	International agreements, FATF
Degree of regulation	Regulated vs unregulated market	Requirements for participants and operations	National financial law

Source: compiled by the author based on S.O. Hrytsay (2022), I.Yu. Guleykov (2025) and E. Michurin (2025)

The presented classification criteria reflect the multidimensionality of legal regulation of digital objects and demonstrate the complexity of creating a unified approach to their qualification. The criterion of legal regime is the basis for the determination of the hierarchy of regulations applicable to a particular object, but in the Ukrainian legal system, there is a conflict between the general provisions of the Civil Code of Ukraine on "digital objects" and special rules on virtual assets, which complicates law enforcement. Functional purpose as a criterion is of particular importance in the context of harmonisation with European law, in particular Regulation (EU) No. 2024/1624 of the European Parliament and of the Council, which

[1] Civil Code of Ukraine. (2003, January). Retrieved from https://zakon.rada.gov.ua/laws/show/435-15.
[2] Law of Ukraine No. 2074-IX "On Virtual Assets". (2022, February). Retrieved from https://zakon.rada.gov.ua/laws/show/2074-20.
[3] Law of Ukraine No. 3321-IX "On Digital Content and Digital Services". (2023, August). Retrieved from https://zakon.rada.gov.ua/laws/show/3321-20#Text.
[4] Regulation of the European Parliament and of the Council No. 2024/1624 "On the Prevention of the Use of the Financial System for the Purposes of Money Laundering or Terrorist Financing (Text with EEA relevance)". (2024, May). Retrieved from https://eur-lex.europa.eu/eli/reg/2024/1624/oj.
[5] Civil Code of Ukraine. (2003, January). Retrieved from https://zakon.rada.gov.ua/laws/show/435-15.

distinguishes between payment, investment and utility tokens, creating different regulatory regimes depending on the economic function of the asset.

The most fundamental problem of Ukrainian legislation on digital objects is the existence of deep systemic conflicts and gaps. There is a conflict of regimes between the general property regime of a "digital object" in the Civil Code of Ukraine and the special regime of a "virtual asset" as an intangible good in the relevant law, a conflict of definitions between different definitions of a "virtual asset" in Law of Ukraine No. 361-IX[1], and a legal vacuum for many types of digital objects, such as domain names, social media accounts, governance tokens, and decentralised autonomous organisations. In general, the legislation is fragmented and unsystematic, as the rules are scattered across different acts, making them difficult to interpret and apply.

The uncertainty of the legal nature of objects creates serious problems with the legal qualification of transactions involving them. When it is unclear whether an asset is an "object", "property", "property right" or "intangible good", it becomes difficult to determine the type of contract (sale, exchange, provision of services), essential terms, the moment of transfer of rights and the consequences of default. Legal definitions are often overly simplistic and do not consider the technical complexity of digital objects. A striking example is the linking of ownership to "key possession", which ignores the realities of the market: custodial services where private keys are stored by the platform, multi-signature wallets, complex smart contracts with autonomous asset management. This gap between legal abstraction and technical reality renders many rules virtually ineffective and demonstrates the limits of national law's effectiveness in the global digital environment.

The practical exercise of rights and their protection in the digital sphere face unique challenges that the traditional legal system is not prepared for. The case law is still being formed, but it already illustrates all the problems of the legislation through specific cases of cryptocurrency seizure. The most illustrative is case No. 991/1512/23[2] of the High Anti-Corruption Court of Ukraine, where the investigating judge granted the prosecutor's motion to seize virtual assets in the form of a ban on the alienation and disposal of Tether (USDT), Tron (TRX), Ethereum (ETH) cryptocurrencies, which were held on the electronic multi-currency crypto wallet of a suspect in a corruption crime under Part 4 of Article 368 of the Criminal Procedure Code of Ukraine[3]. The key legal issue was that the court was forced to justify the seizure of intangible objects using property law constructs. The court noted that although Law of Ukraine No. 2074-IX[4] has not entered into force, "Ukrainian legislation prioritises identification of the holder of the key to a virtual asset with the owner of such a virtual asset". This decision demonstrates the forced application of the unsuccessful legal fiction of a "digital object", as the court was forced to establish ownership of intangible objects through technical control over private keys.

The opposite approach was demonstrated by the Shepetivka City District Court in Case No. 688/3758/23[5], which cancelled the seizure of cryptocurrencies as material evidence, recognising that the seizure of digital assets "given their intangible and non-individualised nature, is inconsistent with the stated purpose of the seizure as the preservation of material evidence". This ruling highlights the conceptual contradiction between the intangible nature of digital objects and attempts to apply traditional property law mechanisms to them. The court recognised that cryptocurrency cannot be material evidence within the meaning of the Criminal Procedure Code of Ukraine, which defines such evidence as "a material object that has retained traces of a crime".

