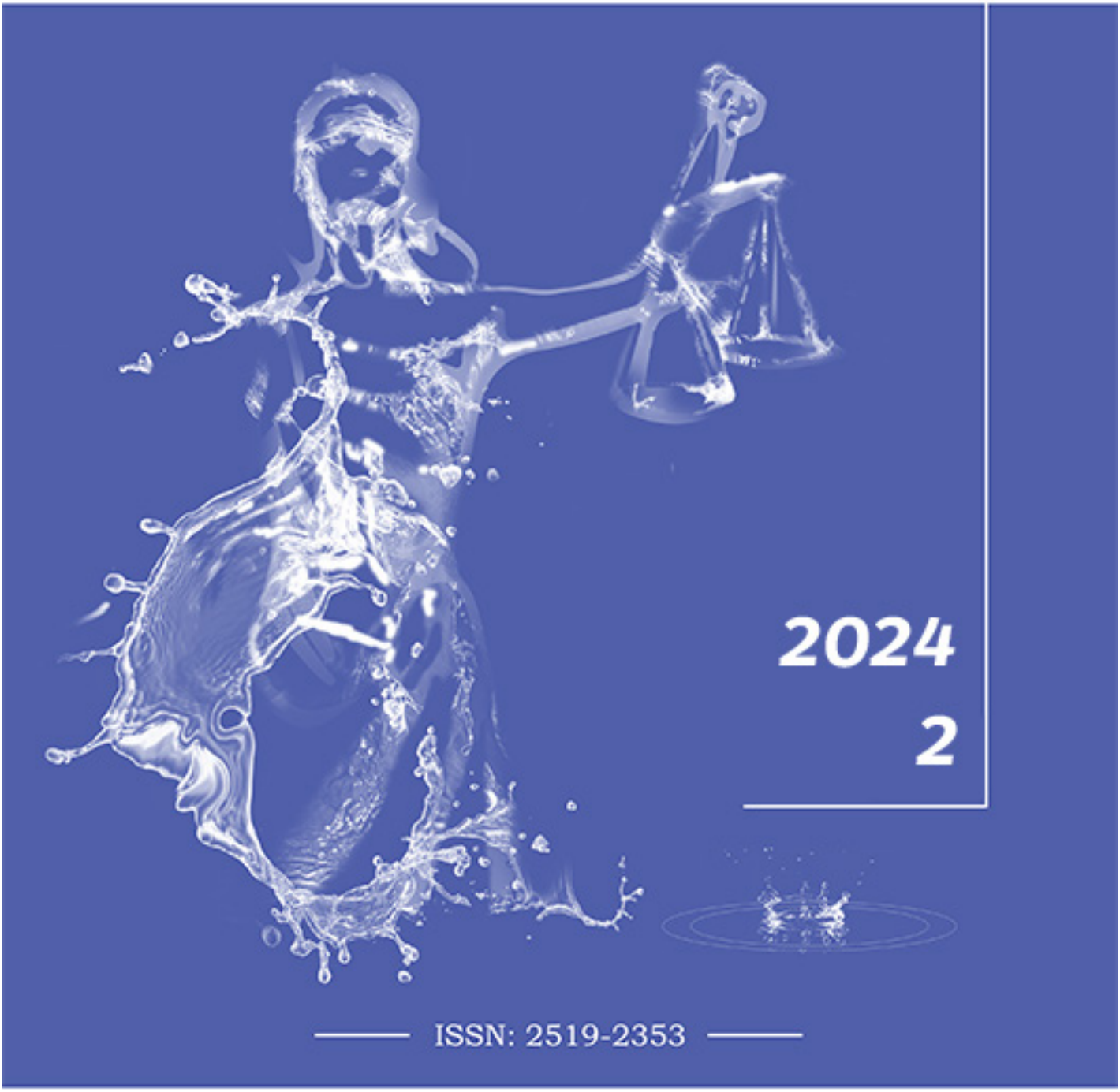
LEGAL HORIZONS

scientific and practical law journal



2024

2

ISSN: 2519-2353

ISSN: 2519-2353

Ministry of Education and Science of Ukraine
Scientific Institution «Legal Horizons»

LEGAL HORIZONS

Research-to-Practice Journal on Legal Science

Founded in 2008
Published four times per year

Vol. 21, No. 2

Kyiv – 2024

ISSN: 2519-2353

Certificate of state registrationof the print media
Series: KV No. 24828-14768 PR dated 21.04.2021

Collection of scientific works included in List of professional publications of Ukraine (Category "B")
in Law Sciences (Order of the Ministry of Education and Science of Ukraine No. 996 of July 11, 2017)

The collection is presentedin the following scientometric databases:
Index Copernicus, Google Scholar, Crossref, DOAJ,
VNLU, Sumy State University Repository

Legal Horizons: Research-to-Practice Journal on Legal Science / Ed. col.:
Yurii V. Harust (Ed.) et al. Sumy: Academic and Research Institute of Law of the Sumy State University
Vol. 21. No. 2. 81 p.
2024.

Founder and publisher:
Scientific Institution «Legal Horizons»
Kyiv, Ukraine
E-mail: info@legalhorizons.com.ua
www: https://legalhorizons.com.ua/en

FOREWORD

We are pleased to present Issue 21, No. 2 of Legal Horizons, which brings together a diverse array of scholarly contributions addressing contemporary challenges and opportunities in legal regulation, criminal justice, and technological innovation. The articles in this issue reflect the dynamic interplay between theoretical research and its application to emerging legal complexities in a globalized world.

The issue opens with **Andrii Matyash,** who explores the **"CHALLENGES AND PROSPECTS OF LEGAL REGULATION OF ADVERTISING ON ONLINE PLATFORMS"**. This article examines the increasing need for balanced and enforceable regulations in the digital advertising sector, addressing concerns over transparency, consumer protection, and fair competition.

Volodymyr Bezditnyi continues the discussion on digital markets with his article on the **"LEGAL REGULATION OF COMPETITION IN ONLINE TRADE AND THE ROLE OF MARKETPLACES AS TRADE ADMINISTRATORS".** He highlights the transformative influence of marketplaces in shaping trade dynamics, emphasizing the legal challenges of ensuring competitive fairness in these rapidly evolving environments.

Turning to criminal law and investigation, **Ganna Sobko** and **Irina Tesliuk** present an insightful analysis of **"THEORETICAL AND MODERN APPROACHES TO THE SEARCH FOR A SUSPECT".** Their work delves into the evolving investigative techniques and legal frameworks aimed at balancing efficiency with the protection of individual rights.

Tamara Kortukova and **Yelyzaveta Yemets** provide a timely contribution with their article on **"TEMPORARY PROTECTION IN THE EUROPEAN UNION: A LEGAL ANALYSIS".** This article sheds light on the EU's approach to managing humanitarian crises through temporary protection mechanisms, offering a critical examination of their legal foundations and practical implications.

In the realm of criminal law theory, **Vitaly Kuts** and **Yana Trynova** explore **"CONCERNING THE CONCEPT OF CRIMINAL OFFENSE AND ITS TYPES"**. Their article revisits fundamental questions of classification and definition, proposing frameworks to enhance clarity and consistency in criminal law.

Oleksandr Babikov addresses a crucial area of procedural law in his article on **"ADDITIONAL GUARANTEES OF OBSERVANCE OF THE RIGHTS AND FREEDOMS OF SPECIALLY DESIGNATED SUBJECTS DURING THE CONDUCT OF COVERT INVESTIGATIVE (SEARCH) ACTIONS".** The author critically evaluates existing safeguards and proposes enhancements to ensure the protection of fundamental rights in high-stakes investigations.

Finally, **Iryna Sopilko** examines one of the most pressing modern challenges in **"STRENGTHENING CYBERSECURITY IN UKRAINE: LEGAL FRAMEWORKS AND TECHNICAL STRATEGIES FOR ENSURING CYBERSPACE INTEGRITY".** Her work bridges the legal and technical domains, offering a comprehensive strategy to bolster national cybersecurity resilience.

We hope that this issue not only enriches academic discourse but also serves as a practical resource for legal practitioners, policymakers, and researchers. The diverse topics covered herein underscore the journal's commitment to addressing both longstanding and emerging issues in law through rigorous scholarship.

Thank you for your continued support of “Legal Horizons.”

Sincerely,

Yurii Harust,
Editor-in-Chief

CONTENTS

CHALLENGES AND PROSPECTS OF LEGAL REGULATION OF ADVERTISING ON ONLINE PLATFORMS

Andrii Matyash
International Law Firm "4B Ukraine"
02000, 4B Parkovo-Syretska Str., Kyiv, Ukraine
e-mail: andriy_matyash@pltch-sci.com
https://orcid.org/0009-0001-3599-6704

Abstract

Online advertisement provides marketers with a low-cost way of reaching large and diverse customers. Some of the spaces utilised by businesses to advertise products include Facebook, Google, and other social networking platforms. Like traditional media, online advertisement is subject to legal regulation. The paper aimed to critically evaluate the challenges and prospects of legal regulation of ads on online platforms. Through a well-conducted literature review of 20 scholarly sources, the article identified the primary challenges as the dynamic nature of technology, false advertising, data privacy issues, and problems related to safeguarding firms from defamatory interviews. Despite the challenges, the research found opportunities such as strengthening privacy laws, detecting false advertisements, and regulating the online marketing of unethical or potentially harmful products. Policymakers, particularly in Congress, must remain aware of the borderless nature of the Internet and the opportunities and threats it avails to regulatory authorities. Moreover, the research underscores the significance of training and capacity-building to guarantee compliance.

Key words: online advertising; laws; policies; Federal Trade Commission; data privacy.

1. Introduction

The rise of the digital age has transformed how businesses communicate with consumers, with online platforms like Facebook and Google becoming central to advertising strategies. These platforms offer unparalleled reach and cost-effectiveness, enabling marketers to target diverse audiences with precision. However, this shift to digital advertising has brought about new regulatory challenges, necessitating a reevaluation of existing legal frameworks. Unlike traditional media, the rapid evolution of technology and the global nature of the internet create complexities in ensuring that online advertisements adhere to legal standards.

As the online advertising ecosystem has grown, so too have concerns about its regulation. The borderless nature of the internet, coupled with the rapid pace of technological innovation, has made it increasingly difficult for existing legal frameworks to keep up. Unlike traditional forms of media, which are often subject to well-established regulatory regimes, online platforms operate in a more fluid and dynamic environment. This has given rise to a range of issues that are unique to the digital age, including challenges related to data privacy, the spread of false or misleading information, and the potential for defamatory content to be amplified through social networks.

In conclusion, while the regulation of online advertising presents numerous

challenges, it also offers opportunities for creating a safer and more transparent digital environment. As technology continues to evolve, so too must the legal frameworks that govern it, ensuring that online platforms can continue to be a force for good in the global marketplace.

This article delves into the intricate landscape of legal regulation for online advertising, exploring the challenges and opportunities that have emerged. By conducting a comprehensive review of scholarly literature, the paper identifies key issues such as the fast-paced technological changes, the prevalence of false advertising, data privacy concerns, and the risks of defamatory content. At the same time, it highlights potential advancements in policy and regulation that could address these issues, emphasizing the need for robust privacy laws, effective detection of misleading advertisements, and tighter control over the marketing of unethical products. The discussion extends to the role of policymakers, particularly in navigating the borderless nature of the internet, and the importance of ongoing education and training to ensure compliance in this dynamic environment.

The article aims to explore issues such as technological advancements, false advertising, data privacy concerns, and the potential for defamatory or unethical content, all of which complicate regulatory efforts. Additionally, the article seeks to examine the prospects for improving regulation in this field, including opportunities to strengthen privacy laws, enhance detection of misleading advertisements, and develop strategies for managing the marketing of harmful products. Through this analysis, the article intends to provide insights and recommendations for policymakers on how to effectively regulate online advertising in a way that balances innovation with consumer protection and legal compliance.

2. Materials and Methods

The article was grounded in a comprehensive collection of scholarly materials. The research incorporated theoretical analysis to explore how traditional legal doctrines, such as contract law, tort law, and intellectual property law, are being applied and adapted to the digital context. This analysis helped in understanding the foundational legal principles that underpin the regulation of online advertising. This method was used to gather and synthesize current knowledge, theories, and findings on the subject, providing a foundation for understanding the challenges and prospects in this area. Through the literature review, the research critically examined various legal frameworks, regulatory challenges, and potential solutions. This method involved evaluating the effectiveness of existing laws, identifying gaps, and analyzing how technological advancements impact the regulation of online advertising.

The study examined significant case law where regulatory bodies or courts have ruled on issues related to online advertising. This included landmark cases that set important precedents in areas such as data privacy, deceptive advertising, and cross-border jurisdiction. he impact of these rulings on the development and enforcement of online advertising regulations was assessed, providing practical insights into how legal principles are applied in practice. The research likely involved comparing different legal approaches and regulations across various jurisdictions, such as comparing the GDPR in the European Union with U.S. regulations. This method helped identify best practices and potential areas for improvement in global and national regulatory frameworks. The study may have employed theoretical analysis to explore underlying legal principles, doctrines, and concepts relevant to online advertising. This approach would allow for a deeper understanding of how existing legal theories apply to the rapidly evolving digital environment.

The research also involved analyzing current policy proposals and discussions within legislative bodies, particularly in areas like data privacy and consumer protection. This helped in identifying future regulatory trends and potential legislative changes. The views and positions of various stakeholders, including regulators, industry representatives, and consumer advocacy groups, were considered to provide a balanced perspective on the prospects of legal regulation.

These methods collectively enabled the researchers to identify the key challenges in regulating online advertising, assess the effectiveness of current legal frameworks, and propose future regulatory strategies. While the research methodology was comprehensive, it is important to acknowledge certain limitations. The fast-evolving nature of technology and online advertising means that some of the legal challenges identified may evolve rapidly, potentially affecting the relevance of the findings. Additionally, the comparative analysis was limited to major jurisdictions, which may not fully capture the global diversity of regulatory approaches.

3. Results and Discussion

3.1. Challenges of legal regulation of advertising on online platforms

Online platforms have become instrumental sources of advertisement due to their cost-effectiveness and ease of use. Virtually any well-established company today uses social media or the Internet in general to reach customers. However, compared to traditional platforms like television and radio, the Internet has minimal regulations or restrictions. In this regard, legal regulators such as the Federal Trade Commission (FTC) might experience challenges tracking falsehood in ads or the protection of data and enhancing its security. Despite the obstacles, policymakers in federal and state governments have many opportunities to improve effectiveness and efficiency in the regulation of advertisements on online platforms. The article will critically evaluate the outstanding issues in legal regulations of online ads and some of the areas that authorities can capitalise on in the near and long-term future.

Since most advertising occurs on the online platform, guided by dynamic technology, regulation by authorities can become extremely difficult. The Internet is one of the most significant attributes of globalisation. The platform has enabled individuals to connect regardless of their geographical locations (Foley, 2020). Despite its usefulness in advertising, national authorities have found it increasingly challenging to regulate advertising in online spaces. Dommett and Zhu (2022) argued that it is extremely challenging to exercise national control over the Internet. Furthermore, many governments, including the United States, face logistical barriers in their quest to control online advertising due to the complex and dynamic nature of digital technology (Dommett & Zhu, 2022). Some of the giant online advertisers in the market today include Facebook and Google. Although these companies originated in the United States, the borderless nature of the Internet means that online advertisers cannot adopt the specific laws and policies of a country (Chapdelaine & Manzerolle, 2021). The ubiquitous and often clandestine nature of the web makes it almost impossible for regulators like the FTC to police what happens on the Internet as far as marketing tactics are concerned. Furthermore, with the advancement of new and sophisticated technologies such as artificial intelligence and machine learning, online advertising has become more efficient and personalised (Zarouali et al., 2022). Accordingly, regulators might not have the privilege to evaluate everything that online advertisers do to market their products.

Implementing policies on false advertising remains another significant challenge facing regulators of online advertisement in the US market. The Lanham Act is one of the legal frameworks that prohibits false advertising by allowing civil lawsuits against

perpetrators who misrepresent the qualities, characteristics, and nature of products and services (Ullrich, 2021). As a result, the Lanham Act is vital in protecting consumer rights. One of the most significant areas that have frustrated FTC's efforts in combating deceptive practices in advertising is the aspect of online reviews. Changchit et al. (2022) argued that online reviews are instrumental in guiding purchase decisions. A business with more positive reviews listed on an online platform like Google, Yelp, and TripAdvisor is likely to attract many new and existing customers (Tayeen et al., 2021). Despite the significance of these platforms, many organisations have reverted to dishonest reviews aimed at promoting subpar or mediocre products. Some organisations have gone to the extent of rating their products as five-star in order to attract unsuspecting customers. Besides undermining the customers' collective power, such practices have severe legal ramifications. However, the FTC finds it increasingly challenging to crack down on these predatory behaviours because it is difficult to differentiate between genuine and dishonest reviews.

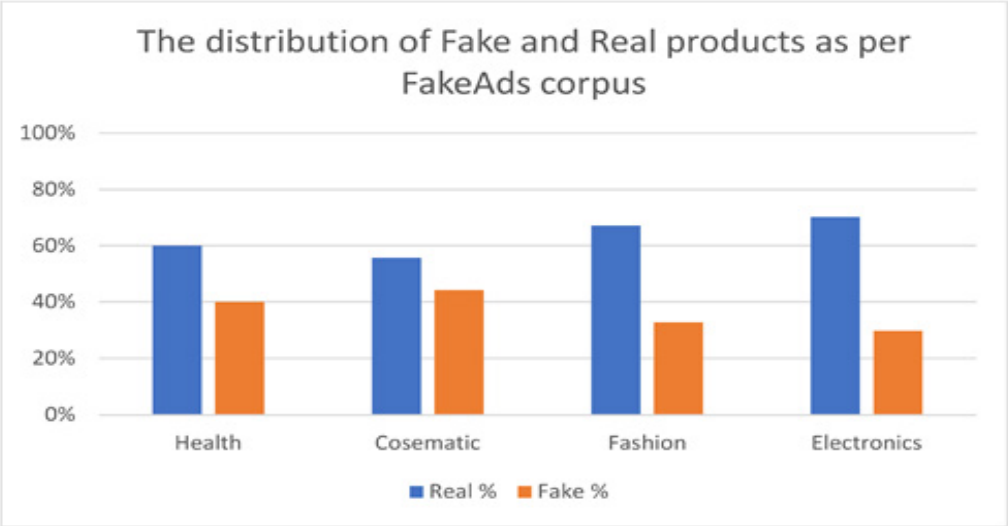


Figure 1. Proportion of fake ads in different fields in the american market[1]
Retrieved from: Alnazzawi, N., Alsaedi, N., Alharbi, F., & Alaswad, N. (2022). Using social media to detect fake news information related to product marketing: The FakeAds Corpus. Data, 7(4), 44.

Another significant challenge affecting online advertising relates to the enhancement of data privacy and user protection. The advancement and growth of the Internet have seen a rise in personalised advertisement (Zarouali et al., 2022). Marketers use sophisticated technologies to gather personal data related to geographical location, consumer preferences, behaviour, and patterns (Casas-Rosal et al., 2023). Such data is essential in ensuring that marketers provide consumers with specific marketing messages that align with their values and perspectives, increasing the likelihood of purchasing. However, the intrusive behaviour associated with the personalised marketing scheme can violate the data privacy and user protection policies and laws (Chandra et al., 2020). Each state in the US has created privacy policies aimed at safeguarding the interests of consumers. An example is the California Consumer Privacy Act (CCPA). The CCPA provides consumers with broad control over the personal data that enterprises collect about them (Mulgund et al., 2021). The FTC is in charge at the federal level. In 2019, the FTC was embroiled in a case with Facebook for its practices that jeopardised consumer privacy. According to FTC, Facebook used deceptive settings and disclosures that undermined the privacy of consumers, including allowing third-party apps to access their information (Hazlett,

1 the cosmetic industry has the highest proportion of fake ads, followed by health

2023). Such cases demonstrate the difficulties of controlling online advertising, especially when it violates the privacy of the clients. Thus, the FTC must ensure that businesses balance their needs for accurate advertising and protection of customer privacy.