The case No. 752/7557/22[6] of the Holosiivskyi District Court also illustrates the practical difficulties: the court seized crypto assets but failed to clearly define the legal nature of such objects and the procedures applicable to them. An analysis of these decisions reveals a systemic problem: courts are forced to resort to "creative" interpretation of legislation or alternative legal approaches to achieve the goals of justice due to the lack of adequate legal regulation of digital objects. The protection of rights is complicated by the difficulty of identifying the infringer in pseudonymous networks, the specificity of proof, the problems of enforcing court decisions on assets on decentralised wallets or foreign exchanges, and the difficulty of inheritance due to technical and legal barriers (Vinnyk, 2023). These precedents convincingly prove that the use of the legal fiction of a "digital object" creates practical legal uncertainty and makes effective justice in the digital sphere impossible.

The legal regulation being implemented in Ukraine and globally is fundamentally transforming the subject

[1] Law of Ukraine No. 361-IX "On Prevention and Counteraction to Legalisation (Laundering) of Criminal Proceeds, Terrorist Financing and Financing of Proliferation of Weapons of Mass Destruction". (2019, December). Retrieved from https://zakon.rada.gov.ua/laws/show/en/361-20.
[2] Judgement of the High Anti-Corruption Court of Ukraine in Case No. 991/1512/23. (2023, June). Retrieved from https://reyestr.court.gov.ua/Review/111590400.
[3] Criminal Procedural Code of Ukraine. (2012, April). Retrieved from https://zakon.rada.gov.ua/laws/show/en/4651-17#Text.
[4] Law of Ukraine No. 2074-IX "On Virtual Assets". (2022, February). Retrieved from https://zakon.rada.gov.ua/laws/show/2074-20.
[5] Judgement of the Shepetivka City District Court of Khmelnytskyi Region in Case No. 688/3758/23. (2023, December). Retrieved from https://reyestr.court.gov.ua/Review/115427588.
[6] Judgement of the Holosiivskyi District Court of Kyiv in Case No. 752/7557/22. (2022, November). Retrieved from https://reyestr.court.gov.ua/Review/107216946.

composition of legal relations in this area, shifting the focus from anonymous users to identified and licensed market participants. The early ideology of cryptocurrencies was based on the principles of anonymity, decentralisation and the absence of intermediaries. However, the high risks of using these technologies for money laundering, terrorist financing and other illegal activities have forced states, including Ukraine, to respond by introducing strict financial monitoring requirements for combating money laundering and terrorist financing following the standards of the Financial Action Task Force (FATF) (n.d.). These requirements are implemented through the institution of licensed intermediaries, VASPs, who control access to the legal market and are required to know their customers (KYC) (Pochynok, 2023). This fundamentally changes the nature of legal relations. Instead of direct peer-to-peer transactions between pseudonyms, the legal circulation of digital assets is increasingly mediated by regulated entities. This approach undoubtedly increases the safety, transparency and security of participants, but at the same time it inevitably reduces the level of decentralisation and privacy that was the ideological core of these technologies at the initial stage. Thus, the law effectively "centralises" decentralised technologies, subjecting them to state interests and control.

Comparative legal analysis of the regulation of digital objects. Analysis of international experience is critical for Ukraine, as it can be used to avoid mistakes, adopt best practices, and harmonise national legislation with global trends. Table 3 shows the approaches of the jurisdictions of China, Switzerland, Germany, Japan, Singapore and the United States, each of which demonstrates unique models of legal regulation of digital assets.

Table 3. Key differences in the regulation of digital objects

Jurisdiction	Legal status of cryptocurrency	Key regulatory authority	Regulatory approach	CBDC
China	"Virtual goods" with limited property rights; trading is prohibited	PBoC	Strict control, ban on trade	Digital yuan (e-CNY)
Switzerland	"DLT rights" as a new asset class; payment tokens	FINMA	Innovative, legal certainty	No operating CBDC
Germany	"Cryptoassets" under the Banking Act[1]; electronic securities	BaFin	Adaptation of traditional law	No operating CBDC
Japan	"Cryptoassets" with strict regulation of exchanges	JFSA	Investor protection and transparency	Development of the digital yen
Singapore	Digital payment tokens (DPT); ownership recognised by courts	MAS	A balanced approach	The Guardian project
USA	Intangible property under the UCC	IRS, state regulators	Innovations at the state level	No federal CBDC

Note: PBoC – People's Bank of China; BaFin – German Federal Financial Services Authority; JFSA – Japan Financial Services Agency; MAS – Monetary Authority of Singapore; IRS – US Internal Revenue Service; UCC – Uniform Commercial Code; CBDC – Central Bank Digital Currency; DLT – Distributed Ledger Technology.
Source: compiled by the author based on J. Feldman *et al.* (2021), NFT regulations in Japan (2021), TeraLex (2022), S. Kaaru (2024), K. Low & M. Hara (2024), A. Fillman (2025), Internal Revenue Service (n.d.), KYC Hub (n.d.)

A comparative analysis of the presented jurisdictions revealed three main regulatory models, each of which reflects different conceptual foundations of state policy towards digital assets. The restrictive model, implemented by China, is characterised by a complete ban on private cryptocurrency circulation while maintaining limited property rights and active development of the state's digital currency, which reflects the priority of financial stability and monetary sovereignty over technological innovation. The liberal model, represented by Switzerland and certain US states, is aimed to create the most favourable investment climate through the introduction of new legal categories and flexible regulatory approaches, which attract capital and stimulate the development of the fintech sector. The balanced model implemented by Germany, Japan, and Singapore combines technological openness with enhanced requirements for investor protection and financial stability, integrating crypto asset regulation into the existing financial framework by adapting traditional legislation. Of note is the approach to the development of digital currencies by central banks, which demonstrates strategic differences: from active implementation in China to experimental projects in Singapore and the absence

[1] Banking Act of the Federal Republic of Germany. (1961, July). Retrieved from https://www.gesetze-im-internet.de/kredwg/BJNR008810961.html.

of federal initiatives in the United States, reflecting different views on the role of the state in the digital transformation of the monetary system.

The European Union's approach is the most comprehensive and systematic among the existing regulatory models. Instead of fragmented regulation of certain aspects, the European Union has developed and adopted a single comprehensive Regulation of the European Parliament and of the Council No. 2024/1624[1] (MiCA), which aims to create a harmonised legal framework for the entire EU single market. The key feature of MiCA is the functional classification of crypto assets, according to which the regulation divides assets not by formal features, but by their economic function into electronic money tokens (EMT), asset-backed tokens and utility tokens (UT) (Zetzsche *et al.*, 2021). At the same time, MiCA establishes strict requirements for issuers and service providers (CASPs), providing detailed rules for the authorisation, operation and supervision of issuers and service providers related to cryptoassets. A substantial element of the European model is the concept of a "European passport", according to which a licence obtained by a service provider in one EU member state entitles it to operate throughout the Union, which contributes to the development of a single market. The Regulation also contains a significant set of rules aimed to protect consumer rights, prevent market manipulation and ensure transparency. For Ukraine, which has the status of a candidate for EU accession, the provisions of the MiCA provide a benchmark for harmonising national legislation with European standards for regulating virtual assets.

The US approach is fundamentally different and is based on a fundamentally different regulatory philosophy. Instead of creating a single special law, US regulators apply existing securities, commodities, and financial services laws, such as the Securities Act of 1933[2], to digital assets, resulting in what is known as "regulation by enforcement". Several agencies are central in this system, with often overlapping responsibilities. The Securities and Exchange Commission (SEC) applies the well-known "Howey Test"[3] to determine whether a digital asset is an "investment contract" and therefore a security subject to its regulation, and the SEC has taken the position that most tokens (except Bitcoin) are securities (Reiff, 2023).

At the same time, the CFTC (2015) considers some cryptocurrencies, including Bitcoin, to be commodities and regulates the market for derivatives on them. The Financial Crimes Enforcement Network (FinCEN) imposes strict anti-money laundering and counter-terrorist financing (AML/CFT) requirements on service providers that qualify as Money Services Businesses. For tax purposes, the Internal Revenue Service (IRS) treats digital assets as property rather than currency, which means that they are subject to capital gains taxation when sold. This approach creates significant regulatory uncertainty for businesses, as the status of many assets is determined not by law, but by litigation initiated by regulators. Switzerland has chosen the path of progressive and flexible regulation, which made it one of the world's centres for the crypto industry, known as the "Zug Crypto Valley"[4]. Instead of creating legislation from scratch, Switzerland has made pointed but systematic changes to existing laws.

The emergence of competing draft laws from the National Securities and Stock Market Commission (NSSMC) and the Ministry of Digital Transformation essentially reflects a debate on how best and most efficiently to implement MiCA approaches into the Ukrainian legal system[5]. This means that the future of Ukrainian regulation will be determined not so much by internal doctrinal disputes as by the external need to adapt to European standards. This sends a clear signal to Ukrainian businesses and investors: it is strategically correct to focus on MiCA requirements, as any purely national regulation is likely to be temporary and will be brought into full compliance with the European one in due course. Summarising the international experience of regulating digital assets, it is possible to state that the global trend is towards creating a comprehensive regulatory framework that combines innovation with adequate investor protection and financial stability. For Ukraine, as a candidate country for EU accession, it is strategically justified to focus on the European MiCA model, which provides legal certainty, consumer protection and the possibility of integration into the single European market. At the same time, it is necessary to consider Switzerland's experience with technology neutrality and flexible licensing, and to avoid the American model of regulation through enforcement, which creates significant uncertainty for market participants. The key challenge for Ukraine remains the need to rapidly implement European standards while maintaining the competitiveness of the national jurisdiction in the global competition for attracting investment in digital technologies.

[1] Regulation of the European Parliament and of the Council No. 2024/1624 "On the Prevention of the Use of the Financial System for the Purposes of Money Laundering or Terrorist Financing (Text with EEA Relevance)". (2024, May). Retrieved from https://eur-lex.europa.eu/eli/reg/2024/1624/oj.

[2] Securities Act of the USA. (1933). Retrieved from https://www.govinfo.gov/content/pkg/COMPS-1884/pdf/COMPS-1884.pdf.