Furthermore, regulatory authorities have significant challenges safeguarding the reputation of companies that might rely on online advertising to market their products. In the age of the Internet, companies are increasingly using social media platforms to market products, including Facebook, X.com, YouTube, and Instagram. Legal frameworks such as the Consumer Review Fairness Act of 2016 protect consumers in their quest to provide honest reviews and feedback about products and services (Martínez, 2021). However, in some instances, negative reviews can harm or even de-market a product, wasting the efforts and the resources that organisations have placed in the advertisement endeavour. Consumers can do this through comments, reviews, feedback, and dislikes, which other potential users can see. Most companies have expressed fear that some malicious consumers can weaponise the customer review and feedback mechanism, causing potential defamation. Besides suffering severe damage, these companies might find it challenging to sue the consumer due to overly protecting policies such as the Consumer Review Fairness Act of 2016 (Martínez, 2021). In this regard, policymakers need to clearly delineate between negative review and defamation to prevent malicious actors from taking advantage of the meaningful provision. Accordingly, this will ensure that consumers advertise their products without the fear that ill-intentioned people will take advantage of the process.

3.2. Future directions in legal regulation of online advertising

The future of legal regulation in online advertising is a critical issue, particularly as digital marketing continues to evolve and become more deeply embedded in the everyday experiences of consumers. With the rise of personalized advertisements driven by big data, there is a pressing need for robust privacy policies and laws that can keep pace with technological advancements. The US government has the opportunity to strengthen privacy policies and laws in the wake of increasing personalised advertisements. Big data has risen to become an integral part of marketing (Gupta et al., 2021). The explosion of big data has transformed how businesses approach marketing. Companies are investing billions of dollars into data collection and analysis to ensure their advertising strategies are as targeted and effective as possible. Companies are now investing billions of dollars in gathering data that is helpful in ensuring that their marketing endeavour is as accurate as possible. However, this comes at the expense of the individual's privacy. The FTC has made concerted efforts to ensure that the consumer is protected from predatory and unethical ventures by marketers and advertisers. However, the current regulatory landscape in the U.S. is fragmented, with individual states developing their own privacy laws that vary in scope and effectiveness. This patchwork approach creates inconsistencies in consumer protection and complicates compliance for businesses operating across state lines. For example, while California's Consumer Privacy Act (CCPA) offers comprehensive protections, other states have far less stringent regulations, leaving many consumers unprotected. (Quach et al., 2022). Online trade occurs across states and countries and knows no boundary. In this regard, there is a need to harmonise these laws to create consistency in accountability and responsibility. Although the autonomy of states to make policies and laws is sacred and must be respected, lawmakers need to realise the globalised nature of online advertising and its borderless ramifications. Thus, there is an opportunity for state and federal governments to work together to guarantee the uniform application of privacy laws to prevent the unethical collection of personal data by marketers and advertisers.

The government can work closely with social media platforms to ensure that the

advertisements aired on the platforms reflect the values of truthfulness, accuracy, and honesty. Fake advertisement has severe implications for the overall well-being of the buyers (Allami et al., 2021). For instance, using deception to advertise food or cosmetic products could have negative ramifications on an individual's well-being or life. With social media ads increasingly becoming ubiquitous, marketers will benefit from social media algorithms powered by machine learning and automation to detect inauthentic advertising (Abdallah et al., 2021). To combat this, there is a growing opportunity to leverage technology, particularly artificial intelligence (AI) and machine learning, to detect and prevent false advertising. For instance, X.com, formerly Twitter, has a powerful algorithm that detects fake news and allows readers of a post to provide context for posts that promote falsehood (Guimarães et al., 2021). The same concept could apply to marketing strategies that use falsehood to gain traction. Using technology in this way is essential because it enhances compliance with the law. FTC can easily take action against perpetrators of falsehood in their marketing endeavours. More importantly, this strategy directly empowers the consumers to know the authenticity behind a specific ad on social media pages.

By integrating these technological solutions into the regulatory framework, the FTC and other regulatory bodies can more effectively enforce advertising standards. This approach not only improves compliance but also empowers consumers by providing them with the tools and information needed to discern the authenticity of online advertisements. Moreover, such a system would place the onus on advertisers to ensure the truthfulness of their claims, knowing that their ads will be subject to rigorous scrutiny by both automated systems and regulatory authorities.

The government should strengthen regulations that prevent companies from misusing online advertisements to promote unethical business practices. A business can be legal but has moral implications for society, especially if it fosters addiction and threatens to destroy the moral fabric of society. Beyond privacy and false advertising, another critical area for future regulatory attention is the use of online advertising to promote unethical business practices. Certain industries, such as gambling and alcohol, pose significant risks to public health and social well-being. While these industries are legal, their advertising practices can have profound moral implications, particularly when they target vulnerable populations. One example is the gambling industry. Gambling has grown in the US at a very rapid rate over the last few years. Under the federal law, gambling is legal. However, each state has the freedom to develop further restrictions depending on the type of advertisement (Torrance et al., 2021). Research shows that excessive consumption of gambling content could lead to addiction, leading to psychological and financial problems for an individual (Allami et al., 2021). The federal government has the opportunity to play a more active role in regulating such advertising. This could involve setting national standards that limit the frequency and content of ads for products like gambling, alcohol, and tobacco. For example, regulations could prohibit advertisements that glamorize gambling or make misleading claims about the likelihood of winning. Additionally, there could be caps on the number of gambling-related ads that a consumer is exposed to within a given timeframe, reducing the risk of developing addictive behaviors.

These regulatory efforts could extend to other risky products, ensuring that advertising practices align with public health objectives and social responsibility. By doing so, the government would strike a balance between the economic benefits of these industries and the need to protect society from the negative consequences of their advertising practices.

Although most legal frameworks seek to safeguard the interests of the consumer, the government must also ensure that companies are equally protected. Businesses depend

on the ads to reach a wider market audience and compete fairly with their counterparts (Trachuk et al., 2021). Quality ads on and off social media platforms are expensive and require heavy investments. In this regard, the government must strengthen the Consumer Review Fairness Act of 2016 and remove loopholes that might prevent a company from suing an individual whose feedback or review of a business results in defamation or damage to the brand's reputation (Narciso, 2022). The law should clearly delineate between constructive criticism and negative review with potential defamatory remarks that de-market an organisation and prevent it from capitalising on its advertisement endeavours in the online space (Martínez, 2021). Another way to safeguard the interests of the companies is through training and capacity-building on the legal framework. With the advent and expansion of online advertising marketplaces, many small and medium enterprises have joined the bandwagon, utilising the Internet to meet consumers worldwide. Thus, FTC and other authorities can conduct frequent training using resources such as webinars to educate companies on the strict regulatory environment of online advertisement.

In addition to legal protections, businesses could benefit from increased training and capacity-building initiatives that help them navigate the complex regulatory environment. As more small and medium-sized enterprises (SMEs) enter the online advertising space, there is a growing need for education on legal compliance. The FTC, along with other regulatory bodies, could offer webinars, workshops, and other resources to help businesses understand their rights and responsibilities in the digital marketplace. Such efforts would not only protect businesses from legal pitfalls but also promote fair competition and high standards in online advertising.

In conclusion, the future of legal regulation in online advertising holds both challenges and opportunities. By strengthening privacy laws, leveraging technology to combat false advertising, regulating ads for unethical practices, and protecting businesses, governments can create a more balanced and effective regulatory framework. As digital advertising continues to evolve, it is crucial that legal frameworks adapt to ensure that the online marketplace remains a safe, fair, and trustworthy environment for all stakeholders.

Conclusions

The regulation of online advertising presents a complex and evolving challenge in the digital age, where the rapid pace of technological advancements has outstripped the capacity of traditional legal frameworks to keep up. As the analysis in this article demonstrates, the current regulatory model has significant weaknesses that undermine its effectiveness in protecting consumers' rights and ensuring fair advertising practices. These shortcomings are particularly evident in the areas of data privacy, the proliferation of false advertising, and the fragmented regulatory environment, especially in markets like the United States, where state-level inconsistencies further complicate enforcement.

One of the most pressing issues identified in this research is the failure of existing regulations to adequately safeguard consumer privacy in the era of big data and personalized advertising. The ability of online platforms to collect and analyse vast amounts of personal information has enabled highly targeted advertising strategies that, while effective from a marketing perspective, often infringe on individuals' privacy rights. The lack of robust legal protections in this area has left consumers vulnerable to exploitation, with their data being used in ways they may not fully understand or consent to. This is compounded by the fact that many consumers are unaware of the extent to which their data is being harvested and utilized for advertising purposes, highlighting the need for greater transparency and stricter regulatory oversight.

Another significant challenge is the pervasive issue of false advertising on online

platforms. The internet's global reach and the ease with which information can be disseminated make it an ideal breeding ground for deceptive marketing practices. From fake ads to misleading product claims, these practices not only harm consumers but also erode trust in digital advertising as a whole. The current legal framework has struggled to keep pace with the innovative tactics used by bad actors, resulting in a regulatory environment that is often reactive rather than proactive. The inability to effectively curb false advertising has serious implications, not only for consumer protection but also for the integrity of online markets.

The borderless nature of the internet exacerbates these regulatory challenges. Inconsistent regulations across different jurisdictions create loopholes that can be exploited by companies looking to bypass stricter legal requirements. This is particularly evident in the United States, where varying state laws create a patchwork of regulations that are difficult to enforce uniformly. The lack of a cohesive, nationwide approach to online advertising regulation makes it easier for companies to engage in practices that might be illegal in one state but permissible in another, further complicating efforts to protect consumers and ensure fair competition.

Despite these significant challenges, there are also promising opportunities for improving the regulation of online advertising. One of the most critical areas for future development is the enhancement of data protection laws. Strengthening these regulations will be essential in addressing the privacy concerns associated with big data and personalized advertising. By establishing clear guidelines on data collection, storage, and usage, and by enforcing stringent penalties for violations, regulators can help ensure that consumers' personal information is handled responsibly and ethically.

Another key opportunity lies in the development of more sophisticated mechanisms for detecting and preventing false advertising. Advances in technology, particularly in artificial intelligence and machine learning, offer the potential to create automated systems that can identify inauthentic ads with greater accuracy and efficiency. By leveraging these technologies, regulators can move from a reactive to a proactive stance, intervening before false advertisements have a chance to cause harm.

Furthermore, there is a growing recognition of the need to regulate advertisements that promote harmful or unethical products and behaviors. Governments should focus on strengthening laws that prevent predatory advertising practices, particularly those that target vulnerable populations. For example, stricter regulations could be implemented to curb ads related to gambling, smoking, or other activities that pose significant social and health risks. By doing so, regulators can help protect consumers from being lured into potentially destructive behaviors by manipulative marketing tactics.

In addition to protecting consumers, there is also a need to consider the rights of businesses in the regulatory framework. Companies must be shielded from defamatory content and malicious campaigns that can damage their reputation and brand. This requires a balanced approach that safeguards free speech while also providing legal recourse for businesses that are unfairly targeted by false or derogatory claims.

In conclusion, while the current legal framework for regulating online advertising has significant gaps, these challenges also present opportunities for reform. By enhancing data protection, improving the detection of false advertising, and strengthening laws against predatory practices, regulators can create a more effective and equitable system. This will not only protect consumers but also foster a healthier and more trustworthy online advertising ecosystem. As technology continues to evolve, it is imperative that legal frameworks adapt in tandem, ensuring that the digital marketplace remains a space where both consumers and businesses can thrive securely and fairly.

References

Abdallah, A. (2021). Fake news, false advertising, social media and the tourism industry. *International Journal of Development Research, 11*(7), 48999-49003.

Allami, Y., Hodgins, D. C., Young, M., Brunelle, N., Currie, S., Dufour, M., & Nadeau, L. (2021). A meta-analysis of problem gambling risk factors in the general adult population. *Addiction, 116*(11), 2968-2977.

Casas-Rosal, J. C., Segura, M., & Maroto, C. (2023). Food market segmentation based on consumer preferences using outranking multicriteria approaches. *International Transactions in Operational Research, 30*(3), 1537-1566.

Changchit, C., Klaus, T., & Lonkani, R. (2022). Online reviews: What drives consumers to use them? *Journal of Computer Information Systems, 62*(2), 227-236.

Chapdelaine, P., & Manzerolle, V. (2021). The regulation of media and communications in the borderless networked society. *Laws, 10*(4), 78.

Dommett, K., & Zhu, J. (2022). The barriers to regulating the online world: Insights from UK debates on online political advertising. *Policy & Internet, 14(*4), 772-787.

Foley, J. P. (2020). Ethics on the Internet. J*ournal of Interdisciplinary Studies, 32(*1/2), 179-192.

Guimarães, N., Figueira, Á., & Torgo, L. (2021). Can fake news detection models maintain the performance through time? A longitudinal evaluation of Twitter publications. *Mathematics, 9(*22), 2988.

Gupta, S., Justy, T., Kamboj, S., Kumar, A., & Kristoffersen, E. (2021). Big data and firm marketing performance: Findings from knowledge-based view. *Technological Forecasting and Social Change, 171*, article number 120986.

Hazlett, T.W. (2023). Populist antitrust: The Case of FTC v. Facebook. *The Antitrust Bulletin, 68*(2), 250-262.

Martínez Otero, J. M. (2021). Fake reviews on online platforms: Perspectives from the US, UK and EU legislation. *SN Social Sciences, 1(*7), 181.

Mulgund, P., Mulgund, B. P., Sharman, R., & Singh, R. (2021). The implications of the California Consumer Privacy Act (CCPA) on healthcare organisations: Lessons learned from early compliance experiences. *Health Policy and Technology, 10*(3), article number 100543.

Narciso, M. (2022). The unreliability of online review mechanisms. *Journal of Consumer Policy, 45*(3), 349-368.

Quach, S., Thaichon, P., Martin, K. D., Weaven, S., & Palmatier, R. W. (2022). Digital technologies: Tensions in privacy and data. *Journal of the Academy of Marketing Science, 50*(6), 1299-1323.

Tayeen, A. S. M., Mtibaa, A., Misra, S., & Biswal, M. (2021). Impact of locational factors on business ratings/reviews: A Yelp and TripAdvisor study. *Big Data and Social Media Analytics: Trending Applications,* 25-49.

Torrance, J., John, B., Greville, J., O'Hanrahan, M., Davies, N., & Roderique-Davies, G. (2021). Emergent gambling advertising; a rapid review of marketing content, delivery and structural features. *BMC Public Health, 21*, 1-13.

Trachuk, T., Vdovichena, O., Andriushchenko, M., Semenda, O., & Pashkevych, M. (2021). Branding and advertising on social networks: Current trends. *International Journal of Computer Science & Network Security, 21*(4), 178-185.

Ullrich, Q. J. (2021). Is this video real? The principal mischief of deepfakes and how the Lanham Act Can address It. *Columbia Journal of Law & Social Problems, 55*, 1-9.

Zarouali, B., Dobber, T., De Pauw, G., & de Vreese, C. (2022). Using a personality-profiling algorithm to investigate political microtargeting: Assessing the persuasion effects of personality-tailored ads on social media. *Communication Research, 49*(8), 1066-1091.

DOI: https://doi.org/10.54477/LH.25192353.2024.2.pp.18-25

LEGAL REGULATION OF COMPETITION IN ONLINE TRADE AND THE ROLE OF MARKETPLACES AS TRADE ADMINISTRATORS

Volodymyr Bezditnyi
International Law Firm "4B Ukraine"
02000, 4B Parkovo-Syretska Str., Kyiv, Ukraine
e-mail: volodymyr_bezditnyi@pltch-sci.com
https://orcid.org/0009-0009-1592-7670

Abstract
Competition is an essential attribute of the capitalist market. The United States has created laws and policies that promote fair competition, preventing monopolistic behaviours. The online trade segment that incorporates bigwigs like Amazon and eBay has not been left out. Federal authorities like the Federal Trade Commission (FTC) demand that these companies refrain from anticompetitive practices. The paper aimed to investigate the legal regulation of competition in online trade and the role of marketplaces as trade administrators. Through a well-conducted review of the literature of 20 sources, the articles make several groundbreaking discoveries. The online environment is regulated using policies and laws like the Sherman Antitrust Act, the Consumer Review Fairness Act of 2016 (CRFA), the Clayton Act, and the Antitrust Criminal Penalty Enhancement and Reform Act (ACPERA) of 2004. Furthermore, this research has shown that online marketplaces are instrumental in trade administration through efforts such as enhancing privacy, promoting transactions, and providing a framework for conflict resolution.

Keywords: online trade; competition; monopoly; trade administrators; regulation.

1. Introduction

In the capitalist market economy, competition serves as a fundamental driving force, ensuring innovation, efficiency, and consumer choice. The United States has historically enacted a range of laws designed to uphold fair competition and prevent monopolistic practices. As the market has evolved, so too have the arenas of commerce, with online trade emerging as a dominant and transformative force. Online trade has expanded since the advent of the Internet and Internet 2.0. Today, the United States online market has taken over trade, threatening to replace traditional brick-and-mortar sales. Most companies that operate traditional stores have also transitioned to the online platform to remain competitive and align with the consumers' needs (Inoue & Hashimoto, 2022). America has some of the biggest firms occupying the online trade space. Examples include Amazon, eBay, Etsy, Target, and Walmart (Yarova & Yurchenko, 2023

As e-commerce platforms and digital marketplaces become central to global trade, understanding the legal frameworks that govern competition within these spaces is crucial. The rapid expansion of online trade has necessitated new approaches to regulation, as traditional competition laws often fall short in addressing the complexities of digital marketplaces. These platforms operate at the intersection of various regulatory challenges, including antitrust issues, consumer protection, and data privacy.

Federal authorities, including the Federal Trade Commission (FTC), have sought to extend competition laws to the online domain, addressing issues such as monopolistic behavior and anti-competitive practices. As trade administrators, online marketplaces wield significant influence over market access, pricing strategies, and the visibility of

goods and services. Their dual role as both facilitators and regulators of trade introduces unique regulatory challenges that differ markedly from those faced by traditional brick-and-mortar retail environments. This article seeks to illuminate these challenges by examining how existing legal frameworks apply to online marketplaces and exploring the need for tailored regulatory approaches that address the specific characteristics of digital trade.

As trade administrators, online marketplaces wield significant influence over market access, pricing strategies, and the visibility of goods and services. Their dual role as both facilitators and regulators of trade introduces unique regulatory challenges that differ markedly from those faced by traditional brick-and-mortar retail environments. This article seeks to illuminate these challenges by examining how existing legal frameworks apply to online marketplaces and exploring the need for tailored regulatory approaches that address the specific characteristics of digital trade.

The article critically evaluates the legal regulation of competition in online trade while also interrogating how the marketplace has become an influential trade administrator.

By analyzing case studies, current legal practices, and emerging trends, this study aims to provide a comprehensive overview of the regulatory landscape governing online competition. The discussion will highlight the balance between fostering innovation and ensuring fair competition, ultimately contributing to a more nuanced understanding of how legal regulation can evolve to meet the demands of the digital marketplace era.

2. Web traffic in online trade: A regulatory perspective

The significant disparity in web traffic among leading online trade firms not only reflects their market influence but also underscores critical legal and regulatory considerations. Understanding how traffic volumes relate to competition and market power is essential for assessing the effectiveness of existing legal frameworks and identifying areas requiring regulatory attention.