[3] Opinion of the Supreme Court of USA in Case "SEC v. W.J. Howey Co., 328 U.S. 293". (1946, May). Retrieved from https://supreme.justia.com/cases/federal/us/328/293/.

[4] Federal Act of Switzerland "On the Adaptation of Federal Law to Developments in Distributed Electronic Register Technology". (2021, February). Retrieved from https://www.bk.admin.ch/ch/d/pore/rf/cr/2019/20192205.html.

[5] Draft Law of Ukraine No. 10225 "On Amendments to the Tax Code of Ukraine and Other Legislative Acts of Ukraine Regarding the Regulation of the Turnover of Virtual Assets in Ukraine". (2023, November). Retrieved from https://itd.rada.gov.ua/billinfo/Bills/Card/43232.

Discussion

The findings of the study confirm the concept of digital objects as a unique *sui generis* legal phenomenon, which correlates with the conclusions of international studies. The prospects for introducing the concept of "digital objects" and "digital content" to expand the scope of regulation of virtual assets, as considered by S. Hrytsai (2023), confirm the problematic application of traditional legal structures to intangible objects identified in the study. At the same time, the results of the analysis of Ukrainian legislation demonstrate deeper systemic conflicts than those indicated in foreign works. In particular, the author reveals a fundamental contradiction between the extension of the property regime to intangible goods in the Civil Code of Ukraine and the special regime of virtual assets as intangible goods in the relevant law, which creates legal uncertainty for market participants. O.M. Vinnyk (2023) studied the specifics of the Ukrainian experience of forming the legal framework for the digital economy and identified critical shortcomings in coordination between different regulatory authorities, which confirms the results of the analysis of competing draft laws from the NSSMC and the Ministry of Digital Transformation. The researcher proved that the fragmentation of Ukrainian legislation creates legal uncertainty and impedes innovative development, proposing a model of a unified institutional architecture for regulation, which fully coincides with the conclusions on the need for a comprehensive review of legislative approaches and the creation of a unified conceptual framework for the regulation of digital assets.

The conclusions regarding the need to recognise the unique legal nature of digital objects are consistent with the research of J. Wyczik (2025), analysing property in the twenty-first century through the prism of digital asset law. However, the results of a comparative analysis of different jurisdictional approaches presented by L. Lee (2024) show a more complex picture of the legal status of digital assets than was revealed in the study of the Ukrainian context alone. The critical analysis shows that the Ukrainian model of a "digital object" is a more radical attempt to integrate digital objects into the traditional legal system than the approaches used in other jurisdictions, which makes it both more ambitious and more problematic. The problematic application of the rules of property law to cryptoassets identified in the study is in line with the findings of P.Ç. Aksoy (2023) on the applicability of the rules of real law to cryptoassets from the standpoint of continental and Anglo-Saxon law. At the same time, the results of the analysis show that the Ukrainian model of a "digital object" creates more serious conceptual contradictions than the approaches considered in foreign studies. Particularly problematic is the application of vindication and negation claims to digital assets, as demonstrated in court practice, particularly in cases of seizure of cryptocurrencies as material evidence. The study of the legal status of digital financial assets as an object of civil rights conducted by T.G. ugli Pulatov (2024) demonstrates similar problems in different legal systems. The results of the analysis of the Uzbek experience indicate the general challenges faced by post-Soviet countries when trying to integrate digital assets into traditional legal frameworks. At the same time, the Ukrainian model appears to be more radical due to the use of the legal fiction of extending property rights to intangible objects, which creates unique legal conflicts.

The complexity of the correlation between the rights to NFTs and underlying objects identified in this study is confirmed by E.C. Lim (2024) on digital art, tokenised assets, and virtual property in the context of copyright. The results of the analysis of Ukrainian legislation demonstrate the lack of a clear distinction between these aspects, which creates additional legal risks. It is critical that the classification of digital content as "digital objects" in the Civil Code of Ukraine[1] directly contradicts the copyright regime of most such objects, which confirms the need to develop a special legal regime for different categories of digital objects. The conclusions regarding the legal nature of non-fungible tokens and property rights correlate with the results of a study by J. Kaisto *et al.* (2024) on tokenisation and property. However, the results of the analysis of Ukrainian legal regulation reveal more fundamental problems in determining the legal status of these objects. In particular, the absence of a distinction between the rights to the NFT itself and the rights to the underlying object creates legal uncertainty that may lead to the violation of both property and exclusive rights. Ukrainian legislation does not address the complex nature of NFTs as a hybrid object combining technological, artistic and legal aspects.

The legal issues of NFTs in the arts sector identified in the study are consistent with the findings of W. Jia & B. Yao (2024) on legal issues and case law. The results of the analysis demonstrate the need to develop special regulations for this area in Ukraine. It is necessary to regulate the relationship between NFT rights and copyright in basic works, which requires a cross-sectoral approach. The necessity of using digital assets to enforce intellectual property rights, substantiated in the study, is supported by C.A. Makridis & J.D. Ammons (2025), who consider the management of shared resources of large language models through digital assets. At the same time, the results of the study show that Ukrainian legislation does not consider these promising areas of development. The lack of regulation of governance tokens and decentralised autonomous organisations creates a legal vacuum for innovative models of intellectual property management in the digital environment.

[1] Civil Code of Ukraine. (2003, January). Retrieved from https://zakon.rada.gov.ua/laws/show/435-15.

The problems of the legal framework for new digital assets identified in the study correlate with the conclusions of C.P. Sempere (2025) on the legal framework for new digital assets, identities and data in the European single market. The results of the analysis demonstrate the need to adapt the Ukrainian legal system to European standards. At the same time, the study determined that the current Ukrainian Law of Ukraine No. 2074-IX[1] contains significant differences from the MiCA approach, including a unique classification of "secured/unsecured" assets, which may complicate future harmonisation with European law. A study of virtual property in the metaverse and challenges to res digitalis by J.P. Ricciardi (2023) revealed promising areas for the development of legal regulation of digital objects. The results of the analysis show that Ukrainian legislation is not ready to regulate complex virtual worlds and the metaverse, where digital objects may have multiple forms of existence and complex interconnections. The concept of a "digital object" is too simplistic to cover the diversity of objects in virtual environments.

The limitations of the current private law on digital assets identified in this study were confirmed by J. Soukupová (2024). However, the results of the analysis show that in the Ukrainian context, these restrictions are more critical due to the use of the unsuccessful legal fiction of a "digital object". Comparative analysis shows that most European legal systems avoid such a radical approach, preferring more flexible and adaptive regulatory mechanisms. The concept of property as a right of virtual objects, developed by J.A.T. Fairfield (2022), offers an alternative approach to research of the legal nature of digital objects, which consists in recognising virtual assets as objects of property rights regardless of their physical nature, with an emphasis on functional characteristics (exclusivity, transferability, stability). The results of the study show that the Ukrainian model partially borrows these ideas, but implements them through a problematic legal fiction. The critical analysis shows that the application of the concept of "virtual objects" requires a more in-depth identification of traditional legal categories than is done in Ukrainian legislation.

The need to redefine property rights in the context of NFTs, identified in the study, correlates with the findings of Á. Juhász (2023) on non-fungible tokens and property rights from a Hungarian perspective. The results of the study demonstrate that the Ukrainian model needs a more radical rethink. The comparative analysis shows that the Hungarian approach is more cautious and considers the specifics of NFTs as objects that combine technological and artistic aspects. The importance of adapting legal regulation to the Fourth Industrial Revolution, substantiated in this study, is supported by the works of V. Giang & V.T.M. Huong (2023), who analysed digital assets in the context of international integration. At the same time, the results show specific challenges for the Ukrainian legal system related to the need to simultaneously implement legal reforms and European integration processes. Critically, current Ukrainian regulation may create barriers to participation in global digital ecosystems.

A general analysis of international experience shows that most leading jurisdictions avoid radical changes in basic legal categories, preferring to create special legal regimes for digital objects. The Ukrainian model of a "digital object" is a unique but problematic attempt to integrate new technologies into the traditional legal system. The results of the study demonstrate the need to revise this approach and employ a more flexible and adaptive regulatory model that incorporates the diversity of digital objects and their specific legal needs.

Conclusions

A comprehensive analysis of the legal nature of digital objects has led to the conclusion that they represent a unique *sui generis* legal phenomenon which does not fully fit into classical civil law constructs. The study demonstrated that the attempt to apply the outdated legal fiction of "object" to digital objects, as enshrined in the Civil Code of Ukraine, was determined to be theoretically contradictory, created systemic conflicts with other laws, and proved to be practically ineffective, as evidenced by the first attempts at law enforcement in court practice. An analysis of the current legal regulation in Ukraine has shown that it is fragmented, incomplete and largely ineffective. The key problem was the ineffective status of the fundamental Law of Ukraine No. 2074-IX, which hindered the development of the legal market and left its participants without proper legal protection. At the same time, the simultaneous existence of several parallel and partially contradictory legal regimes created additional legal uncertainty for all digital market participants.

A comparative legal analysis of international experience has made it possible to identify three main regulatory models: restrictive (China), liberal (Switzerland, certain US states) and balanced (Germany, Japan, Singapore), which reflect different conceptual foundations of the State policy on digital assets. The study established that for Ukraine, as a candidate country for EU accession, it is strategically justified to prioritise the European MiCA model, incorporating the Swiss experience of technological neutrality and flexible licensing. A system of classification criteria for digital objects has been developed, including legal regime, functional purpose, technical substitutability, materiality, type of issuer, territory of circulation, and degree of regulation. This system can be used for the formation of differentiated

[1] Law of Ukraine No. 2074-IX "On Virtual Assets". (2022, February). Retrieved from https://zakon.rada.gov.ua/laws/show/2074-20.

legal regimes for different categories of digital assets depending on their specific characteristics and economic functions.