The data reveals that Amazon, with 4.81 billion monthly visits, stands as a dominant force in the online marketplace. This level of web traffic signifies a substantial market share, raising important antitrust concerns. Under U.S. antitrust laws, particularly the Sherman Antitrust Act and the Clayton Act, practices that may hinder competition or create monopolistic conditions are scrutinized. Amazon's dominance necessitates careful examination to ensure it does not engage in anti-competitive practices such as predatory pricing, unfair competition, or exclusionary tactics that could stifle competition and harm consumers.

The substantial web traffic of other major players, such as eBay (1.18 billion visits) and Walmart (387.2 million visits), also positions them as significant market entities. While their competitive practices are subject to scrutiny, their relatively lower traffic compared to Amazon suggests a less pronounced market dominance. However, their competitive strategies, including exclusive partnerships or platform policies, are still relevant in assessing their impact on market competition and consumer choice.

The considerable web traffic of platforms like Etsy (373.2 million visits) and Wayfair (98.98 million visits) highlights their substantial role in their respective market segments. Consumer protection laws, such as the Consumer Review Fairness Act of 2016 (CRFA), play a critical role in ensuring that these platforms maintain fair practices. The CRFA, for example, prohibits businesses from using non-disclosure agreements to suppress negative reviews, ensuring that consumer feedback remains transparent and reliable.

With significant traffic, these platforms are also tasked with upholding privacy and data protection standards. The Federal Trade Commission (FTC) enforces regulations that require platforms to secure consumer data and provide clear privacy policies. The volume of visits implies a large amount of consumer data, which necessitates stringent adherence to data protection laws and practices.

The Antitrust Criminal Penalty Enhancement and Reform Act (ACPERA) of 2004 and other regulatory frameworks play a crucial role in addressing anti-competitive behaviors. As online platforms continue to evolve, regulatory bodies must adapt existing laws to address emerging challenges such as algorithmic bias, platform monopolization, and data monopolies. The significant web traffic of leading platforms suggests a need for updated regulations that account for the unique dynamics of digital trade.

Table 1. Firms in Online trade and their visits per month

Name	Category	Visits Per Month
Amazon	General	4.81B
eBay	General	1.18B
Walmart	General	387.2M
Etsy	Arts, Crafts, & Gifts	373.2M
Target	General	165.9M
Wayfair	Homewares	98.98M

The web traffic data for prominent online trade firms underscores the importance of rigorous legal and regulatory oversight. As these platforms wield substantial market power and influence, ensuring fair competition and consumer protection remains paramount. The analysis highlights the necessity for ongoing evaluation and adaptation of legal frameworks to address the evolving landscape of online trade, ensuring that regulatory measures effectively safeguard competition and consumer interests in the digital marketplace.

3. Legal regulation of competition in online trade

Antitrust laws are central to the regulation of competition in online trade. The United States has a well-established legal framework that encourages market competition and restricts monopolistic behaviours. In 1890, the US government passed the Sherman Antitrust Act that made it illegal to run monopolies, trusts, and cartels, with the ultimate objective of increasing competitiveness in the market (Johnson & Green, 2021). The Federal Trade Commission (FTC), with the help of the Department of Justice Antitrust Division, is responsible for the implementation of the Sherman Antitrust Act. In light of the online trade sector, the antitrust regulation prevents monopolies, prohibits anticompetitive behaviours, and safeguards consumer rights.

The US antitrust laws regulate the market by preventing monopolies and anticompetitive practices. Monopoly occurs when a single firm has excessive power to control all the market dynamics, including the demand, supply, and pricing (Kumar & Stauvermann, 2021). Like in physical businesses, the FTC is responsible for monitoring large e-commerce organisations to avoid activities that prevent competition with their smaller and less dominant counterparts (Wörsdörfer, 2022). Some of the most powerful entities in the online market include companies like Google, Amazon, and Facebook. Over the last decade, these mega companies have been accused of engaging in predatory and anticompetitive practices that exploit their market power with little consideration for the interests of the consumers. For instance, in 2023, the FTC and 17 other states sued Amazon for violating antitrust policies (Hebda, 2023). The lawsuit accused Amazon of many things, including controlling its third-party partners' prices, hiding cheaper listings, and charging exorbitant fees to sell on its platform. Although the case is ongoing, «FTC v. Amazon» 2023 is a classic example of how the federal government regulates competition in online trade.

The FTC also controls mergers and acquisitions as part of its strategies to prevent monopolies and anticompetitive practices. Through the Bureau of Competition, the FTC prevents unnecessary mergers and acquisitions that are likely to reduce competition in the market, inadvertently leading to higher prices. The control of mergers and acquisitions occurs in line with the Clayton Act. In 1914, Congress passed the landmark Clayton Act 1914 to regulate anticompetitive practices, such as mergers and acquisitions, that deliberately increased the market size of dominant companies (Agulhon & Mueller, 2023). For instance, Facebook acquired Instagram and WhatsApp in 2012 and 2014, respectively, expanding its market share (Morton & Dinielli, 2022). Although Facebook is not traditionally an online trader, it has features that allow customers to market and sell their products. The FTC unsuccessfully challenged the decision, citing that Facebook has engaged in acquisitions that potentially violated the Clayton Act. In 2020, the DOJ filed a case against Google for potential antitrust practices when the company made a deal with Apple to make Google the default search platform (Adams, 2022). Although this agreement was not a bona fide acquisition or merger, it was a practice aimed at reducing the online search market in a manner that favoured Google against any other competitors.

The Consumer Review Fairness Act of 2016 (CRFA) has played an instrumental role in enhancing fair competition in the American online market. Consumer feedback is central in a capitalist system where different organisations share the market. The CRFA allows customers to share honest opinions regarding services, products, or conduct in any forum, including social media or other review sites (Zhang et al., 2023). Product reviews are essential in empowering the consumer or potential customer to make the right decision. Congress passed the CRFA due to reports that some organisations deliberately prevented individuals from providing honest feedback regarding their products (Zhang et al., 2023). For instance, some firms put in place clauses in their terms and conditions that allowed them to penalise or take legal action against customers who provided negative reviews of products (Zhang et al., 2023). Adversarial reviews are essential in a capitalist system because they allow companies to compete fairly based on merit, competence, and quality. However, some companies take a cautionary attitude toward the feedback due to the possibility of malicious intent. Regardless, CRFA is important, especially for online companies, as it allows customers to review products and services based on merit (Zhang et al., 2023). Therefore, this framework is essential in enabling free competition where demand and supply determine market conditions rather than the size or dominance of the organisation.

Another fundamental legal framework that guides competition in the online markets is the Antitrust Criminal Penalty Enhancement and Reform Act (ACPERA) of 2004. ACPERA is one of the most extensive legal policies that strengthen antitrust behaviour among organisations (Marvão & Spagnolo, 2023). The legal provision serves two fundamental roles, including providing a framework for punishing antitrust violations. Secondly, the law offers organisations incentives, including leniency extensions, if accused companies agree to cooperate with antitrust investigations (Marvão & Spagnolo, 2023). Thus, online firms that engage in antitrust acts are likely to face punitive actions, especially when they fail to cooperate in line with the provisions of ACPERA.

4. Role of marketplaces as trade administrators

As trade administrators, online marketplaces facilitate transactions by creating a virtual space where buyers and sellers can connect virtually. Unlike the traditional brick-and-mortar model, online marketplaces are unique because they allow customers to interact with many buyers and diverse products (Tang et al., 2021). One distinctive element of the online marketplace is that it restores the power to the consumer by giving them the advantage of choice and alternatives. Rather than fixating on one product, customers can access different options, ensuring they purchase the most

effective product or service that aligns with their unique interests (Kleisiari et al., 2021). The convenience further extends to processing the payments. Online marketplaces provide an effective payment method that guarantees security and safety (Williams, 2021). Moreover, customers have diverse ways of payment, from card payments (credit and debit) to digital transactions such as PayPal. Accordingly, besides merely acting as enablers for transactions, online marketplaces provide a high level of convenience that consumers in the brick-and-mortar model cannot achieve.

Online marketplaces serve a critical role as trade administrators by ensuring customer trust and safety. Online marketplaces have a strict way of verifying the credibility of traders to protect them from scams and other fraudulent activities. For instance, Amazon has made concerted efforts to prevent scammers from taking advantage of gullible customers (Crane, 2022). Some of the steps that Amazon has taken include detecting and responding to fraudulent attempts and creating educational initiatives that can assist consumers in differentiating between legitimate and illegitimate businesses (Crane, 2022). Furthermore, Amazon has a team of well-trained professionals, including software developers, machine learning scientists, and investigators, who protect customers from potential scams and proactively deactivate questionable websites from the platform. The reviews and feedback left on the platforms can aid future customers in making effective decisions, leading to the safety of the customers, especially the new ones (Kim & Kim, 2022). The implementation of the Escrow services in the online marketplace has also played a critical role in promoting trust and safety. An Escrow account is a platform whereby commodities are held in trust as parties complete a transaction, in most cases, an online transaction where face-to-face interaction is non-existent (Tan & Saraniemi, 2023). Through such measures, the online marketplaces manage themselves, earning trust and legitimacy among the users.

Furthermore, most marketplaces have ratings and review systems to enhance accountability for the products and services given. Customer feedback is an essential element in determining a competitive edge (Wu et al., 2022). Negative reviews and poor rating scores can have a detrimental impact on the seller on the online trading platform, adversely affecting their reputation and competitive edge. Narciso (2022) argued that the online review system is an essential source of information for customers. From a legal standpoint, online reviews can aid a consumer in gaining sufficient information needed to enter into a contract (Narciso, 2022). The customer feedback acquired from the online platforms is accessible and easy to understand. However, one of the most significant challenges in customer review is the possibility of dishonesty, especially by malicious actors. Moreover, Narciso (2022) noted that information overload can have more negative than positive impacts on the customer. Thus, despite the benefits of the reviews, failure to control them could have adverse implications for the consumer.

The online marketplaces also provide customers with frameworks for conflict resolution. Disputes can result from various causes due to the nature and characteristics of the online trading platform. Aspects like anonymity, trust deficiency, and the inability to interact with the commodity remain a significant threat to the peace and coexistence of the customers and the sellers (Liu & Wan, 2023). The nature of commodities in the online trading sector can also increase the likelihood of conflict. For instance, Liu and Wan (2023) noted that the online second-hand marketplace is prone to many wrangles due to uncertainties regarding the sellers and their products. In this regard, Liu and Wan (2023) proposed an online dispute resolution (ODR) mechanism that utilises internet-related technology. In the US, several online marketplaces have made concerted efforts to ensure that they create platforms for resolving conflicts. For instance, in 2000, eBay established a third-party platform called Square Trade for dispute settlement (Liu & Wan, 2023). A decade later, eBay improved the platform by allowing stakeholders to solve their issues more efficiently and urgently. Some of the most common conflict resolution mechanisms used on these platforms include online arbitration, online meditation, and

online negotiation (Liu & Wan, 2023). Depending on the method chosen, the goal is to guarantee justice to all the parties involved. Thus, dispute resolution restores confidence in the online markets due to the self-sufficiency involved.

5. Conclusions

In conclusion, while the online trade segment presents unique challenges related to anticompetitive practices, government authorities are actively deploying a range of mechanisms and strategies to address these issues and promote a fair and competitive marketplace. Central to these efforts are key legal frameworks such as the Sherman Antitrust Act, the Antitrust Criminal Penalty Enhancement and Reform Act (ACPERA), and the Consumer Review Fairness Act (CRFA). Each of these laws plays a distinct role in curbing anticompetitive behavior and protecting consumers, thereby fostering a more equitable environment for both businesses and consumers.

The Sherman Act remains a cornerstone of antitrust regulation, designed to prevent anticompetitive mergers and acquisitions that could stifle competition and harm consumers. By scrutinizing and, where necessary, blocking such mergers, the Sherman Act aims to maintain a competitive market structure. However, the Act's effectiveness is challenged by the evolving nature of digital markets, where dominant players like Amazon and Google can leverage their scale and market power to influence competition.

To complement the Sherman Act, ACPERA enhances the legal tools available to combat anticompetitive practices by extending criminal liability. This act imposes harsher penalties for firms engaged in anticompetitive behavior, thereby deterring such practices and promoting compliance with antitrust laws. Despite these measures, the sheer scale of dominant players and their complex strategies often find ways to circumvent traditional regulatory approaches, indicating a need for more nuanced and adaptive regulatory mechanisms.

The CRFA addresses another critical aspect of consumer protection by prohibiting companies from using legal action to suppress negative reviews and honest consumer feedback. This law ensures that consumers can freely share their experiences and opinions about products and services, which is vital for maintaining transparency and accountability in the marketplace. The ability to access and act on genuine consumer feedback empowers buyers and contributes to a healthier competitive environment.

Despite these advancements in regulation, significant disparities remain between large and smaller firms in the online trade sector. Larger players, with their vast resources and market influence, can often outmaneuver smaller competitors, highlighting the need for additional policy measures. Congress should consider enacting new policies that enhance the competitive capabilities of smaller firms, ensuring that they can compete on a more level playing field with industry giants. Such policies might include support for innovation, targeted subsidies, or regulatory adjustments designed to reduce the competitive advantages of dominant players.

Moreover, the role of online marketplaces as trade administrators introduces another layer of complexity. These platforms not only facilitate transactions but also play a critical role in maintaining market integrity by controlling transaction processes, enhancing safety and security, and providing mechanisms for conflict resolution. Their ability to manage these aspects effectively helps build consumer trust and ensures a smooth business experience that often surpasses the capabilities of traditional brick-and-mortar markets.

In summary, while existing regulatory frameworks have made strides in addressing anticompetitive practices and protecting consumers, the dynamic nature of online trade necessitates ongoing adaptation and innovation in legal and policy approaches. Strengthening the competitive position of smaller firms and enhancing the regulatory oversight of dominant market players will be crucial for ensuring a fair and competitive

online marketplace. As the digital economy continues to evolve, continued vigilance and reform will be essential to uphold the principles of competition and consumer protection that underpin a thriving capitalist market.

References

Adams IV, R.B. (2022). United States v. Google: Why the Department of Justice should drop its case against the tech giant. *Cumberland Law Review, 52*, 525.

Agulhon, S., & Mueller, T. M. (2023). How the drafting of the Clayton Antitrust Act helped spread the managerial approach to efficiency. *Administration & Society, 55*(3), 591-612.

Crane, J. P. (2022). Trust in the digital marketplace: Amazon, third-party sellers, and information fiduciaries. *Notre Dame Journal on Emerging Technology, 3*, 136.

Hebda, K. (2023). What is the FTC actually claiming in its Amazon lawsuit? *Business Law Today.*

Inoue, Y., & Hashimoto, M. (2022). Changes in consumer dynamics on general e-commerce platforms during the COVID-19 pandemic: An exploratory study of the Japanese market. *Heliyon, 8*(2).

Johnson, C. D., & Green, B.N. (2021). Looking back at the lawsuit that transformed the chiropractic profession, Part 7: Lawsuit and decisions. J*ournal of Chiropractic Education, 35*(S1), 97-116.

Kim, Y. J., & Kim, H. S. (2022). The impact of hotel customer experience on customer satisfaction through online reviews. *Sustainability, 14(*2), 848.

Kleisiari, C., Duquenne, M.N., & Vlontzos, G. (2021). E-Commerce in the Retail Chain Store Market: An Alternative or a Main Trend? *Sustainability, 13*(8), 4392.

Kumar, R.R., & Stauvermann, P.J. (2021). Revisited: Monopoly and long-run capital accumulation in two-sector overlapping generation model. *Journal of Risk and Financial Management, 14*(7), 304.

Liu, Y., & Wan, Y. (2023). Consumer satisfaction with the online dispute resolution on a second-hand goods-trading platform. *Sustainability, 15*(4), 3182.

Marvão, C., & Spagnolo, G. (2023). Leniency inflation, cartel damages, and criminalisation. *Review of Industrial Organization, 63*(2), 155-186.

Morton, F. M. S., & Dinielli, D. C. (2022). Roadmap for an antitrust case against Facebook. *Stanford Journal of Law, Business & Finance, 27,* 268.

Narciso, M. (2022). The unreliability of online review mechanisms. *Journal of Consumer Policy, 45*(3), 349-368.

Strandell, J. (2024). The World's Top Online Marketplaces. Retrieve from: https://besedo.com/blog/the-worlds-top-online-marketplaces-2022/

Tan, T. M., & Saraniemi, S. (2023). Trust in blockchain-enabled exchanges: Future directions in blockchain marketing. *Journal of the Academy of Marketing Science, 51*(4), 914-939.

Tang, H., Rasool, Z., Khan, M. A., Khan, A. I., Khan, F., Ali, H., ... & Abbas, S. A. (2021). Factors affecting e-shopping behaviour: Application of theory of planned behaviour. *Behavioural Neurology, 2021*(1), article number 1664377.

Williams, M. D. (2021). Social commerce and the mobile platform: Payment and security perceptions of potential users. Computers in Human Behavior, 115, article number 105557.

Wörsdörfer, M. (2022). What happened to 'Big Tech ' and antitrust? And how to fix them! *Philosophy of Management, 21*(3), 345-369.

Wu, D. C., Zhong, S., Qiu, R. T., & Wu, J. (2022). Are customer reviews just reviews? Hotel forecasting using sentiment analysis. *Tourism Economics, 28*(3), 795-816.

Yarova, I., & Yurchenko, A. (2023). Marketplaces as a key driver of global E-commerce. *Socio-Economic Relations in the Digital Society, 4*(50), 61-71.

Zhang, Q., Patel, P., & Lowery, C. M. (2023). Protecting low-income consumers in the era of digital grocery shopping: Implications for WIC online ordering. *Nutrients, 15*(2), 390.

DOI: https://doi.org/10.54477/LH.25192353.2024.2.pp.26-35

THEORETICAL AND MODERN APPROACHES TO THE SEARCH FOR A SUSPECT

Ganna Sobko
Department of Criminal Law and Criminology
Odesa State University of Internal Affairs
65000, 1 Uspenska Str., Odesa, Ukraine
e-mail: g-sobko@edu.cn.ua
https://orcid.org/0000-0001-9147-2625

Irina Tesliuk
Department of Postgraduate (Adjunct) and Doctoral Studies
Odesa State University of Internal Affairs
65000, 1 Uspenska Str., Odesa, Ukraine
e-mail: Irinatesliuk@gmail.com
https://orcid.org/0000-0001-8081-2743

Abstract

The article is devoted to changes in the legislation on the search for a suspect which may occur in accordance with the specific needs of society caused by current trends and problems. Such changes may take into account technological progress, international standards, human rights and other factors. Established individual identity of the wanted person is a mandatory condition. It is the established individuality of the wanted object that serves as the main criterion for distinguishing between wanted and search (when the individuality of the object has not yet been established), since it makes it possible to clearly identify the object and narrow the scope of the investigator's search activities. The author proves that investigation is a comprehensive system of detective, investigative and other procedural actions, operational and search activities based on criminal procedure, operational and search legislation and bylaws, which is carried out by the subjects authorized by law and is aimed at locating known objects. The article examines both theoretical and modern means of searching for a suspect, and considers the possibility of introducing a special warrant for collecting electronic evidence. Another important innovation of this institution is the definition of clear deadlines for making a decision on the execution of a European arrest warrant: the decision on execution must be made within 60 days after the arrest of the wanted person, and in rare cases this period may be extended to 90 days. If the detained person consents to the transfer, the relevant decision to execute the European Arrest Warrant must be taken within 10 days after the consent is received. This provision of the Framework Decision has definitely contributed to the improvement of the timing of the execution of the European Arrest Warrant. In addition, the European Union legislation establishes deadlines for the transfer of a wanted person, which should be carried out as soon as possible, determining the date agreed between the relevant authorities. Nevertheless, such a person must be handed over no later than ten days from the date of the final decision to execute the warrant. If the transfer of the person becomes impossible within this period due to force majeure, the judicial authorities shall agree on a new date for the transfer of the person. However, the scientific literature has expressed the opinion that the legal regulation of covert activities in the implementation of the European Investigative Warrant should be considered unsatisfactory. This is due to the fact that the rules governing this activity do not include minimum procedural standards and requirements for its conduct, and the conclusions drawn regarding the development of ways to search for a suspect. At the present stage, with the development of information technology and mass data

collection, the search has become a more systematic and automated process. The use of biometric technologies, the analysis of large amounts of data, and cooperation between countries play a key role in modern search methods.