The study determined that to build an effective and modern system of legal regulation of digital objects in Ukraine, it is necessary to conceptually revise the approach enshrined in the Civil Code of Ukraine. The author establishes the expediency of abandoning the unsuccessful fiction of a "digital object" and supplementing Article 177 of the Civil Code of Ukraine with a new, independent category of civil rights objects called "digital assets" or "digital goods" with a clear definition of their intangible nature and establishment of the specifics of the legal regime through special legislation. The need to harmonise the terminology by unifying the definition of a "virtual asset" in all legal acts, incorporating international FATF standards and the functional classification of the MiCA Regulation, proved to be critical. The study has shown that the primary and urgent task is to adopt amendments to the Tax Code of Ukraine to establish set, comprehensible and competitive rules for taxation of transactions with virtual assets, which will enact the basic law and launch the process of forming a legal market. Prospects for further research include the legal regulation of decentralised autonomous organisations and governance tokens, the use of artificial intelligence in the field of digital assets, central bank digital currencies, personal data protection in blockchain systems, and the development of international instruments to harmonise the regulation of cross-border circulation of digital assets.

Acknowledgements

None.

Funding

The study was not funded.

Conflict of Interest

None.

References

[1] Aksoy, P.Ç. (2023). The applicability of property law rules for crypto assets: Considerations from civil law and common law perspectives. *Law, Innovation and Technology*, 15(1), 185-221. doi: 10.1080/17579961.2023.2184140.

[2] CFTC. (2015). *CFTC orders bitcoin options trading platform operator and its CEO to cease illegally offering bitcoin options and to cease operating a facility for trading or processing of swaps without registering*. Retrieved from https://www.cftc.gov/PressRoom/PressReleases/7231-15.

[3] Dmytryk, O. (2021). Virtual assets and digital assets: To the question of correlation of concepts. *Law and Innovation Society,* 17(2), 248-254. Retrieved from https://surl.li/seuavu.

[4] Fairfield, J.A.T. (2022). Tokenized: The law of non-fungible tokens and unique digital property. *Indiana Law Journal*, 97(4), article number 4.

[5] Feldman, J., Raykin, A., & Gove, J. (2021). *Delaware unclaimed property act applies to cryptocurrency*. Retrieved from https://surl.li/lncfgk.

[6] Fillman, A. (2025). *Update of German law aspects of crypto assets*. Retrieved from https://www.restructuring-globalview.com/2025/02/update-of-german-law-aspects-of-crypto-assets/.

[7] Financial Action Task Force. (n.d.). *FATF Recommendations*. Retrieved from https://surl.li/ngbucf.

[8] FINMA publishes guidelines on ICOs. (2018). Retrieved from https://surl.lu/tenkrt.

[9] FINMA. (n.d.). *Fintech approval*. Retrieved from https://surl.lu/bkksey.

[10] Garcia-Teruel, R.M., & Simón-Moreno, H. (2021). The digital tokenization of property rights. A comparative perspective. *Computer Law & Security Review*, 41, article number 105543. doi: 10.1016/j.clsr.2021.105543.

[11] Giang, V., & Huong, V.T.H. (2023). Digital assets in the context of the fourth industrial revolution, international integration, and Vietnamese law. *Cogent Social Sciences*, 9(1), article number 2187010. doi: 10.1080/23311886.2023.2187010.

[12] Guleykov, I.Yu. (2025). *Digital assets in civil turnover of Ukraine*. Kyiv: National Academy of Legal Sciences of Ukraine Scientific Research Institute of Private Law and Entrepreneurship named after Academician F.G. Burchak.

[13] Hrytsai, S. (2023). Prospects for introducing the concept of "digital things" and "digital content": Expanding the scope of regulation of virtual assets. *Krakow Lesser Poland Studies*, 38(2), 7-25.

[14] Hrytsay, S.O. (2022). The legal essence of the definition of "virtual assets" in the Law of Ukraine. *Electronic Scientific Publication "Analytical and Comparative Law"*, 1, 244-248. doi: 10.24144/2788-6018.2022.01.45.

[15] Internal Revenue Service. (n.d.). *Digital assets*. Retrieved from https://www.irs.gov/filing/digital-assets.

[16] Jia, W., & Yao, B. (2024). NFTs applied to the art sector: Legal issues and recent jurisprudence. *Convergence*, 30(2), 807-822. doi: 10.1177/13548565231199966.

[17] Juhász, Á. (2023). Time for rethinking? Non-fungible tokens and ownership rights from the Hungarian point of view. *Multidisciplinary Sciences,* 13(3), 36-46. doi: 10.35925/j.multi.2023.3.4.