Keywords: search; suspect; wanted persons; special procedure; international standards.

1. Introduction

The search for suspects in criminal investigations is a complex process that combines theoretical foundations, legal frameworks, and modern technological advancements. As crime evolves in an increasingly interconnected world, law enforcement agencies face new challenges that require innovative approaches to locating and apprehending individuals who evade justice. Traditional methods of suspect searches, rooted in established legal doctrines, now operate alongside cutting-edge tools and strategies that enhance the effectiveness of investigations. The search for a suspect is a critical component of criminal investigations, requiring a blend of theoretical knowledge and practical techniques. Over the years, traditional methods of suspect identification and apprehension have evolved significantly, driven by advances in technology, forensic science, and investigative strategies. This article explores both theoretical foundations and modern approaches to suspect search, examining how classical theories inform contemporary practices. The evolution of these approaches has led to more sophisticated methods, integrating psychological profiling, data analytics, and artificial intelligence to enhance the efficiency and accuracy of suspect identification. Theoretical frameworks such as criminology, behavioral science, and investigative psychology provide the groundwork, while modern tools like facial recognition software, digital forensics, and social media analysis offer powerful means to track and apprehend suspects. Having considered the theoretical approaches to the definition of the concept of "wanted", it is necessary to pay attention to how "wanted" is enshrined in the current legal provisions. An analysis of the criminal procedure law leads to the conclusion that this concept is used in different meanings.

Firstly, search means the activities of the investigator and, on the basis of his/her order, the investigating authority, aimed at identifying suspects and accused persons whose whereabouts are unknown or who have disappeared. This is what, in our opinion, the legislator means when establishing the obligation of the investigator in such cases to take measures to establish their whereabouts or search for them. Secondly, search is used as a synonym for "detection" in the sense of the result of activities in relation to. Thus, the use of the term "search" in either of these meanings is legitimate.

As for the definition of a European arrest warrant, it is a judicial decision issued by a Member State for the purpose of detaining and transferring a wanted person to another Member State. This decision serves to conduct criminal prosecution or to execute a sentence of imprisonment or detention. According to V. V. Zuev, the European Arrest Warrant is a legal basis for the detention of a suspect, accused or convicted person in respect of whom a court decision similar to domestic counterparts has already been adopted and entered into force (Zuiev, 2018).

This article delves into the intersection of traditional and modern techniques, highlighting key strategies and innovations that shape current suspect search methodologies. By understanding these approaches, law enforcement agencies can improve their ability to identify suspects quickly and effectively, ensuring that investigative processes keep pace with the complexities of modern crime. By analyzing the strengths and limitations of current practices, the article aims to provide a comprehensive understanding of the strategies used to locate and apprehend suspects, emphasizing the need for continued adaptation in the face of new challenges in criminal justice.

DOI: https://doi.org/10.54477/LH.25192353.2024.2.pp.26-35

2. Modern approaches to the search for a suspect

The search for suspects in criminal investigations has significantly evolved with the integration of modern technologies and innovative methods. Traditional techniques, such as physical surveillance and witness interviews, remain essential; however, the incorporation of advanced technologies has greatly enhanced the efficiency, accuracy, and speed of identifying and apprehending suspects. This chapter explores the key modern investigative tools and approaches that law enforcement and security agencies employ today.

One of the most powerful tools in modern suspect search is the use of electronic databases. These information technology resources allow for the collection, storage, and rapid analysis of vast amounts of data concerning individuals. Key databases include those that hold passport information, driver's license details, criminal records, fingerprints, photographs, and other biometric data. Access to these databases enables investigators to cross-reference data points quickly, facilitating the identification of suspects through patterns or matching specific identification details. Electronic databases are often interconnected, allowing for the seamless sharing of information across agencies and jurisdictions. For example, law enforcement agencies can compare fingerprints from a crime scene against national and international fingerprint databases, leading to the rapid identification of suspects who may have committed crimes in different locations.

The proliferation of video surveillance cameras in public and private spaces has revolutionized the suspect search process. Cities worldwide are equipped with extensive networks of cameras installed in streets, public transport stations, airports, and other key locations. These cameras continuously capture video footage, documenting the movements and actions of individuals in real-time. Video surveillance systems serve as an invaluable tool in tracking the movements of suspects before, during, and after a crime. By analyzing footage, investigators can piece together a suspect's route, associates, and behavior patterns. Moreover, in cases of high-profile crimes, video evidence often provides crucial leads that direct law enforcement to potential suspects.

Facial recognition technology has become an increasingly prominent tool in modern policing. This technology analyzes facial features captured in video recordings or live camera feeds, comparing them against a database of known individuals. Facial recognition systems are used at critical points such as airports, border crossings, and public events, where rapid identification of suspects is essential for public safety. The technology has proven particularly effective in identifying suspects who attempt to evade capture by altering their appearance or using false identification documents. By matching facial features with high precision, even in challenging conditions, facial recognition systems offer a powerful means of locating and confirming the identity of suspects.

Biometric technologies encompass a range of identification methods that rely on unique physical or behavioral characteristics. Key biometric tools include fingerprint analysis, handwriting recognition, iris scanning, and DNA profiling. These technologies are essential in the search for suspects because they provide highly accurate identification, often linking individuals directly to crime scenes. For instance, DNA traces left at crime scenes can be matched against national DNA databases, aiding in the identification of repeat offenders. Similarly, fingerprint databases allow law enforcement to connect suspects to multiple crime scenes or confirm the identity of detained individuals with criminal histories.

Satellite technology plays a critical role in suspect searches, especially in cases involving cross-border crime or remote areas. Satellites equipped with high-resolution imaging capabilities can monitor vast geographical areas, enabling the tracking of suspect movements. Law enforcement agencies can utilize satellite data to pinpoint a suspect's location, monitor escape routes, and gather real-time intelligence in high-stakes situations such as manhunts. Additionally, satellite technology can assist in

mapping suspect activity by identifying the movement of vehicles or other objects of interest, providing law enforcement with a strategic advantage in planning and executing capture operations.

The use of mobile applications has introduced new avenues for public involvement in the search for suspects. Mobile apps designed for law enforcement and public safety can disseminate information about wanted individuals, including photographs, descriptions, and last known locations. These apps often allow citizens to report sightings or tips directly to authorities, enhancing the scope of search efforts. Moreover, mobile location data and communications can be critical in tracking suspects. With appropriate legal permissions, investigators can access call records, GPS data, and other digital traces left on mobile devices, aiding in the rapid identification and apprehension of suspects.

The digital footprint left by individuals on social media platforms, forums, and other internet resources provides a wealth of information for suspect searches. Investigators often monitor online activity to gather insights into a suspect's whereabouts, connections, and behavior. Social networks are particularly useful for identifying associates, tracking movements, and uncovering evidence of criminal intent. Internet investigations also involve digital forensics, where investigators analyze devices seized from suspects to extract valuable data such as emails, messages, and location history. This digital evidence can be crucial in constructing a comprehensive profile of a suspect's activities and movements.

In addition to technological tools, large-scale interrogation and investigation operations remain a cornerstone of modern suspect searches. These operations involve deploying significant resources to conduct widespread searches, canvassing neighborhoods, interviewing potential witnesses, and engaging the public through media appeals. Such efforts are especially critical in cases where immediate information is needed to prevent further criminal activity or locate a suspect on the run. Public outreach and collaboration play a pivotal role in these operations, as community tips and witness testimonies often provide the missing pieces needed to locate suspects. The combination of traditional investigative techniques with modern technology enhances the effectiveness of these large-scale operations, making them indispensable in the pursuit of justice.

The search for suspects has been fundamentally transformed by the integration of modern technologies and methodologies. Tools such as electronic databases, biometric technologies, and social media investigations have not only streamlined the investigative process but also significantly improved the accuracy and speed of suspect identification. As these technologies continue to evolve, law enforcement agencies are better equipped than ever to tackle complex criminal investigations and ensure the swift apprehension of those who pose a threat to public safety.

3. Harmonization of criminal law in the EU: European warrants and cross-border cooperation

The newest stage also includes the emergence of harmonization processes in the European Union's legislation, which is tracked in the main EU documents, namely the Maastricht and Amsterdam Treaties. According to these treaties, the EU member states undertook to develop cooperation in the criminal law area and provide legal assistance in criminal cases. The subsequent period was marked by the adoption of a number of important regulations in the field of cooperation in criminal matters. One of these acts is the EU Council Framework Decision on the European Arrest Warrant and the Extradition Procedure between Member States, adopted on June 13, 2002 (Council Framework Decision No 2002/584/JHA..., 2002). Criminal law cooperation - the European Arrest Warrant. This warrant provided for a unified procedure for the detention and transfer of a wanted person to another Member State for criminal prosecution or for the execution of a sentence or security measures related to deprivation of liberty.

It is important to note that in 2008, a framework decision was adopted that provided for the introduction of a European Evidence Warrant (Council Framework Decision 2008/978/JHA..., 2008), although this instrument facilitated transnational evidence collection, its practical implementation was accompanied by significant shortcomings, and, as a result, it was canceled in 2016.

Moreover, the possibility of introducing a special warrant for the collection of electronic evidence is being considered. In 2018, a proposal for a Regulation on a European warrant for the production and preservation of electronic evidence in criminal proceedings was presented (Proposal No 52018PC0225..., 2018).

This proposal includes rules that would allow judicial and law enforcement authorities of one EU Member State to send requests directly to a provider in another EU Member State to obtain certain data.

1) The features of European warrants can be defined as follows:

2) Acting on the basis of the principle of mutual recognition of judgments in criminal matters, which has a legal basis in Article 82 of the Treaty on the Functioning of the European Union.

3) Mandatory participation of two entities - the state issuing the warrant and the state executing the warrant, usually referred to as the "requesting party" and the "requested party". Each EU Member State may independently determine the authorities that will be authorized.

4) Variety of entities issuing and executing the warrant. For example, a European investigation warrant may be issued not only by a court or prosecutor, but also by any other authority authorized to conduct pre-trial investigations under the national law of a Member State, such as the police.

5) Specific purpose for issuing the warrant, for example, a European arrest warrant is issued for the detention and surrender by another Member State of a wanted person for criminal prosecution or the execution of a custodial sentence or security measures.

6) A defined and limited list of grounds for refusal to execute a warrant. Each warrant has its own grounds for refusing to recognize and execute it, as well as specific time limits for execution.

7) The existence of a unified form of the European warrant, which is usually provided in an annex to the relevant legal act establishing the legal basis for a particular warrant. For example, the form of the European Investigation Warrant is set out in Annex A to the European Investigation Warrant Directive (Directive No 2014/41/EU..., 2014).

This instrument is based on the Council Framework Decision No. 2002/584/EC on the European Arrest Warrant and Extradition Procedures between Member States (Council Framework Decision No 2002/584/JHA..., 2002). The said decision was amended and supplemented by the Framework Decision No. 2009/299/PVD of February 26, 2009, which concerned the trial of missing persons (Directive No 2014/41/EU.., 2014). One of the key novelties of this decision was the addition of a new ground for refusing to execute the warrant - the absence of a person at the court hearing.

A European warrant is a procedural decision issued by a national court or other competent authority of an EU member state and intended to be executed in the territory of another EU member state to achieve a specific purpose set out in the warrant, such as conducting investigative actions, obtaining evidence or protecting a person. The features of European warrants include:

1. Acting on the basis of the principle of mutual recognition of judgments in criminal matters based on Article 82 of the Treaty on the Functioning of the European Union.
2. Mandatory participation of two subjects - the state that issues the warrant and the state that executes the warrant.
3. Diversification of the subjects of issuing and executing the warrant, including various bodies authorized to conduct pre-trial investigation.

4. The existence of a specific purpose for issuing the warrant, such as detention and transfer of a person for criminal prosecution or execution of a sentence.

5. An exhaustive and limited list of grounds for refusal to execute the warrant.

6. Specified timeframe for execution of the warrant, in particular for the European investigation warrant, no more than 30 days from the date of receipt by the competent authority of the requested state.

7. The existence of a unified form of the European warrant, which is usually represented by an annex to the relevant legal act establishing the legal basis for a particular warrant.

4. Efficiency and challenges of European warrants: Execution deadlines and legal safeguards

Another important innovation of this institution is the definition of clear deadlines for making a decision on the execution of a European arrest warrant: the final decision on execution must be made within 60 days after the arrest of the wanted person, and in rare cases this period may be extended to 90 days. If the detained person consents to the transfer, the relevant decision on the execution of the European arrest warrant must be taken within 10 days after the consent is received.

This provision of the Framework Decision has clearly contributed to the improvement of the timing of the execution of the European Arrest Warrant. In 2018, the average time between the arrest and transfer of a person was 45 days in case there was no consent to the transfer (van Ballegooij, 2020).

In addition, the legislation of the European Union sets deadlines for the transfer of a wanted person, which should be carried out as soon as possible, determining the date agreed between the relevant authorities. Nevertheless, such a person must be handed over no later than ten days from the date of the final decision to execute the warrant. If the transfer of the person becomes impossible within this period due to force majeure, the judicial authorities shall agree on a new date for the transfer of the person.

However, the scientific literature has expressed the opinion that the legal regulation of covert activities in the implementation of the European Investigative Warrant should be considered unsatisfactory. This is due to the fact that the rules governing this activity do not include minimum procedural standards and requirements for its implementation (Kostoris, 2018). We consider it appropriate to support this position.

Based on a systematic interpretation of the provisions of the Directive, we can identify specific features of the European investigation warrant

- clear time limits for execution of the warrant are set - 30 days;
- the possibility of obtaining all types of evidence within the framework of international cooperation between EU countries is enshrined;
- an exhaustive list of grounds for refusing to execute the warrant has been defined;
- standardized the form and procedure for sending the warrant to the requested party;
- can be used both for carrying out procedural actions on the territory of another EU state and for obtaining evidence located on the territory of another EU member state (Klymkevych, 2020).

Based on the analysis of the main provisions of the Directive, the definition of the European Investigation Warrant contained in Article 1 of the Directive appears to be incomplete and does not take into account the main characteristics of this legal institution. Taking into account the systematic interpretation of the provisions of the Directive, the following definition of the concept of a warrant can be offered: a European investigation warrant is a request from the authorities competent to conduct pre-trial investigation and judicial proceedings of one EU Member State to the relevant competent authorities of another EU Member State to conduct investigative (search) actions and certain covert investigative actions aimed at collecting and transferring evidence or

requesting the receipt of evidence located in another Member State. However, despite these advantages of this institution, there are certain problematic aspects of its legal regulation.

One of the important problems is the lack of legal regulation of ensuring the rights of a person during the execution of the warrant (Klymkevych, 2019). Despite the fact that the Directive is based on the principle of respect for human rights, as confirmed by paragraph 19 of the preamble to the Directive, which states that "the creation of a space of freedom, security and justice within the Union is based on mutual trust and the presumption that other Member States will respect Union law, including fundamental rights of the individual", this presumption is not absolute.

In addition to the right to a legal representative, minors have the right to a defense counsel, which is enshrined in Article 6 of the Directive. EU Member States must provide minors with a lawyer without undue delay from the moment they become aware that they are suspected or accused of a criminal offense. The Directive establishes the cases when a defense counsel is mandatory for minors:

- before interrogation by pre-trial investigation authorities, other judicial or law enforcement agencies;
- before carrying out investigative (detective) actions or other actions aimed at collecting evidence by pre-trial investigation authorities;
- immediately after deprivation of liberty;
- when summoned to a court that has jurisdiction to consider criminal proceedings, in advance of their appearance in court.

However, these cases of mandatory involvement of a defense counsel for a minor are not absolute. European law provides for certain exceptions to this rule. The Directive indicates only two such grounds, namely: the existence of an urgent need to prevent adverse consequences that may threaten the life, liberty and physical integrity of a person, and when urgent actions of pre-trial investigation bodies are necessary to prevent a significant threat to criminal proceedings in cases of serious crimes.

However, there has been no legal act that would establish minimum standards for the rights of victims of criminal acts. Therefore, in order to establish a comprehensive approach to solving this problem and to ensure minimum standards of protection of the rights of victims in criminal proceedings, in 2001 the European Parliament and Council adopted the Framework Decision on the Status of Victims in Criminal Proceedings No. 2001/220/PVD (Council Framework Decision No 2001/220/JHA..., 2001).

One of the peculiarities of this institution is that there is no need to apply new security measures to a person; instead, the existing measures applied to a person in the territory of another EU member state are continued. Among the advantages of the legal regulation of the European protection order are the existence of a unified form of the order and clear grounds for refusing to execute the order. However, this institution is not doomed to be without certain disadvantages, among which it is important to note the absence of a time limit for the execution of the protection order.

5. Challenges and legal frameworks in the search for suspects in Ukraine: Procedural gaps and "in absentia" investigations

The practice of law enforcement agencies shows that in most cases, when a person hides from pre-trial investigation authorities and does not live at the place of registration or actual residence, this fact is confirmed by a report of a district or operational officer. In practice, there are no specific reasons for people's decision to hide from the investigation.

It should be noted that the current Criminal Procedure Code of Ukraine does not have a specific mechanism for searching for persons who evade pre-trial investigation and court. The law does not define the list of special measures in the search process. The responsibility for the organization and effectiveness of the search, as emphasized, lies with the investigator.

Instructing investigators to conduct a search for persons hiding from pre-trial investigation bodies to operational units of the National Police of Ukraine is considered the most effective way to proceed. In practice, it is often the operational units that use their capabilities to conduct the search. It is also worth noting that the tax police units of the State Fiscal Service of Ukraine are engaged in the search for persons who violate tax laws.

Operational and investigative measures in the search for persons evading pre-trial investigation are based on the provisions of Article 6 of the Law of Ukraine "On Operational and Investigative Activities". It is noted that the grounds for conducting operational and investigative activities are the availability of sufficient information that needs to be verified through these measures regarding persons hiding from pre-trial investigation authorities, investigators, judges or evading criminal sentences.

The procedural execution of the order to search for persons hiding from the pre-trial investigation authorities is regulated by a separate order of the investigator, which contains the necessary information about the wanted person, the chosen preventive measures, places of possible location and other important details (Klymchuk, 2015).

In accordance with the Criminal Procedure Code of Ukraine, the subjects of search by law enforcement agencies are authorized officials, i.e. persons who are granted the right to detain by a special law. Unlike the CPC of Ukraine of 1960, the modern criminal procedure legislation allows not only inquiry bodies and investigators to conduct search operations. An important innovation is the possibility for citizens to conduct criminal procedural searches (anyone who is not an authorized official) under Article 207 of the CPC of Ukraine. In fact, citizens could search for and detain offenders even before the CPC of Ukraine came into force in 2012, but this process was not regulated by the provisions of the criminal procedure law. Since there may be a situation when the personal data of a wanted person remains unknown for various reasons, it gives the authorized official the opportunity to carry out the detention procedure with mandatory observance of the lawful procedure, which is important in the context of the requirements of the European Convention on Human Rights and national criminal procedure legislation. The introduction and further improvement of non-personal data recording in the criminal procedural detention procedure is necessary and timely, since the absence of personal data of a wanted person should not prevent compliance with the lawful search and detention procedure.