[18] Kaaru, S. (2024). *Digital asset ownership legal in China: Shanghai judge*. Retrieved from https://coingeek.com/digital-asset-ownership-legal-in-china-shanghai-judge/.
[19] Kaisto, J., Juutilainen, T., & Kauranen, J. (2024). Non-fungible tokens, tokenization, and ownership. *Computer Law & Security Review*, 54, article number 105996. doi: 10.1016/j.clsr.2024.105996.
[20] Kiskis, M. (2024). Private law framework for blockchain. *Frontiers in Blockchain*, 7, article number 1205461. doi: 10.3389/fbloc.2024.1205461.
[21] Klyan, A., & Selivakin, I. (2023). *NFT in Ukraine: Technology and legal regulation*. Retrieved from https://eba.com.ua/nft-v-ukrayini-tehnologiya-ta-pravove-regulyuvannya/.
[22] Kostyuchenko, Ya.M. (2021). The experience of legal regulation of the development of the digital economy on the example of the leading countries of the world. *Actual Problems of Domestic Jurisprudence*, 3, 189-194. doi: 10.15421/392171.
[23] KYC Hub. (n.d.). *A global overview of cryptocurrency regulations in 2025*. Retrieved from https://www.kychub.com/blog/cryptocurrency-regulations-around-the-world/.
[24] Lawrange. (n.d.). *Cryptocurrency exchange license in Switzerland*. Retrieved from https://surl.li/glzjbi .
[25] Lee, L. (2024). Examining the legal status of digital assets as property: A comparative analysis of jurisdictional approaches. *SSRN*. doi: 10.2139/ssrn.4807135.
[26] Lim, E.C. (2024). Finding nemo: Digital art, tokenised assets, virtual property and the right of communication in copyright law. *Journal of World Intellectual Property*, 27(1), 69-87. doi: 10.1111/jwip.12290.
[27] Low, K., & Hara, M. (2024). *Cryptoassets and property*. Retrieved from https://surl.lu/aupjwk.
[28] Makridis, C.A., & Ammons, J.D. (2025). Governing the large language model commons: Using digital assets to endow intellectual property rights. *Journal of Institutional Economics*, 21, article number e19. doi: 10.1017/S1744137425000165.
[29] Michurin, E. (2022). Digital technology objects and their legal regulation. *Copernicus Political and Legal Studies*, 1(3), 22-29. doi: 10.15804/CPLS.20223.03.
[30] Michurin, E. (2025). The digital thing and other digital goods as objects of civil rights. *Uzhhorod National University Herald. Series: Law*, 1(88), 323-327. doi: 10.24144/2307-3322.2025.88.1.47.
[31] Moringiello, J.M., & Odinet, C.K. (2022). The property law of tokens. *Florida Law Review*, 74(4), 607-670. doi: 10.2139/ssrn.3928901.
[32] Neskorodzhena, L.L., Bon, B.O., & Kononets, O.M. (2024). Current state of legal regulation of cryptocurrencies in Ukraine. *Legal Scientific Electronic Journal*, 3, 197-200. doi: 10.32782/2524-0374/2024-3/44.
[33] NFT regulations in Japan. (2021). Retrieved from https://law.asia/nft-regulations-japan/.
[34] Pochynok, A. (2023). Structure of legal relations related to the circulation of virtual assets. *Bulletin of Lviv Polytechnic National University. Series: Legal Sciences*, 10(4), 219-231. doi: 10.23939/law2023.40.219.
[35] Popov, R.V. (2024). EU regulation of the virtual assets market. *Law and Public Administration*, 3, 295-300. doi: 10.32782/pdu.2024.3.42.
[36] Reiff, N. (2023). *Howey Test Definition: What it means and implications for cryptocurrency*. Retrieved from https://www.investopedia.com/terms/h/howey-test.asp.
[37] Ricciardi, J.P. (2023). *Virtual property in the metaverse: The upcoming challenges of res digitalis.* Lisbon: Catholic University of Portugal.
[38] Sempere, C.P. (2025). The legal framework for new digital assets, identities, and data spaces. Introduction. In *Governance and control of data and digital economy in the European Single Market: Legal framework for new digital assets, identities and data spaces* (pp. 3-21). Cham: Springer. doi: 10.1007/978-3-031-74889-9_1.
[39] Shapovalova, I. (2024). Internal challenges of regulating virtual assets in Ukraine. *Bulletin of the National Academy of Ukrainian Academies*, 9(104), 42-43.
[40] Slipchenko, A.S., & Slipchenko, S.O. (2024b). Determination of the legally significant essence of a digital thing in the Civil Law of Ukraine. *Forum Prava*, 78(1), 88-96. doi: 10.5281/zenodo.10870775.
[41] Slipchenko, S.O., & Slipchenko, A.S. (2024a). Legal regime of digital things in the context of the domestic concept of property rights. *Legal Scientific Electronic Journal*, 4, 216-223. doi: 10.32782/2524-0374/2024-4/50.
[42] Soukupová, J. (2024). *Digital assets and the limits of the current private law*. Prague: Charles University.
[43] TeraLex. (2022). *Terralex cross-border guide to crypto assets: Switzerland*. Retrieved from https://www.lalive.law/wp-content/uploads/2024/02/TerraLex-Website-report-27_Sep_2022_05_20_39_039.pdf.
[44] Trofymenko, D.S., & Fedorenko, D.O. (2022). Problematic aspects of understanding the legal nature of digital content. *European Law Science*, 1, 43-47.
[45] ugli Pulatov, T.G. (2024). Digital financial assets as an object of civil rights. *Uzbekistan Law Review,* 17(4), 53-59.
[46] Vinnyk, O.M. (2023). *Law of the digital economy of Ukraine.* Kyiv: Research Institute of Private Law and Entrepreneurship named after Academician F. G. Burchak of the National Academy of Sciences of Ukraine.