The organization of the search for persons evading pre-trial investigation and prosecution is characterized by various problems, including regulatory, organizational and technical aspects. The adoption of the Criminal Procedure Code of Ukraine in 2012 and changes in many aspects of pre-trial investigation have created a number of problems in practical application. For example, Article 281 of the Criminal Procedure Code of Ukraine stipulates that if the whereabouts of a suspect are unknown during the pre-trial investigation, the investigator or prosecutor must put the suspect on the wanted list. However, the process of putting an accused person on the wanted list is regulated by the provisions of Article 335 of the Criminal Procedure Code of Ukraine, and the legislator does not take into account the motives and reasons for evading the authorities.

In particular, there are shortcomings in the current criminal procedure legislation, as well as problems related to the organization of law enforcement agencies, the level of corruption in the judicial system, and other factors.

The Law of Ukraine No. 1689-VII dated October 7, 2014, which amended the Criminal Code and the Code of Criminal Procedure, introduced the "in absentia" procedure. This procedure applies to crimes within the competence of the Security Service of Ukraine, such as crimes against national security, public safety, peace, human security and international law and order. The "in absentia" procedure is a special procedure for conducting criminal investigations and trials in Ukraine in the absence of the suspect or

accused. This type of criminal proceedings is used in such countries as France, Germany, the Netherlands, Austria, Denmark, Bulgaria, Moldova, Estonia and others.

A special investigation is conducted in cases where the suspect has been evading investigation and trial for more than six months in order to avoid criminal liability or is outside Ukraine in the temporarily occupied territory.

It is important to note that Ukraine already has precedents of conducting special investigations "in absentia", in particular, case No. 225/1957/21. In this context, the Supreme Court determined that the pre-trial investigation authorities additionally took measures to inform the suspect, including the publication of information in the media and the Internet.

Compliance with international standards, in particular Article 6 of the Convention for the Protection of Human Rights and Fundamental Freedoms, and the practice of the European Court of Human Rights in ensuring the participation of a defense counsel in criminal proceedings "in absentia" play an important role.

Summarizing the above, in the context of the conflict, the judicial system of Ukraine develops judicial practice that complies with international conventions, and criminal proceedings "in absentia" are conducted in accordance with high standards to ensure justice and inadmissibility of evasion of punishment.

6. Conclusion

The search for suspects remains a critical component of criminal investigations, influenced by both traditional theoretical foundations and the rapid evolution of modern technologies. While theoretical approaches provide the legal and procedural bedrock, modern tools—such as biometric identification, electronic databases, and satellite tracking—have transformed the landscape of suspect searches, enabling law enforcement agencies to operate with unprecedented efficiency and precision. The analysis shows that hiding perpetrators of criminal offenses is aimed at avoiding responsibility and delaying the possibility of conducting a pre-trial investigation. The problems of organizing the search for such persons are caused by imperfect legislation and insufficient efficiency of law enforcement agencies. Criminalistics recommendations and research in this area are also insufficient.

In the European Union, harmonized legal frameworks, such as the European Arrest Warrant and European Investigation Warrant, have greatly enhanced cross-border cooperation. These instruments establish clear guidelines and timelines that ensure suspects can be swiftly detained and transferred between member states, thereby reflecting a commitment to upholding justice across national boundaries. However, these advancements are not without challenges, as procedural gaps, organizational inefficiencies, and the need for standardized safeguards to protect fundamental rights continue to pose significant obstacles.

In Ukraine, the search for suspects is marked by a complex interplay of legal constraints, practical limitations, and ongoing reforms. The absence of specific mechanisms within the Criminal Procedure Code and reliance on operational units highlight the need for improved legal frameworks and coordinated efforts among law enforcement agencies. Additionally, the implementation of "in absentia" procedures has provided a crucial tool for prosecuting suspects who evade investigation and trial, although these measures must be continually refined to align with international human rights standards.

Based on the above analysis, conclusions can be drawn regarding the development of ways to search for a suspect:

At the present stage, with the development of information technology and mass data collection, the search has become a more systematic and automated process. The use of biometric technologies, the analysis of large amounts of data and cooperation between countries play a key role in modern methods of search.

This development reflects the efforts of society and law enforcement agencies to improve and effectively use methods of searching for suspects in order to ensure law and order and security.

The current state of the art utilizes electronic databases, video surveillance systems, facial recognition systems, biometric technologies, satellite technologies, mobile applications and technologies, social media and internet investigations, and large-scale interrogation and investigation operations.

Referencese

Council Framework Decision No 2001/220/JHA "On the standing of victims in criminal proceedings". (2001). Retrieved from: https://www.eumonitor.eu/9353000/1/j9vvik7m1c3gyxp/vitgbgi8vbys

Council Framework Decision No 2002/584/JHA "On the European arrest warrant and the surrender procedures between Member States – Statements made by certain Member States on the adoption of the Framework Decision". (2002). Retrieved from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32002F0584

Council Framework Decision No 2008/978/JHA "On the European evidence warrant for the purpose of obtaining objects, documents and data for use in proceedings in criminal matters". (2008). https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32008F0978

Directive No 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters. OJ L 130. 1.5.2014. P. 1–36

Klymchuk, M. P. (2015). Execution of orders as a form of interaction between investigative and operative units in criminal proceedings. *Herald of Criminal Justice, 1,* 46–50.

Klymkevych, R. (2020) Yevropeiskyi order na provedennia rozsliduvannia. *Visegrad Journal on Human Rights, 1*(1), 88–92

Klymkevych, R. (2019). European warrant for investigation in the context of criminal justice reform. In: Krasnytsky I. V. (Ed) T*heoretical and applied problems of legal regulation in Ukraine* (363–368). Lviv: LvDUVS.

Kostoris, R.E. (2018). *Handbook of European Criminal Procedure*. London: Springer International Publishing AG, 445 p.

Proposal No 52018PC0225 for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters. (2018). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A225%3AFIN

van Ballegooij, W. (2020). European implementation assessment 2004–2020 on the European arrest warrant. *Eurocrim, 2,* 149–154

Zuiev, V.V. (2018) Simplified issuance procedure: European experience. *Pre-trial investigation: Current problems and ways to solve them, 10(iuvil.)*, 60–64.

DOI: https://doi.org/10.54477/LH.25192353.2024.2.pp.36-45

TEMPORARY PROTECTION IN THE EUROPEAN UNION: A LEGAL ANALYSIS

Tamara Kortukova
Department of International, Civil and Commercial Law
State Trade and Economics University
02156, 19 Kyoto Str., Kyiv, Ukraine
e-mail: t.kortukova@knute.edu.ua
Orcid: https://orcid.org/0000-0002-3376-0159

Yelyzaveta Yemets
Faculty of International Trade and Law
State University of Trade and Economics
02156, 19 Kyoto Str., Kyiv, Ukraine
e-mail: lizayemets2004@gmail.com
Orcid: https://orcid.org/0009-0006-6313-5369

Abstract

Russia's full-scale invasion of Ukraine in 2022 led to a mass migration of people to European Union countries. This, in turn, has highlighted the issue of legal regulation of temporary protection for such individuals. Analyzing this issue is essential for understanding the mechanisms of providing assistance, defining the rights and obligations of beneficiaries of temporary protection, and assessing the effectiveness of European legislation in the context of a large-scale humanitarian crisis. The aim of the article is to conduct a comprehensive study of the legal regulation of temporary protection in the European Union, including an analysis of the relevant norms of European and national legislation of EU member states, as well as the practice of their application in the context of the Ukrainian crisis. To achieve the research goal, methods such as legal analysis, through which a detailed analysis of Directive 2001/55/EC on temporary protection and other relevant regulatory documents was carried out, were used. Using the comparative analysis method, a comparison was made of the national legislation of different EU member states to identify common features and differences in approaches to providing temporary protection. The results of the study can be used for further research into such issues as the long-term consequences of temporary protection for EU migration policy; the integration of beneficiaries of temporary protection into the labor market of EU member states; and the problems of the return of beneficiaries of temporary protection to their countries of origin after the end of the war.

Keywords: mass influx; Directive 2001/55/EC; activation of the Directive 2001/55/EC; rights of beneficiaries of temporary protection.

1. Introduction

Humanity has faced a long history of displacement, forced by wars, natural disasters, and other adverse events. These crises have resulted in massive migration flows, underscoring the urgent need for effective protection mechanisms for displaced persons. The European Union, as a prominent global actor, has been at the forefront of developing and implementing such mechanisms.

The recent conflict in Ukraine has highlighted the pressing need for temporary protection measures within the EU. Russia's unprovoked invasion has led to a mass

exodus of Ukrainians, with over 4.1 million individuals seeking refuge in EU member states as of June 2024 (Temporary protection for persons fleeing Ukraine - monthly statistics - Statistics Explained, 2024). This unprecedented influx has placed a significant strain on the EU's support services (Kuzmenko et al., 2023).

In response to this humanitarian crisis, the EU activated Directive 2001/55/EC on temporary protection, marking a significant departure from its previous reluctance to invoke this mechanism. While the directive had been in place for over two decades, it had remained largely dormant until the Ukrainian crisis. This activation underscores the EU's recognition of the urgent need for a coordinated approach to protect displaced persons during times of crisis.

The decision to activate temporary protection for Ukrainians was influenced by several factors. First, the scale and nature of the Ukrainian crisis, characterized by a sudden and massive influx of refugees, necessitated a swift and effective response. Second, the geographical proximity of Ukraine to EU member states facilitated the rapid movement of refugees and increased the urgency of providing protection. Third, the predominantly female composition of the Ukrainian refugee population, coupled with the presence of a significant Ukrainian diaspora within the EU, created solidarity among European citizens.

Moreover, the EU's visa-free travel regime for Ukrainian citizens and the absence of significant racial or religious differences between Ukrainians and Europeans facilitated the integration of refugees into host communities. These factors combined to create a favorable environment for the activation of temporary protection and the provision of essential services to displaced Ukrainians (Fullerton, 2023).

This article aims to contribute to a deeper understanding of the EU's migration policy and its effectiveness in responding to humanitarian crises. It will delve into the legal regulation of temporary protection within the EU, exploring its historical development, underlying principles, and practical application. By examining the relevant EU directives, national legislation, and case law, we will gain a comprehensive understanding of the rights and obligations of both individuals seeking temporary protection and EU member states.

Furthermore, the article will analyze the challenges and opportunities associated with the implementation of temporary protection regimes. These include issues such as access to services, integration into host communities, and the potential for abuse of the system. By addressing these challenges, policymakers can ensure that temporary protection remains an effective tool for providing humanitarian assistance to those in need. A comprehensive analysis of these aspects will enable policymakers to identify areas for improvement and ensure that temporary protection remains a viable and effective tool for protecting displaced persons in the future.

2. Literature Review

The issue of temporary protection in the European Union has gained significant attention in recent years, particularly due to the ongoing Russian war against Ukraine. Several scholars have explored various aspects of this phenomenon, providing valuable insights into its implications and potential future developments.

For example, M. Ciğer offers a forward-looking perspective by focusing on potential scenarios and solutions for people from Ukraine following the end of the current temporary protection regime in the EU. This analysis is crucial for understanding the potential challenges and opportunities that may arise in the future (Ciğer, 2023).

M. Dei M et al. contribute to the literature by analyzing the peculiarities of the concept of temporary protection in the EU within the context of defense against threats. Their work highlights the intersection between migration and security, providing a broader understanding of the implications of temporary protection policies (Dei et al., 2023).

F. Maryellen offers a multifaceted explanation for the activation of temporary protection in the EU, considering various factors such as geographical proximity, the perception of a temporary armed incursion, the demographic composition of refugees, the existence of a Ukrainian diaspora, visa-free travel, and the absence of racial and religious differences. This analysis provides valuable insights into the complex interplay of factors that influenced the EU's decision to activate temporary protection (Fullerton, 2023).

C. Xhardez and D. Soennecken (2023) take a comparative approach, analyzing the policy responses of the EU and Canada to the Ukrainian crisis. Their study, using a paired comparison strategy, sheds light on the similarities and differences between these two influential regions in their approach to temporary protection during a major crisis. This comparative perspective enriches the understanding of how temporary protection is implemented within different regions.

These studies collectively contribute to a growing body of literature on temporary protection in the EU. They offer diverse perspectives and insights, providing a comprehensive understanding of the phenomenon and its implications. By examining the potential future scenarios, the relationship between temporary protection and hybrid threats, and the factors that influenced the EU's decision to activate temporary protection, these studies offer valuable contributions to the field.

3. Results and Discussion

3.1. The historical basis for temporary protection

Nowadays, temporary protection is a highly relevant issue for discussions related to international migrant protection. For a long time, it has been seen as one of the instruments available to a state facing a massive influx of migrants.

Temporary protection started to form during the Balkan crisis of the 1990s. According to statistics, in the 1970s the number of asylum applications in Western Europe reached 13 000 per year, and 15 years later it exceeded 100 000. In the early 1990s, EU member states received 674,000 asylum applications (Koo, 2016). After the outbreak of the war, UNHCR introduced temporary protection as a response to the humanitarian crisis and encouraged states to implement protection regimes. Consequently, European states began to implement various schemes for the temporary acceptance of displaced persons during the conflict in former Yugoslavia (Genç et al., 2019). Thus, at that time, there were no unified rules or approaches to the provision of temporary protection.

In turn, the European Commission set the aim of a collective response to the conflict. In 1992-1993, a meeting of European ministers was held to discuss the problem of displaced persons and the need to develop approaches to solving it. The result of this meeting was the adoption of Council Resolution No 31995Y1007(01) (1995) on burden-sharing with regard to the admission and residence of displaced persons on a temporary basis and Council Decision of 4 March 1996 on an alert and emergency procedure for burden-sharing with regard to the admission and residence of displaced persons on a temporary basis, that established the range of persons whom EU member states are ready to accept on a temporary basis in the event of an armed conflict or civil war: prisoners-of-war, injured, seriously ill, victims of sexual violence, and those who came directly from the war zones (Article 1(a) of the 1995 Resolution) (Council Resolution No 31995Y1007(01)..., 1995; Malynovska, 2023).

But the documents on temporary protection that were introduced in the EU were not unified, so the policies implemented by the EU states varied.

An agreement that paved the way for harmonization in the field of immigration and asylum was the Treaty of Amsterdam. According to the provisions of Title IIIa on visas, asylum, immigration and other policies related to the free movement of persons, namely Article 73k, the EU Council must adopt "minimum standards for giving temporary protection to displaced persons from third countries who cannot return to their

country of origin and for persons who otherwise need international protection" (Treaty of Amsterdam amending the Treaty on European Union, the Treaties establishing the European Communities and certain related acts, 1995). The main legislative act adopted by the EU on temporary protection is the Temporary Protection Directive (Kortukova et al., 2022). Under Article 1, "the purpose of this Directive is to establish minimum standards for giving temporary protection in the event of a mass influx of displaced persons from third countries who are unable to return to their country of origin and to promote a balance of effort between Member States in receiving and bearing the consequences of receiving such persons" (Council Directive No 2001/55/EC..., 2001).

3.2. Directive 2001/55/EU in the context of the russian invasion of Ukraine

The Temporary Protection Directive, adopted in 2001, was activated for the first time in 2022, in response to russia's unprecedented invasion of Ukraine (Dei et al., 2022). The European Commission quickly proposed the activation of the Temporary Protection Directive on March 2, 2022, following a call by the Home Affairs Ministers. On March 4, 2022, the Council of the EU voted unanimously to adopt Decision 2022/382 granting temporary protection to those fleeing the war in Ukraine (Temporary protection. Migration and Home Affairs, 2001). The Council of the EU referred in particular to the provisions of Article 5 of The Directive on the 'existence of a mass influx of displaced persons': as of March 1, 2022, more than 650,000 displaced persons had arrived in the Union from Ukraine through Poland, Slovakia, Hungary, and Romania (Malynovska, 2023); as of March 9, 2022, more than 2.3 million people had left Ukraine: Poland has received 1,400,000 of all people who fled Ukraine; Hungary - 214,160; Slovakia - 165,199; Moldova - 82,732; Romania - 84,671 (according to UNHCR) (Carrera et al., 2022).

The interesting thing is that, according to paragraph 15 of the preamble to the Decision, the EU Member States agreed not to apply Article 11 of Directive 2001/55/EC. This means that persons enjoying temporary protection can move freely within the EU without the risk of losing their temporary protection (Document No 52022XC0321(03)..., 2022).

Since Council Decision (EU) 2022/382 on the application of the Temporary Protection Directive was introduced for the first time, it can be called a precedent. This raises a logical question: why has this Directive not been used until now, and why did the situation in Ukraine lead to this decision? Since the adoption of The Directive in 2001, Europe has experienced several 'migration crises', the most relevant of which was probably the migration crisis of 2015 and 2016. Nevertheless, EU member states didn't use the legal act in these situations, which led some international lawyers to believe that the law would be a dead letter. According to scholars, one of the main reasons for non-application is the concept of 'mass influx' (Bidonko, 2023). Because the directive doesn't give a numerical value to this concept, there is uncertainty as to what number of persons equals a 'mass influx' for the mechanism of temporary protection to be implemented. Secondly, most EU Member States and the EU itself have preferred alternative instruments to deal with the influx of refugees instead of the Temporary Protection Directive (for example, emergency funding, enhanced assistance from the European Union Agency for Asylum). Another reason is related to the content of the Temporary Protection Directive. Some EU Member States considered The Directive too liberal, as temporary protection grants a wide range of rights, is collective in nature and has a fast mechanism for obtaining it, and access to work is granted instantly. They also feared that the activation of The Directive would create a 'pull factor' for more migrants from crisis regions to come to the EU (The EU's Response to Displacement from Ukraine ECRE's Recommendations..., 2023).

As for the situation in Ukraine, firstly, the EU member states recognized the Ukrainian displacement as a 'mass influx', which is the first step towards granting temporary protection. Secondly, according to Esin Küçük, the activation of The Directive

was considered necessary to prevent accusations of EU inaction. It was well fitted to the circumstances and didn't cause interstate disputes. The solidarity scheme was the main reason why the negotiations on the reform proposal reached a deadlock (Küçük, 2023). In the case of Ukraine, the decision was taken very quickly, in just a few days. Thirdly, the peculiar nature of the russian invasion of Ukraine shocked many Europeans, which contributed to the rapid activation of The Directive. And given that Ukraine is in the process of 'European integration', the EU was interested in helping Ukrainians in this war. Another reason for the activation of The Directive was the so-called 'whiteness' or 'Europeanness' of Ukrainians. According to Bulgarian Prime Minister Petkov, «these are not the refugees we are used to... these people (i.e., Ukrainians) are Europeans»; 'these people are intelligent, they are educated people. ... This is not the refugee wave we have been used to, people we were not sure about their identity, people with unclear pasts, who could have been even terrorists...' (Europe welcomes Ukrainian refugees but others, less so, 2022).

3.3. The challenges of activating Directive 2001/55/EU

In general, the reaction of EU member states to the emergency in Ukraine with the number of people in need of protection changed the traditional concept. The Directive was initiated not only by the required qualified majority, but also by the unanimous support of all Member States. However, the activation of The Temporary Protection Directive led to a number of discussions and criticisms.

The first problem faced after The Directive came into force was the criticism of the EU's double standards. Of course, Council Decision (EU) 2022/382 isn't a mistake. However, scholars and experts don't abandon their thoughts about the reluctance of EU member states to activate the same mechanism in previous crises (Arab Spring 2010 or crisis in Syria 2015) (Garavello, 2022). At one time, even the European Commission itself concluded that it was unlikely to reach an agreement on The Directive's possible activation (Proposal for a regulation of the european parliament and of the council addressing situations of crisis and force majeure in the field of migration and asylum, 2020). The current crisis situation has obviously shattered all preconceptions, demonstrating that "there was simply no political will in the Commission and the Council to activate it" (Ciger, 2023). Therefore, one cannot be sure that the EU would have activated The Directive if the aggressor country against Ukraine had not been russia.