[47] Wyczik, J. (2025). Ownership in the 21st century: Property law of digital assets. *Information & Communications Technology Law*, 34(2), 187-206. doi: 10.1080/13600834.2024.2408917.
[48] Yarotsky, V.O. (2023). Concept and types of virtual assets that may be in circulation under the legislation of Ukraine. *Academic notes of the V.I. Vernadsky TNU. Series: Legal Sciences*, 34(4), 101-107. doi: 10.32782/TNU-2707-0581/2023.4/15.
[49] Zerov, K. (2023). *Digital things, digital content, NFT and copyright: the relationship within the expanded range of civil rights objects*. Retrieved from https://surl.li/sigjtu.
[50] Zetzsche, D.A., Annunziata, F., Arner, D.W., & Buckley, R.P. (2021). The markets in crypto-assets regulation (MiCA) and the EU digital finance strategy. *Capital Markets Law Journal*, 16(2), 203-225. doi: 10.1093/cmlj/kmab005.
[51] Zozulyak, O.I., & Maksymiv, L.M. (2024). Digital things as objects of civil rights: Updated approaches. *Law and Society*, 6, 45-52. doi: 10.32842/2078-3736/2024.6.7.

Цифрові об'єкти як новий вид об'єктів цивільних прав: теоретичні аспекти та критерії класифікації

Богдан Шуляка
Аспірант
Європейський університет
03187, просп. Академіка Глушкова, 42, м. Київ, Україна
https://orcid.org/0009-0006-2895-705X

Анотація
Метою дослідження був комплексний аналіз правової природи цифрових об’єктів як нового виду об’єктів цивільних прав, а також розроблення теоретичних засад їх ефективного правового регулювання в умовах цифрової трансформації суспільства. Методологічну основу дослідження становили: порівняльно-правовий метод – для аналізу підходів до правового регулювання цифрових об’єктів у правових системах Китаю, Швейцарії, Німеччини, Японії, Сінгапуру й США; формально-юридичний метод – для дослідження чинного українського законодавства; системний аналіз – для вивчення цифрових об’єктів як комплексного явища. У дослідженні встановлено, що цифрові об’єкти є унікальним правовим явищем, яке не повною мірою відповідає класичним цивілістичним конструкціям і потребує створення спеціального правового режиму. Виявлено фрагментарність і суперечливість українського правового регулювання, зокрема системні колізії між загальним речово-правовим режимом цифрових речей у Цивільному кодексі України й спеціальним режимом віртуальних активів у профільному законі. Доведено проблематичність застосування юридичної фікції поширення речового права на нематеріальні об’єкти, що створює правову невизначеність і ускладнює правозастосування. Аналіз судової практики встановив практичні проблеми застосування чинного законодавства, зокрема під час арешту криптовалют як речових доказів у кримінальних провадженнях. Обґрунтовано необхідність перегляду підходу шляхом відмови від фікції цифрової речі й створення окремої категорії цифрових активів з особливим правовим режимом. Практична цінність дослідження полягає у створенні теоретичного підґрунтя для вдосконалення правового регулювання цифрових об’єктів і можливості використання результатів у законотворчій діяльності, правозастосовній практиці та подальших наукових дослідженнях

Ключові слова:
кастодіальні сервіси; віртуальний актив; токени; блокчейн; транзакції

ЮРИДИЧНИЙ ЧАСОПИС
НАЦІОНАЛЬНОЇ АКАДЕМІЇ ВНУТРІШНІХ СПРАВ

Науковий журнал

Том 15, № 3, 2025

Заснований 2011 року. Виходить чотири рази на рік

Оригінал-макет видання виготовлено у відділі організації наукової діяльності
Національної академії внутрішніх справ

Відповідальний редактор:
Я. Шумко

Підписано до друку 29 вересня 2025 р. Формат 60*84/8
Умов. друк. арк. 12,7
Наклад 50 прим.

Адреса видавництва:
Національна академія внутрішніх справ
03035, пл. Солом'янська, 1, м. Київ, Україна
Тел.: +38 (044) 520-08-47
E-mail: naia@lawjournal.com.ua
https://lawjournal.com.ua/uk

LAW JOURNAL
OF THE NATIONAL ACADEMY OF INTERNAL AFFAIRS

Scientific Journal

Volume 15, No. 3, 2025

Founded in 2011. Published four times per year

The original layout of the publication is made in the Organisation of Scientific Activity of National Academy of Internal Affairs

Managing Editor:
Y. Shumko

Signed for print of September 29, 2025. Format 60*84/8
Conventional printed pages 12.7
Circulation 50 copies

Editors office address:
National Academy of Internal Affairs
03035, 1 Solomianska Sq., Kyiv, Ukraine
Tel.: +38 (044) 520-08-47
E-mail: naia@lawjournal.com.ua
https://lawjournal.com.ua/en