The second problem is discrimination against third world countries. The fact is that by Council Decision (EU) 2022/382, The Temporary Protection Directive was activated in relation to Ukrainian citizens. This creates unequal conditions for asylum seekers from other countries (Bidonko, 2023). When analyzing the legal status of persons under temporary protection and regular asylum seekers, the situation of the former is more beneficial. Although UNHCR welcomes the special status provided for in The Temporary Protection Directive, it also emphasizes the importance of non-discrimination (Rodrigues & Tobler, 2022). Thus, states have a right, rather than an obligation, to extend temporary protection to this category of persons. Only eight out of twenty-seven EU Member States have decided to include the last category in their implementation schemes.

The next set of problems and gaps are primarily related to the practice of EU Member States in applying The Temporary Protection Directive. The European Council on Refugees and Exiles, analysing this aspect, notes the following existing gaps:

1) failure to provide or delayed provision of residence permits, exacerbated by the lack of access to an effective remedy and clear information on the rights of beneficiaries of temporary protection;

2) the lack of clear information on the rights of beneficiaries, available in appropriate languages and in an easily accessible form;

3) the problem of a narrow definition of family: there have been cases of discriminatory treatment of unmarried partners and third-country nationals married to

fleeing Ukrainians who are not covered by The Directive, which is also inconsistent with the Decision;

4) different interpretations of freedom of movement: although the European Commission has publicly confirmed that beneficiaries of temporary protection can move to another EU Member State and apply for temporary protection there, and Council Decision (EU) 2022/382 contains an agreement that Article 11 of Directive 2001/55/EC will not apply, this is not always respected by Member States (The EU's Response to Displacement from Ukraine ECRE's Recommendations, 2023).

With regard to access to socio-economic rights, the following problems arose: 1) limited access to long-term separate housing; 2) lack of simplified procedures for the recognition of qualifications and affordable training; 3) limited access to education; 4) limited access to medical and social assistance (Op-ed: Two years since the triggering of the Temporary Protection Directive: The dilemma of unity over fragmentation for the transitioning phase, 2024).

Temporary Protection Directive was adopted in 2001 and has been implemented into national law in all EU Member States. After Council Decision (EU) 2022/382, most countries introduced temporary protection for displaced persons from Ukraine at the national level. The first countries to introduce temporary protection for displaced persons from Ukraine were Hungary and Slovakia, while other border or neighboring countries (Poland, Latvia and Estonia) provided unrestricted access on the basis of short-term or long-term visa schemes (Rapid response by EU+ countries to address the needs of displaced people from Ukraine, 2022).

According to Article 9 of the Directive, the Member States shall provide persons enjoying temporary protection with a document, in a language likely to be understood by them, in which the provisions relating to temporary protection and which are relevant to them are clearly set out (Council Directive No 2001/55/EC..., 2001). As technology, in particular digital and social communication, has advanced, all EU countries have launched dedicated websites or webpages to provide all necessary information on entry, documents, protection schemes and practical advice. All websites are available in several languages, mainly in English and the official national language of the country, but also in Ukrainian. Further platforms for sharing information were social media and YouTube. For example, Latvia shared video instructions on how to register; Germany, in order to decentralise inbound flows, posted a video message from the German Federal Minister of the Interior on YouTube to explain the support, reception and integration services available; and the Czech Republic introduced virtual assistant technology to answer questions via a voice bot on its Ukrainian refugee helpline (Analysis of Measures to Provide Protection to Displaced Persons from Ukraine: Situational Report, 2022).

Initially, reception centers were created as temporary shelters and resting places for people arriving in host countries. After the implementation of temporary protection, these structures were transformed into service centers where different agencies work under one roof. The services provided range from information, registration, advice on accessing rights, counselling, accommodation referrals, basic care, biometric data documentation and security checks. One-stop service points have been established in, for example, Belgium, the Czech Republic, Estonia, France, Greece, Latvia, Lithuania, Portugal, and Spain (Analysis of Measures to Provide Protection to Displaced Persons from Ukraine: Situational Report, 2022).

Article 10 of the Temporary Protection Directive establishes the obligation of Member States to register the personal data of persons enjoying temporary protection. In particular, the name, nationality, date, and place of birth, marital status, family relationships (Council Directive No 2001/55/EC..., 2001). In the Operational Guidelines, the European Commission pointed out the fact that large-scale IT systems (e.g. Eurodac) and EU databases could not be used to register persons enjoying protection (Document No 52022XC0321(03)..., 2022). Therefore, Member States have to register such persons

in their national registers for foreigners or other national registers in accordance with the General Data Protection Regulation. But there is a problem - working only with national databases limits the possibilities of sharing information exchange, so the Commission, together with the EU Agency for Asylum, decided to provide a platform for information exchange. In practice, registration for temporary protection differs across the EU in terms of the responsible authority, documentation issued and processing time. According to the analysis provided by the European Union Agency for Asylum (EUAA), 1) in 17 EU countries, the authority that carries out the registration also issues the relevant documentation; 2) in 7 countries, several authorities control the registration procedure. As for the documentation, 17 EU countries issue the relevant documents on the day of registration, the rest - from 24 hours to 2 weeks (Analysis of Measures to Provide Protection to Displaced Persons from Ukraine: Situational Report, 2022). Therefore, in order to manage registration flows more efficiently and speed up personal reception procedures, some EU countries have introduced electronic services for online registration, pre-registration or appointment making.

The Temporary Protection Directive provides for relevant rights, such as access to the labour market, education, and training (Article 12), healthcare, social welfare, and means of substance (Article 13), and access to the education system (Article 14). For this reason, free access to the relevant services is ensured by the issued documents (e.g. temporary protection certificate or residence permit). For emergency medical care, access is granted even before registration for temporary protection upon presentation of the relevant document (for example, a passport). With regard to employment, several countries offer personalised consulting services provided by accommodation centers or competent employment authorities, as well as special platforms for job opportunities (Analysis of Measures to Provide Protection to Displaced Persons from Ukraine: Situational Report, 2022).

4. Conclusions

The concept of temporary protection, while relatively recent in international law, has emerged as a vital mechanism for safeguarding the rights of displaced persons during times of crisis. Its development can be traced back to the armed conflicts of the late 20th century, particularly the Yugoslav Wars, which precipitated a significant influx of refugees into neighboring countries and the EU. It served as a catalyst for the EU's adoption of the Temporary Protection Directive in 2001.

Temporary protection is a unique mechanism designed to offer immediate and temporary safeguards to individuals facing mass displacement. Unlike refugee status, which is granted on an individual basis and requires a rigorous assessment of persecution or well-founded fear of persecution, temporary protection is a collective measure that applies to a group of individuals fleeing a specific conflict or crisis. It differs from refugee status in terms of legal framework, applicable subjects, and procedures. This allows for a more expedited process, enabling authorities to provide essential services and support to displaced persons quickly.

The 2022 Russian invasion of Ukraine marked the first activation of the Temporary Protection Directive. This decision was driven by the political will and solidarity of EU member states, coupled with the scale of the displacement, which qualified as a "mass influx".

However, the implementation of the directive has not been without challenges. Issues such as double standards and discrimination against third-country nationals have surfaced. Furthermore, inconsistencies in the implementation of temporary protection across EU member states can lead to confusion and disparities in treatment. This can hinder the effective protection of displaced persons and undermine the EU's collective efforts to address migration challenges. These challenges underscore the need for further refinement of the temporary protection framework.

To address these challenges, it is essential to strengthen the legal framework governing temporary protection, promote consistency in its implementation, and ensure that it is applied in a fair and equitable manner. By doing so, the EU can continue to play a leading role in safeguarding the rights of displaced persons and promoting human rights on a global scale.

Based on the analysis presented in this article, several recommendations can be made to enhance the effectiveness of temporary protection within the European Union and ensure that it remains a viable mechanism for safeguarding the rights of displaced persons:

Firstly, the EU should review and update the Temporary Protection Directive to address the challenges and lessons learned from its implementation during the Ukrainian crisis. This may include clarifying eligibility criteria, expanding access to services, and strengthening enforcement mechanisms.

Secondly, member states should work together to develop common standards and guidelines for the implementation of temporary protection. This will help to ensure that displaced persons are treated fairly and consistently across the EU.

Thirdly, member states should strengthen their cooperation and coordination in managing temporary protection schemes. This includes sharing information, best practices, and resources, as well as working together to address common challenges.

By implementing these recommendations, the EU can enhance the effectiveness of temporary protection and ensure that it remains a valuable tool for safeguarding the rights of displaced persons during times of crisis.

Acknowledgements

The study was carried out as part of the grant Jean Monnet Module «EU MIGRATION POLICY WITHIN HYBRID THREATS» (project number: 101081717, project acronym: EUMPHT, call: ERASMUS-JMO-2022-HEI-TCH-RSCH. Project duration: 2022-2025) supported by the European Education and Culture Executive Agency.

References

Analysis of Measures to Provide Protection to Displaced Persons from Ukraine: Situational Report. (2022). *European Union Agency for Asylum*. Retrieved from https://euaa.europa.eu/publications/analysis-measures-provide-protection-displaced-persons-ukraine-situational-report

Bidonko, H. (2023). *Development of the EU migration policy as a result of russian invasion to Ukraine:* thesis of 24.02.2022. Kyiv: National University of Kyiv-Mohyla Academy.

Carrera S.,Ciger M.I.,Vosyliute L., & Brumat L.(2022). The EU grants temporary protection for people fleeing war in Ukraine. Time to rethink unequal solidarity in EU asylum policy. CEPS Policy Insights No 2022-09. Retrieved from https://cdn.ceps.eu/wp-content/uploads/2022/03/CEPS-PI2022-09_ASILE_EU-grants-temporary-protection-for-people-fleeing-war-in-Ukraine-1.pdf

Ciger, M. I. (2023). Reasons for the activation of the Temporary Protection Directive in 2022: A tale of double standards. In *Carrera S., Ciger M.I., EU Responses to the Large-Scale Refugee Displacement from Ukraine: An Analysis on the Temporary Protection Directive and Its Implications for the Future EU Asylum Policy* (p.59-85). Italy: European University Institute. Retrieved from https://www.academia.edu/98291912/Reasons_for_the_Activation_of_the_Temporary_Protection_Directive_in_2022_A_Tale_of_Double_Standards

Ciğer, M.I. (2023). When Temporary Protection Ends: longer-term solutions for refugees from Ukraine. *Swedish Institute for European Policy Studies*, 1-9. Retrieved from https://www.sieps.se/globalassets/publikationer/2023/2023_11epa.pdf

Council Directive No 2001/55/EC "On minimum standards for giving temporary protection in the event of a mass influx of displaced persons and on measures promoting a

balance of efforts between Member States in receiving such persons and bearing the consequences". (2001). Retrieved from http://data.europa.eu/eli/dir/2001/55/oj

Council Resolution No 31995Y1007(01) "On burden- sharing with regard to the admission and residence of displaced persons on a temporary basis". (1995). Retrieved from https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX:31995Y1007(01)

Dei, M., Hrytsai, I., Davydova, N., Serdiuk, N., & Yurovska, V. (2023). Analysis of the Peculiarities of the Concept of Temporary Protection in the Eu in the Context of Defense against Hybrid Threats. *Pakistan Journal of Criminology,* 15(1), 139–155. Retrieved from https://www.pjcriminology.com/publications/analysis-of-the-peculiarities-of-the-concept-of-temporary-protection-in-the-eu-in-the-context-of-defense-against-hybrid-threats/

Document No 52022XC0321(03) "Communication from the Commission on Operational guidelines for the implementation of Council implementing Decision 2022/382 establishing the existence of a mass influx of displaced persons from Ukraine within the meaning of Article 5 of Directive 2001/55/EC, and having the effect of introducing temporary protection. 2022/C 126 I/01". (2022). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022XC0321(03)&qid=1647940863274#ntr13-CI2022126EN.01000101-E0013

Europe welcomes Ukrainian refugees but others. (2022). NPR. Retrieved from https://www.npr.org/2022/02/28/1083423348/europe-welcomes-ukrainian-refugees-but-others-less-so

Fullerton, M. (2023). Temporary Protection for Ukrainians in the European Union: Why Now and When Again? *Vanderbilt Journal of Transnational Law, Forthcoming, Brooklyn Law School, Legal Studies Paper,* 749, Retrieved from https://ssrn.com/abstract=4571254

Garavello, E (2022). The challenges of EU temporary protection: double standards vs. durable solutions. *The LAU School of Arts and Sciences*. Retrieved from https://soas.lau.edu.lb/news/2022/05/the-challenges-of-eu-temporary-protection-double-standards-vs-du.php

Genç, H. D., & Şirin Öner, N. A. (2019). Why not Activated? The Temporary Protection Directive and the Mystery of Temporary Protection in the European Union. *International Journal of Political Science & Urban Studies, 7*(1), 1–18. https://doi.org/10.14782/ipsus.539105

Koo, J (2016). The European Union Temporary Protection Directive: an example of solidarity in law but not in practice. A Review of Temporary Protection in the European Union 1990-2015. *The Future of Refugee Law: RLI Working Paper Series Special Edition* (16–22), 96-113. Retrieved from https://sas-space.sas.ac.uk/9171/1/WPS%20Special%20Edition%201st%20Annual%20Conference_final.pdf

Kortukova, T., Kolosovskyi, Y., Korolchuk, O. L., Shchokin, R., & Volkov, A. S. (2022). Peculiarities of the Legal Regulation of Temporary Protection in the European Union in the Context of the Aggressive War of the Russian Federation Against Ukraine. *International Journal for the Semiotics of Law - Revue internationale de Sémiotique Juridique, 36*, 667-678. Retrieved from https://doi.org/10.1007/s11196-022-09945-y

Küçük, E. (2023). Temporary Protection directive: testing new frontiers? *European Journal of Migration and Law, 25*(1), 1–30. Retrieved from https://doi.org/10.1163/15718166-12340142

Kuzmenko, O., Ryndiuk, V., Kozhura, L., Chorna, V., & Tytykalo, R. (2023). Legal aspects of temporary protection for Ukrainians in the member states of the European Union. *Juridical Tribune, 13(*2), 224-240. https://doi.org/10.24818/tbj/2023/13/2.04

Malynovska, O. (2023). How temporary is temporary protection: The example of forced migrants from the former Yugoslavia. *Demography and Social Economy, 51*(1), 53–72. https://doi.org/10.15407/dse2023.01.053

Op-ed: Two years since the triggering of the Temporary Protection Directive: The dilemma of unity over fragmentation for the transitioning phase. (2024). European Council on Refugees and Exiles (ECRE). Retrieved from https://ecre.org/op-ed-two-years-since-the-triggering-of-the-temporary-protection-directive-the-dilemma-of-unity-over-fragmentation-for-the-transitioning-phase/

Proposal for a regulation of the european parliament and of the council addressing situations of crisis and force majeure in the field of migration and asylum. (2020). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020PC0613#footnote13

Rapid response by EU+ countries to address the needs of displaced people from Ukraine. (2022). *European Union Agency for Asylum*. Retrieved from https://euaa.europa.eu/publications/rapid-response-eu-countries-address-needs-displaced-people-ukraine

Rodrigues, P., & Tobler, C. (2022). Reception of people from Ukraine: Discrimination in international protection? *Leiden Law Blog*. Retrieved from https://www.leidenlawblog.nl/articles/reception-of-people-from-ukraine-discrimination-in-international-protection

Temporary protection for persons fleeing Ukraine - monthly statistics - Statistics Explained. (2024). Retrieved from https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Temporary_protection_for_persons_fleeing_Ukraine_-_monthly_statistics

Temporary protection. Migration and Home Affairs. (2001). Retrieved from https://home-affairs.ec.europa.eu/policies/migration-and-asylum/common-european-asylum-system/temporary-protection_en

The EU's Response to Displacement from Ukraine ECRE's Recommendations. (2023). European Council on Refugees and Exiles (ECRE). Retrieved from https://ecre.org/wp-content/uploads/2023/10/ECRE-Ukraine-reponse-messages-10.10.2023.pdf

Trauner, F., & Valodskaite, G. (2022). The EU's Temporary Protection Regime for Ukrainians: Understanding the Legal and Political Background and Its Implications. *CESifo Forum, 23*(4), 17-20. Retrieved from https://www.cesifo.org/en/publications/2022/article-journal/eus-temporary-protection-regime-ukrainians-understanding-legal

Treaty of Amsterdam amending the Treaty on European Union, the Treaties establishing the European Communities and certain related acts. (1997). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:11997D/TXT

Xhardez, C., & Soennecken, D. (2023). Temporary Protection in Times of Crisis: The European Union, Canada, and the Invasion of Ukraine. *Politics and Governance, 11*(3), 264-275. https://doi.org/10.17645/pag.v11i3.6817

DOI: https://doi.org/10.54477/LH.25192353.2024.2.pp.46-52

CONCERNING THE CONCEPT OF CRIMINAL OFFENSE AND ITS TYPES

Vitaly Kuts
Department of Criminal, Criminal and Executive Law and Criminology
Penitentiary Academy of Ukraine
14000, 34 Honcha Str., Chernihiv, Ukraine
e-mail: Profkvn55@gmail.com
https://orcid.org/0000-0001-9227-3775

Yana Trynova
Department of Criminal, Criminal and Executive Law and Criminology
Penitentiary Academy of Ukraine
14000, 34 Honcha Str., Chernihiv, Ukraine
e-mail: drtrynova@ukr.net
https://orcid.org/0000-0002-5416-2756

Abstract

The article proves the necessity of rethinking one of the dogmas of criminal law - the concept of a criminal offense. A new look at the essence and meaning of this phenomenon and its types is offered with appropriate arguments. The authors propose to change the angle of view on the concept of a criminal offense, transferring it from the public plane to a private one and to consider such an offense mainly as the cause of a private legal conflict between the person who committed the criminal and illegal act and the victim. Such a proposal is primarily due to the expansion of the arsenal of means of criminal-legal response to the commission of a criminal offense compared to the past, when punishment was considered to be almost the only such means. Therefore, the concept of the criminal offense itself must evolve in the same way. Such an approach will contribute to the restoration of a sense of social justice between the parties to the conflict, the saving of human, material and procedural resources when conducting criminal pre-trial/trial proceedings, and, accordingly, will relieve the judicial system, leaving only those conflicts that could not be resolved by extrajudicial methods. It is proposed to revise the content of the concept of a criminal offense, excluding from it such a feature as «guilt», «guilt» and considering it as an optional feature of this phenomenon. According to certain criteria, criminal offenses have been classified, which has not only theoretical, but also practical significance.

Keywords: criminal law; criminal offense; types of criminal offense; criminal liability; application of criminal liability.

1. Introduction

The concept of a criminal offense, which has recently practically displaced the concept of a crime from the criminal law lexicon, is one of the main categories of criminal law, along with such as criminal liability, punishment, etc. Certain aspects of criminal offense research are highlighted in the publications of P. Andrushko, M. Bazhanov, Y. Baulin, P. Berzin, V. Burdin, R. Veresha, Y. Grodetskyi, O. Kruglov, O. Mykytchyk, V. Navrotskyi, M. Panov, I. Sydoruk and other domestic forensic scientists. It should be noted that most of them were committed during the period of dominance in criminal law of only one type of such offense - a crime. There is no comprehensive monographic study of criminal offenses in Ukraine.

The current understanding of the criminal offense is based on the general

theoretical understanding of the offense as the exclusively guilty non-fulfilment of the duty assigned to the subject, the violation of the right of prohibition defined by the norm, which causes damage to certain values or creates a danger of causing it (Skakun, 2001; Goosebumps, 2016). For such understanding the essence of the offense, firstly, a prominent place in its content is given to the fact of violation of the norms of objective law, not the subjective rights of the victim (hereinafter - the victim)[2] , and as a result, the offense is perceived as a conflict between the offender and the law, and not with the victim or his legal representative, recognized as a victim in accordance with the established procedure; secondly, only an act committed in the presence of guilt is considered a crime.

One of the authors of this article put forward a hypothesis regarding the expediency of rethinking the above-mentioned aspects of the essence of a criminal offense. Regarding the first of them, it was proposed to shift the emphasis from the offender's conflict with the law to his conflict with the victim (Dudorov, 2014). In other words, it was emphasized the expediency of focusing attention on the violation of the subjective right and only then on the objective right. At the same time, it was noted that the state usually «appropriates» a criminal conflict without proper grounds and settles it by punishing one of its participants, which has proven to be an insufficiently effective method of regulating criminal-legal relations, since it does not always satisfy the legitimate interests of the participants in such a conflict, and most importantly, it does not contribute to ensuring social peace in society. Regarding the second of the above-mentioned aspects of the understanding of a criminal offense, doubts have been expressed regarding the recognition of an exclusively culpable act as a criminal offense, while the Criminal Code provides for criminal-legal means of responding to the facts of causing damage even in the absence of guilt (Kuts, 2023).

The above-mentioned circumstances and the need for further research into the phenomenon of criminal offense determined the relevance of the proposed article, the purpose of which is to substantiate the author's position regarding the essence, content and types of criminal offense.

Material and Methods

The material and method section of this study includes a rigorous approach to understanding and redefining the concept of a criminal offense. We applied a series of both general and specialized scientific methods to analyze existing definitions, evaluate their limitations, and propose a redefined perspective on criminal offenses. A descriptive method was utilized to clarify parts of the cited legislative provisions and the views of legal scholars, while analytical methods were applied to evaluate existing definitions and identify gaps. Synthesis allowed us to integrate these insights and create a new model that reflects the current needs of criminal law reform.

Among special legal methods, specific sociological research was used to process and extract necessary information regarding criminal offenses as a legal phenomenon. Content analysis and comparative legal methods were instrumental in distinguishing common features in jurists' definitions and aligning them with the evolving perspectives on criminal law. The formal-legal method was applied to analyze legislative structures, examining key provisions within the current criminal code and exploring their adequacy in addressing contemporary issues. This multi-method approach allowed us to provide a structured yet innovative view on the concept of a criminal offense. We have proposed that this concept be viewed not merely as a conflict with the state or a violation of legal prohibitions but as a private legal conflict between the offender and the victim, with a significant emphasis on restoring justice and providing adequate compensation to the victim.

---

1 We are not supporters of the use of the term «victim» in criminal law, considering it exclusively procedural.

By examining alternative legal responses and focusing on subjective rights rather than purely objective prohibitions, this research redefines criminal offenses in a way that balances public safety with the legitimate interests of individuals involved in criminal conflicts.

Results and Discussion

In the process of finding an answer to the question about the essence and content of a criminal offense, it turns out that it is a rather complex criminal-legal phenomenon that is difficult to define unambiguously. In educational publications devoted to the main aspects of the theory of criminal law, as well as in most special publications on the topic, a socially dangerous, illegal, culpable act, provided for by the criminal code, committed by the subject of a criminal offense is recognized as a criminal offense (Tatsia et al., 2020; Panov, 2019; Vasiliev et al., 2020; Navrotsky, 2013; Veresha, 2024; Grodetskyi, 2022; Kruglov, 2021; Sydoruk, 2022). Its main features are public danger, criminal illegality of an act, guilt, commission of an act by the subject of a criminal offense. In such a situation, the cases of causing even serious damage in the absence of the subject's fault or due to his/her youth, lack of judgment and some other circumstances are not recognized as criminal offenses. The question arises, does this correspond to the natural and legal principles of the functioning of society? Answers to it within traditional, mostly dogmatic ideas about criminal-legal reality and its regulation, which has received the name «criminal-legal regulation» are to be sought in vain. However, sometimes there are slightly different definitions of a criminal offense. O. Mykytchyk (2023) offers a definition that differs from the previous ones and in some respects corresponds to the ideas about the criminal offense of the authors of this article. He claims that a criminal offense can be defined as a type of antisocial illegal behavior that is directed against the interests of society, that is, universal human values, and is expressed in actions that cause significant harm to a person in the system of social relations, for which the criminal law provides punishment. As we can see, this definition does not indicate the sign of guilt and the subject of a criminal offense in its legal sense, reflected in the article 18 of the Criminal Code of Ukraine (2024), that is, he does not consider them mandatory signs of a criminal offense.

We are also convinced that, from the point of view of natural law, it does not matter to the victim whether, with or without fault, significant damage has been caused to their legitimate interests, for example, property has been destroyed or damaged, life has been endangered, bodily harm has been caused, etc. The main thing for them is to receive compensation for the damage caused and to satisfy their sense of justice. By the way, this is what the victim wants, but also the public. Perhaps it is precisely because of the latter cases of innocent harm that they fell into the sphere of criminal law regulation. Compensation for property or other physical damage alone is successfully achieved not by criminal law, but, by the way, civil law. But in order to satisfy the public sense of justice, more powerful socio-legal «levers» are needed, which are criminal-legal means of response. At the same time, it is important to choose and apply them correctly. Domestic anti-criminal legislation provides such means of response, and not only for guilty, but also for innocent violations of the rights of the victims.

The current inclusion of guilt among the mandatory elements of a criminal offense, among other things, is explained by the existing until recently tradition of equating all means of criminal legal response with criminal responsibility in the form of punishment, which can really be applied only to a person who acted in the presence of guilt in the committed act. However, awareness of the fact that criminal responsibility is not the only means of criminal legal response, that the law also provides for other means, allows us to assume that a criminal offense is not only culpably causing significant damage to the legitimate interests of the victim, but also causing such damage in the absence of fault.

Based on the achievements of world and domestic humanitarian thought, Ukrainian criminal law theory takes the first steps in the direction of naturalization of criminal law, that is, bringing its norms into line with the norms of natural law (Kostenko, 2008), global bioethics and modern humanitarian standards (Trynova, 2019). Important aspects of this process are the distribution of criminal offenses, and, accordingly, of offenders, into potential and actual recognition as a criminal offense not only of a crime and a misdemeanor, but also of other cases of causing significant harm provided for by the criminal law, including in the absence of the subject's fault. In addition, it should be noted that the concepts of potential and actual criminal responsibility have long been known to criminal law doctrine and practice (Baulin, 2004). It is quite permissible to talk about potential and real other criminal legal means of response. But all of them are derived from potential and actual criminal offenses

Taking into account the above, we offer the following definition of a criminal offense. This is an act provided for by the Criminal Code of Ukraine, which creates a conflict due to one of its participants causing significant damage to another or creating a danger of such damage, the legal means of solving which is the application of criminal responsibility or other criminal legal means of response.

The given definition is a kind of theoretical model that includes both potential and actual criminal offenses. Everything depends on how to understand the term «application» in it, because it reflects both the process and the corresponding result. In the first case, we have a definition of a potential criminal offense, and in to the second, when certain criminal legal means have already been applied to the offender by a court decision, a real criminal offense arises.

Our proposed definition, firstly, shifts the emphasis from the offender's conflict with the law to his conflict with the victim, thus focusing attention on the interests of the victim, not the state; secondly, it allows cases of causing significant damage in the absence of the subject's fault to be classified as criminal offenses provided for by the Criminal Code; thirdly, it emphasizes that there is not only criminal responsibility, but also other criminal-legal means of response to resolve this conflict; fourth, certifies the presence of potential and actual criminal offenses.

The specified understanding of a criminal offense and its division into potential and real allows to single out the following mandatory signs that make up the content of the first of them: 1) the person's commission of a socially dangerous act; 2) the specified actions causing significant damage or creating a real danger of such damage; 3) the occurrence of a conflict between the subject of a criminal offense or his legal representative and the victim due to this; 4) determination of the criminal offense by the relevant provisions of the Criminal Code; 5) the presence in the law of material and legal means of responding to the commission of an act, which at the same time are means of resolving such a conflict, and itself – of criminal liability or other criminal legal means.

The content of the second type of criminal offense, real, in addition to the above, includes one more mandatory feature - the presence of a conviction or other procedural decision of the court that has acquired legal force on the recognition of the corresponding act as a criminal offense. This feature can be called procedural.

Like any other phenomenon of objective reality, a criminal offense has forms of its existence, which makes it possible to further divide them into appropriate types according to another criterion. Until recently, the problem of dividing criminal offenses into types did not exist, since crime was recognized as their only form. All other harmful acts provided by the criminal law were not considered as criminal offenses mainly because of the existing general theoretical approach to solving this problem.

In fact, in view of the above-defined signs of a criminal offense that correspond to the current criminal legislation, criminal offenses should be considered not only crimes and criminal misdemeanors, as defined in Art. 11 of the Criminal Code, but also the so-

called excesses of minors and those without judgment, as well as harmful actions that do not «deserve» criminal liability, due to which the legislator excludes the possibility of its application (case) or allows to refuse its application (so-called exemption from criminal liability).

The legislative definition of the last method of responding to the commission of a criminal offense as «exemption» from responsibility cannot be recognized as correct, as it does not accurately reflect the essence and content of such a response. To be freed, obviously, is possible only from what has already come. In the situation under consideration, responsibility has not yet accrued, so there is nothing to dismiss yet. The means of criminal legal response, named in the law as exemption from criminal liability, is actually a refusal from its application (Kuts, 2023).

The above also draws attention to the fact that there are doubts about the expediency of classifying an act, to which the state responds by refusing to apply criminal liability, to the number of crimes or criminal misdemeanors. However, the vast majority of criminologists are convinced of the opposite, while forgetting that in such a situation there is no such mandatory sign of a crime or a misdemeanor as the conviction of the subject by a final court verdict. Therefore, when the application of criminal liability is refused, the crime or misdemeanor is transformed into another form of criminal offense, which can claim its independent type, which is not yet distinguished and independently investigated by the criminal law doctrine.

In theory and practice, the essence of an unfinished criminal act provided for by the Special Part of the Criminal Code, in respect of which there was a voluntary refusal to bring it to an end, is not defined equally in theory and practice. Some consider such an act to be an unfinished crime or a misdemeanor, and non-responsibility for its commission is an exemption from criminal liability (Baulin, 2004). Others believe that such an act is not a criminal offense at all, and therefore criminal liability for its commission is excluded (Matyshevskyi, 2001).

We propose a third position, which consists in recognizing such an act as an independent type of criminal offense, different from a crime or a criminal misdemeanor. First, in a real pending criminal offense, there is no such mandatory feature of the crime or misdemeanor as the conviction of the subject by a final judgment of the court. Secondly, the legislative definition of the criminal consequences of such an act (Part 2 of Article 17 of the Criminal Code) suggests that it does not require exemption from responsibility, but something else. Therefore, there are reasons to recognize such an act as a separate type of criminal offense. The form of response to it should be the exclusion of criminal responsibility.

It is debatable whether the facts of causing significant harm or creating a corresponding danger in the state of the so-called incident, as well as minors or incompetents, are considered criminal offenses. In the absence of the slightest doubt that such facts cannot be recognized as a crime or a criminal misdemeanor, it is appropriate to consider them as a separate type of criminal offense, as they have all the necessary features of the latter.

The division of criminal offenses into types, like any other classification of phenomena, can be considered justified only if it is carried out according to some single criterion. So, above, we divided offenses into potential and real ones according to such a criterion as the absence or presence of the fact of committing an illegal act and the criminal-legal reaction to it. In the presence or absence of guilt at the time of their commission, criminal offenses are divided into «guilty» and «innocent», and the first of them, according to the form of guilt, into intentional and careless.

The division of criminal offenses into types according to such a criterion as the form of criminal-legal response to their commission is of theoretical interest and practical importance. According to the specified criterion, all criminal offenses are divided into two types: 1) those that entail criminal liability; 2) those that entail the application of

other criminal legal means. In turn, each of these types can be divided into subtypes (types) depending on either the forms of criminal liability (the first type) or the forms of other criminal legal means (the second type).

The current Criminal Code of Ukraine includes crimes and misdemeanors among first-degree criminal offenses (those that attract criminal liability), and the latter since 2018.

The second type of criminal offenses (those that involve the use of other criminal legal means) mainly represent the following cases: 1) committing acts provided for by the Special Part of the Criminal Code of Ukraine by unconvinced or minors; 2) committing acts provided for by the Special Part of the Criminal Code of Ukraine in the state of a so-called incident; 3) committing the acts provided for by the Special Part of the Criminal Code of Ukraine under circumstances that require or allow the so-called exemption from criminal liaibility, but in fact - the refusal of its application; 4) voluntary cessation of preparations or attempts to commit acts provided for by the Special Part of the Criminal Code of Ukraine.

The proposed classification is primarily cognitive. It simplifies the process of learning about this part of criminal law reality, as it provides a more complete picture of the object of knowledge. Such a classification is not devoid of practical meaning, including criminal law significance. Attribution of the offense to one or another type determines the expediency and possibility/impossibility of applying the appropriate form of criminal legal response to its subject. In this regard, we note that the domestic legislator made a regrettable mistake by establishing criminal liability as a criminal legal means of responding to criminal misdemeanors and also in the form of punishment. Under such circumstances, the meaning of distinguishing a criminal misdemeanor is completely lost. Indeed, if the punishment is a consequence of both the crime and the misdemeanor, why separate them. The separation of a misdemeanor in national law will appear as rational only if the means of response to it is not liability, but other criminal legal means in the form of criminal penalties, which we have repeatedly informed the relevant expert environment (Trynova & Kuts, 2019; Kuts, 2022). Unfortunately, the latter does not respond to our calls, as evidenced, in particular, by the draft of the new Criminal Code of Ukraine (2024), which proposes to maintain criminal liability for committing a criminal misdemeanor.

5. Conclusions

In light of the evolving perspective on criminal offenses, this article emphasizes the necessity of reframing criminal offense concepts, shifting from a state-centric to a victim-centric approach. Traditional views have long prioritized the violation of public order and state norms, treating criminal offenses as conflicts between an offender and the law. However, this perspective often overlooks the individual victim's subjective rights, leading to limited effectiveness in ensuring justice and social harmony. By viewing a criminal offense primarily as a private conflict, it acknowledges the victim's interests and their need for redress, which may extend beyond traditional punitive measures to restorative ones, enhancing the victim's sense of justice.

Furthermore, the traditional reliance on «guilt» as a defining characteristic of a criminal offense is questioned. Modern criminal law increasingly recognizes situations where significant harm may be caused even without direct fault. This shift enables criminal law to address a wider range of harmful actions, expanding the scope of legal responses beyond mere punishment. This perspective aligns with a broader humanitarian approach, integrating principles from natural law and global bioethical standards, which view criminal offenses as diverse in nature—ranging from culpable to non-culpable harms.

The proposed above understanding of the essence and content of a criminal offense as well as its types is a kind of model that includes both potential and actual

criminal offenses, which can be used in the theoretical knowledge of this phenomenon, its legislative consolidation and practical application.

In conclusion, redefining criminal offenses through the lens of conflict between individuals, rather than exclusively between the offender and the state, aligns criminal justice more closely with the needs of society and its victims. This paradigm shift advocates for an adaptive criminal law that balances justice, resource efficiency, and societal harmony by employing a diverse toolkit of legal responses, thereby enriching the criminal justice system and enhancing its capacity to resolve conflicts constructively.

References

Baulin, Y.V. (2004). *Exemption from criminal liability.* Kyiv: Attica, 296 p.

Criminal Code of Ukraine. (2024). Retrieved from: https://zakon.rada.gov.ua/laws/show/en/2341-14#Text

Draft of the new Criminal Code of Ukraine. (2024). Retrieved from: https://newcriminalcode.org.ua/criminal-code

Dudorov O.O., & Havronyuk, M.I. (2014). *Criminal law: Study guide.* Kharkiv: Waite, 944 p.

Goosebumps, E. (2016). *General theory of law.* Kyiv: Waite, 392 p.

Grodetskyi, Yu.V. (2022). Criminal offence. Crime. Criminal misdemeanor. *Bulletin of the Criminal Law Association of Ukraine, 2(*18), 186-206. https://doi.org/10.21564/2311-9640.2022.18.268273

Kostenko, O.M. (2008). *Culture and law - in opposition to evil.* Kyiv: Attica, 352p.

Kruglov, O. (2021). Regarding the concept of a criminal offense. *Bulletin of the Penitentiary Association of Ukraine, 2(*16), 24-32. https://doi.org/10.34015/2523-4552.2021.2.03

Kuts, V.M. (2022). *Problems of criminal liability.* Chernihiv: ADPtS, 180 p.

Kuts, V.M. (2023). *Refusal to apply criminal liability (substantive-legal and procedural aspects).* Kyiv: Norma Prava, 118 p.

Matyshevskyi, P.S. (2001). *Criminal law of Ukraine.* Kyiv: A.S.K, 352 p.

Mykytchyk, O. (2023). The concept of a criminal offense in the system of definitions of antisocial behavior. *Philosophical and Methodological Problems of Law, 1*(25), 78-85.

Navrotsky, V.O. (2013). *Ukrainian criminal law. General part.* Kyiv: Yurinkom Inter, 712p.

Panov, M.I. (2019). *Criminal offense and its types.* Kharkiv: Pravo. Retrieved from: http://nulau.edu.ua/materials/files/criminal_law_2/0003/01.pdf

Skakun, O.F. (2001). *Theory of the state and law.* Kharkiv: Konsum, 656p. Retrieved from: http://politics.ellib.org.ua/pages-1714.html

Sydoruk, I.I. (2022). Regarding the definition of the term «criminal offense». *Scientific Bulletin of the Uzhhorod National University, 2022,* 399-404 https://doi.org/10.24144/2307-3322.2022.70.64

Tatsia, V.Ya., Tyutyugina, V. I., & Borisova, V.I. (2020). *Criminal law of Ukraine: General part.* Kharkiv: Pravo, 584 p.

Trynova, Ya.O. (2019). *Bioethics of criminal law enforcement against crime.* Kharkiv: Pravo, 536 p.

Trynova, Ya.O., & Kuts, V.M. (2019). A new look at the essence of a criminal offense. Criminal offense: national and foreign dimensions. *Materials of the International Scientific and Practical Conference, 2019,* 71-73.

Vasiliev, A. A., Gladkova, E. O., & Zhitny O. O. (2020). *Criminal law of Ukraine.* Kharkiv: Ministry of Internal Affairs of Ukraine, 428 p

Veresha, R.V. (2024). *Criminal law of Ukraine.* Kyiv: Alerta, 604 p.

Babikov, O. (2024). Additional guarantees of observance of the rights and freedoms of specially designated subjects during the conduct of covert investigative (search) actions. *Legal Horizons, 21*(2), 53-68. https://doi.org/10.54477/LH.25192353.2024.2.pp.53-68

ADDITIONAL GUARANTEES OF OBSERVANCE OF THE RIGHTS AND FREEDOMS OF SPECIALLY DESIGNATED SUBJECTS DURING THE CONDUCT OF COVERT INVESTIGATIVE (SEARCH) ACTIONS

Oleksandr Babikov
Department of Criminal Law and Procedure
Kyiv University of Law of the National Academy of Sciences of Ukraine
02000, 7A Academic Dobrohotov Str., Kyiv, Ukraine
e-mail: oleksandr.babikov@edu-knu.com
https://orcid.org/0000-0003-4473-851X

Abstract

The article examines the additional guarantees provided to specially designated subjects—such as lawyers, journalists, medical professionals, and public officials—during covert investigative (search) actions. These subjects hold positions that require heightened protections due to the sensitive nature of their roles and responsibilities. The study analyzes the legal frameworks, both national and international, that aim to safeguard the rights and freedoms of these individuals when subjected to covert surveillance, searches, or other investigative activities. It emphasizes the need for stringent oversight mechanisms, legal safeguards, and procedural transparency to prevent abuse and ensure that any encroachment on rights is justified, proportionate, and lawful. The article also identifies gaps in existing regulations and suggests enhancements to better protect specially designated subjects, thereby balancing the needs of law enforcement with the preservation of fundamental human rights.

Keywords: Covert investigative actions; Specially designated subjects; Human rights; Legal frameworks; Search actions.

Introduction

Conducting covert activities aimed at obtaining information, and primarily related to invasion of privacy, breach of secrecy of communication, correspondence, inviolability of the home, especially when it comes to special entities, including judges, lawyers, people's Deputy of Ukraine, necessitates weighing the effect of their use in criminal proceedings and the possible threat of abuse by law enforcement officers, unjustified restrictions on human and civil rights, unlawful influence on the court, political decisions or obstruction of the right to defense. Several issues remain controversial today, including determining the legal basis for conducting covert investigative (search) actions (CI(S)A), the procedures for their implementation and the use of their results, as well as the requirements for documenting these procedural actions.

Therefore, the purpose of this article is to determine and assess the feasibility of use and threats arising from emergency (S)A in relation to special entities, identify risks of unwarranted interference in private life during their application, development of criteria and general principles of emergency (S)A on special actors for the harmonious combination of the interests of society in the field of justice and the proper provision of fundamental human rights and freedoms.

Along with this, the secrecy of the CI(S)A, which, although a necessary property, makes it possible to avoid proper control by the state and society (Babikov, 2021). And if such emergencies (S)A as audio, video surveillance of a person or place, control of a crime, covert intrusion, surveillance of a person, is usually carried out when the

prosecution has already received sufficient information indicating possible preparation, attempt or commission crime, conducting such an emergency (S)A as the removal of information from transport telecommunications networks (wiretapping) is usually considered by law enforcement officers not as a means of obtaining evidence of guilt, but primarily as a means of monitoring life, obtaining information about connections, routes , establishing permanent meeting places or receiving information about the planned meeting place on-line. Information transmitted through such channels is hardly used as evidence of a person's guilt, but may contain sensitive information and be used as a means of blackmail or other unlawful influence. This state of affairs is known to all participants: investigators, prosecutors, investigating judges. However, cases of refusal to approve this measure by investigating judges are quite rare. This can be explained by the perfection and validity of the petitions, the convincing report of the investigator or prosecutor, however, such justification should be treated critically. To do this, it is sufficient to analyze the sentences contained in the Unified State Register of Judgments (USRJ) in order to refer to the information obtained during the interception of telephone conversations as proof of guilt of the convicted person. Such cases are rare.

This state of affairs is not a revelation for the parties to the criminal proceedings. The inconsistency of the declared expected results during the interference in private communication with the actual data obtained, which from time to time have no significance for criminal proceedings, gives grounds to conclude that the risk of unfounded approval of the request by the investigating judge is much less than the risk of being criticized by law enforcement for «obstructing the fight against crime.» In fact, operational units, investigators, prosecutors and judges «formed a community» of mutual interest, as a result of which the prosecution's arguments about the exclusivity and necessity of the CI(S)A in most cases are not criticized by investigating judges. And given the fact that investigators and prosecutors usually do not meet the requirements of Art. 253 of the CPC of Ukraine regarding the notification of a person about the emergency (S)A, the facts of unjustified restriction of constitutional rights and freedoms remain behind the «seven seals» and without proper response. Elimination of violations of procedural law and compensation for damage caused by unjustified restrictions on rights and freedoms does not occur, which «encourages» law enforcement agencies to further abuses. Unfortunately, this state of affairs is typical not only in Ukraine, but also in other European countries, where the issue of protection of human rights and freedoms is given much more attention.

Thus, in the publication of the Kharkiv Human Rights Group «Telephone tapping in international law and legislation of eleven European countries (UK, Germany, Finland, France, Switzerland, Sweden, Hungary, Poland, Russia, Romania, Ukraine)» Dennis Tellborg (Interception of telephones in the international law and legislation of eleven European countries..., 2014) whether covert surveillance helps in the fight against crime states: "The basic principles of the Swedish Government Act and the Code of Judicial Procedure are the principle that the inviolability of the person is a priority in relation to the detection of crime. Measures that violate (limit) the inviolability of the person may, according to the law, be used to solve crimes only in exceptional cases. The decision to apply such measures is always made by the court and should be directed against persons in respect of whom there are grounds to suspect them of committing a completed crime (or at least preparation, attempt or aiding and abetting). However, we are convinced that this is not enough for the police to investigate organized crime, drug traffickers, etc., and not enough for the Security Police: in all these cases, the police work mainly before the crime, not retrospectively. The purpose of wiretapping (or other intrusion into private life) is to gather information about a person, organization, or event in order to determine how further investigation will be directed. Naturally, wiretapping is one of the many methods of operational and investigative activities. But

even in such cases, wiretapping is used not so much to obtain evidence of a criminal offense as to plan action.

Materials and Methods

The initial stage, stage or step in any study is the development and use of methodological tools in the context of the study, as this depends on the strategy of the basic concept for the study of additional guarantees of rights and freedoms of specially designated entities during covert investigations. (search) actions, and hence the effectiveness of scientific achievements, the formulation of theoretical and applied conclusions and recommendations. Since the problem of methodology in any science, including and in the criminal procedure, is one of the most important, complex and relevant, then in its selection should take into account the specifics of the object and subject of research, discussed above. At the same time, it should be noted that in modern science there is an insufficient level of mastery by researchers of the system of methodological and methodological knowledge, which can lead to errors. In addition, the success of scientific research depends on the availability and degree of development of certain methodological prerequisites, in the absence of which the applied action is useless or even dangerous, generating results that do not meet certain goals and objectives.

Thus, the methodology of scientific knowledge includes a system of various components that allow you to cover and explore the whole set of events and phenomena that are most interested in the science of a particular field. The tools used in this case should cover all available methods for research: dialectical, system-structural and system-functional analysis, historical-legal, comparative-legal, hermeneutic, statistical, sociological, mathematical, modeling, description, comparison, experiment, modeling, observation, etc.

Thus, in the process of scientific research of additional guarantees of observance of the rights and freedoms of specially designated subjects during covert investigative (investigative) actions, we chose the following methods: 1) dialectical (this method is central among philosophical methods of scientific knowledge, because allows to consider the corresponding criminal-procedural phenomenon in development and taking into account the basic laws of dialectics); 2) Comparative law is a method that involves understanding the unknown by comparing it with the known; clarifying the characteristics of a phenomenon by contrasting its qualities with its other properties or those of a different phenomenon; and identifying patterns by comparing objects across different time periods, analyzing changes or trends by examining their past and present qualities. This approach aids in defining the content and essence of legislative and theoretical provisions regarding additional guarantees for the rights and freedoms of specially designated entities during covert investigative actions. 3) dogmatic (alternative names: formal-dogmatic, formal-logical, logical-legal, legal, etc.). This method establishes the content of the studied legal norms and regulations, reveals the laws of law through the rules of legal logic. Thus both external, and internal forms of the legal phenomenon (or its «dogma») are investigated. It is based on the laws of logic and syntax, providing commentary on the provisions of additional guarantees of respect for the rights and freedoms of specially designated entities during covert investigative (search) actions and practices, as well as serving to systematize criminal procedure, timing, disclosure concepts, construction of legal constructions, clarification of the true content of certain norms by their interpretation. With the help of this method, it is also possible to analyze the norm of the criminal procedure law in view of the observance of the rules of legislative technique of constructing articles in the CPC.Thus, as a result, it is possible to identify shortcomings and gaps in the norms of the CPC of Ukraine, which regulate our criminal procedure; 4) The systems method centers on exploring the integrity of an object and the mechanisms that sustain it,

aiming to identify the various relationships within a complex object and integrate them into a cohesive theoretical framework. By employing a systems approach, complex dynamic entities are examined, revealing the internal mechanisms of their individual components, clarifying how these components function, and tracing their interactions across different levels.

The materials studied are international treaties, EU legislation, the case law of the European Court of Human Rights, the Supreme Court, the work of scientists, information on the results of the work of Ukrainian law enforcement agencies and materials of criminal proceedings.

The research utilized both general scientific and specialized methods, including comparative law, to analyze international and national legislation of Ukraine and other countries, as well as scientific categories, definitions, and approaches. The formal dogmatic method was employed to elucidate the content of procedural law requirements and the legal positions of the European Court of Human Rights (ECtHR). Additionally, the dialectical method was used to establish the legal nature and the preconditions for the development of principles related to additional guarantees for specially designated subjects.

Results and Discussion

Unspoken receipt of information as one of the oldest and most effective forms of establishing the circumstances of a criminal offense provides an opportunity, by recording on technical media, to recreate before the participants in the criminal process an authentic picture of events with minimal risk of misperception. On the other hand, covert measures to obtain information restrict the rights and freedoms guaranteed by international acts and national legislation, interfere with his private life, secrecy of communication, violate the inviolability of housing and other rights and freedoms that determine the content and direction of the state.

The tasks of criminal justice (exposing perpetrators of criminal offenses, bringing them to justice) are certainly important for society, but it should be remembered that the establishment and protection of human rights and freedoms is the main duty of the state in Art. 3 of the Constitution of Ukraine (1996). The conflict between the purpose of wiretapping, as defined in the Code of Judicial Procedure (ie prosecuting criminals), and its convenience as a means of preventing crime, has led to police tactics, which do not provide all collected material «for tactical reasons.» It may seem reasonable to keep some information for a month in order for the court to extend its sanction for wiretapping. As a result, each time only a small part of the information gathered is provided to the court, on the basis of which the court extends the sanction.

Here, perhaps, is one of the reasons why courts, intuitively realizing the true purpose of such measures, almost always satisfy requests for measures combined with interference in private communication, even if the result is so little to initiate criminal proceedings and sentencing individuals. in respect of which a tacit hearing was applied by a court decision. This situation is exacerbated by the fact that a judge who refuses to authorize such events risks further devastating criticism if a terrorist carries out an avoidable attack by tapping the phone. On the other hand, by imposing sanctions on hundreds of secret interceptions, the judge does not risk anything. In Sweden, a person subject to such measures will never be aware of it, regardless of whether wiretapping, wiretapping or other measures have been taken legally or illegally.

This view is currently shared by three judges from the so-called Eavesdropping Commission. They write: “In a system without oversight, it is inevitable that decision-makers will eventually adjust to each other’s interests and begin to hold the same views on the appropriateness of measures restricting rights and freedoms. Therefore, there is a growing risk that the decision to apply such measures will be made automatically (SOU 1988: 46, p. 518). I dare say – and this has already become an empirical fact in

Norway (see Lund-report, Rapport till Stortinget 1995-96, n-15) - that this is why requests to listen in on telephone conversations are almost never or never rejected. The same, of course, applies to electronic listening, etc. Naturally, the danger that the court will allow illegal electronic wiretapping is no less than in the case of telephone wiretapping. If we accept the view of the police that these measures are necessary to successfully combat crime - and probably too late to bring the case back - it seems necessary to recognize that these measures are preventive and will remain so in the future. It must also be acknowledged that the court is not and cannot be a guarantee against abuse, as it seems at present, and as everyone wanted to believe. The only way to avoid abuse is transparency of procedures: it is necessary to introduce rules – as introduced by Germany and Austria, as well as many other countries – according to which the person subject to covert measures is informed about their implementation after such actions. This gives him the only opportunity to claim damages if such measures have been taken against him unlawfully. If such cases are tried, the authorities that decide on the use of covert measures will be held accountable. I believe that in this state of affairs, requests for covert measures will be considered more carefully, with a more responsible attitude, taking into account human rights and possible negative consequences in each case. This is probably the only way to be sure that the system meets the requirements of the European Convention on Human Rights. «

Therefore, the organization and conduct of the CI(S)A, especially when it comes to special entities, is extremely important, as they can promote the restoration of violated rights, rule of law, justice, and disrespect guaranteed by the Constitution of Ukraine, international acts and criminal procedural law fundamental rights and freedoms of man and citizen.

The most important international legal act defining the general principles, guarantees of rights and inviolability that apply to the conduct of the CI(S)A is the UN General Assembly Resolution 217 A (III) of December 10, 1948 of the Universal Declaration of Human Rights. This act initiated the protection of human and civil rights and fundamental freedoms at the international level, including protection against unlawful interference with privacy, communication, exchange of correspondence, etc (Universal Declaration of Human Rights, 1948). In particular, Article 12 of the UN Universal Declaration states that no one shall be subjected to undue interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone is guaranteed the right to protection of the law against such interference or encroachment.

Along with the Universal Declaration of Human Rights, the confidentiality of communication is also guaranteed by the European Convention (Convention for the Protection of HRFF (1950)), the International Covenant on Civil and Political Rights (1973), the UN Convention on Migrant Workers (1975). These guarantees are reflected in the national legislation of Ukraine (Criminal Procedure Code of Ukraine, 2022). However, neither at the international nor at the national level is the right to confidentiality, inviolability of communication, prohibition to interfere in private and family life not considered absolute. Article 12 of the UN Universal Declaration prohibits “unjustified” interference. Article 8 of the European Convention allows public authorities to interfere with the right to respect for private and family life, home, and correspondence, provided that such interference is legally justified. It must be necessary in a democratic society for reasons such as national and public security, the economic well-being of the country, the prevention of disorder or crime, the protection of health and morals, or the safeguarding of the rights and freedoms of others.Thus, interference in private communication is permissible under appropriate conditions. Public authorities must have grounds for restricting human rights and freedoms, but it must be carried out on the basis and in the manner prescribed by law and the purpose of such interference may be: the interests of national and public security; economic well-being of the country;

prevention of riots or crimes; protection of the health, morals, rights and freedoms of others. It is important to keep in mind that these international acts focus on the form of legal regulation of issues related to interference in private communication. The procedure for limiting confidentiality is subject to regulation exclusively by law and not by-laws, which increases the level of protection of such rights.

Along with the general principles of guaranteeing rights and fundamental freedoms set out in the UN Universal Declaration and the European Convention, it was the European Court of Human Rights in its decisions that specified such principles, defined the basic conditions and permissible limits of privacy. by the state in private communication and the exercise of other rights. Analyzing the provisions of the UN Universal Declaration and the European Convention, the ECtHR not only explains the main provisions, but also indicates ways to address issues that are not directly regulated by these international acts.

Thus, in the case of Klass and Others v. Germany, it was concluded that despite the absence in the Convention of the term «wiretapping», the content of Art. 8 of the Convention gives grounds to believe that telephone conversations are covered by the concepts of «privacy» and «correspondence». It is also important to interpret such a condition for covert activities as defined in the Convention as «necessary in a democratic society».

The Court has taken the legal view that the right to secret surveillance of citizens is inherent in police states, and in democracies, according to the Convention, such surveillance may be permissible only in cases of extreme necessity for the preservation of democratic institutions. The implementation of this position of the ECtHR was embodied in Art. 246 of the CPC of Ukraine, which stipulates that CI(S) A may be conducted only in exceptional cases where it is otherwise impossible to obtain information about the crime and the person who committed it, as well as in Part 1 of Art. 258 of the CPC of Ukraine, which states that any interference in private communication is possible only with the relevant decision of the investigating judge. The CPC of Ukraine does not provide for exceptions to this rule. The existence of such threats to democratic institutions as terrorism, espionage, and transnational crime necessitates the use of measures such as covert surveillance, correspondence control, and other forms of communication, but the ECtHR emphasizes that in a democratic society the use of any surveillance system must be combined with adequate and effective safeguards to prevent abuse.

In the case of Juvig v. France (European Court of Human Rights: The case of Yuvig v. France, 1990) in 1990, the ECtHR focused on the fact that guarantees of rights and freedoms should be established by law (other acts having the force of law), should contain the following main positions:

1. The composition of the crime, during the investigation of which interference in private communication is allowed;

2. Limits on the duration of interference in private communication;

3. Detailed rules for recording information obtained as a result of interference in private communication;

4. Guarantees that the court will receive records of conversations without corrections and notes;

5. The circumstances under which the received records can and should be destroyed;

6. Rules for the destruction of records or their decryption in cases of acquittal of the accused by the court.

Thus, the ECtHR, as a result of considering a number of cases, including Klass and others v. Germany, Juvig v. France, Malone v. The United Kingdom, Kruslen v. France, formed the main criteria, compliance with which 8 of the Convention.

“On the basis of law” – is that the invasion of privacy occurs on the basis of the

law, which meets the following requirements:

- availability of the law – according to the written or unwritten law, a person has the opportunity to make sure that the interference in his private life meets the requirements of the law applicable in this particular case;
- predictability – a person has the opportunity (including with the help of a lawyer) to predict the consequences of any possible action;
- quality – the law should provide adequate and effective means of possible abuse.

"Qualitative Law" provides:

- a list of crimes, the investigation of which may be grounds for invasion of privacy;
- exclusivity of application, limited to cases where it is otherwise impossible to obtain evidence;
- permission to intervene may be granted on the basis of a motivated written request by a person who has a certain (high, independent) status;
- actual interference in private communication is possible only after obtaining the appropriate permission of the authorized person (preferably a judge);
- the period during which the invasion of privacy may occur;
- regulation of fixing the received information;
- measures to preserve and protect the information received, the introduction of rules for the exchange of such information between different government agencies;
- conditions and grounds for destruction of the received information;
- measures for information, its copies in case of acquittal.

"Necessary in a democratic society" provides:

- only to the extent necessary for the security of democratic institutions;
- in exceptional circumstances necessary in a democratic society in the interests of national security and / or the prevention of riots and the commission of crimes.

In Ukraine, the legal framework for covert measures involving interference in private communication was first established with the adoption of the Law of Ukraine «On Operational and Investigative Activities» (Law No. 2135-XII) in 1992. This framework was further codified in laws governing the formation and activities of law enforcement bodies, including the Laws of Ukraine «On Police,» «On the Security Service of Ukraine,» and the Law «On Organizational and Legal Basis of Combating Organized Crime» (1993). Following the 2012 revision of the Criminal Procedure Code of Ukraine (CPC), the 1992 Law was updated to align with Chapter 21 of the CPC, which regulates decisions on conducting operational and investigative measures, including the submission, consideration, implementation, documentation, and use of results. This update has led to a more unified approach in regulating measures that restrict human and civil rights and freedoms during criminal investigations and operational activities.

Analysis of the basic principles and guarantees of the CI(S)A, regulated in Chapter 21 of the CPC of Ukraine gives grounds to conclude that the introduction of the CI(S) A was a measure aimed at ensuring compliance with the UN Universal Declaration, European Convention, ECtHR and unification. approaches to the organization and conduct of activities related to interference in private communication and restrictions on human and civil rights and freedoms, approximation to generally accepted standards in this area. Along with the general principles governing the grounds and procedure for conducting an emergency (S)A, the CPC of Ukraine establishes certain features regarding the submission of requests for an emergency (S)A for special entities.

In particular, the CPC of Ukraine established the peculiarities of conducting an emergency (S)A in relation to the following special entities:

- judges;
- judges of the Supreme Anti-Corruption Court;
- the lawyer;
- People's Deputy of Ukraine

According to Part 9 of Article 49 of the Law of Ukraine "On the Judiciary and

the Status of Judges" (2016), investigative actions involving a judge, which require court authorization, must be based on a court decision obtained at the request of the Prosecutor General or their deputy, or the head of a regional prosecutor's office or their deputy.

In addition to these safeguards for judges, the Criminal Procedure Code of Ukraine (CPC) outlines specific provisions for conducting covert investigative (search) actions (CI(S)A) involving judges of the High Anti-Corruption Court. Article 480-1 of the CPC mandates that any information suggesting a criminal offense by a judge of the High Anti-Corruption Court must be recorded in the Unified Register of Pre-Trial Investigations by the Prosecutor General (or Acting Prosecutor General). The Prosecutor General must then notify the Supreme Court within 24 hours of entering such information.

Accordingly, a request for permission to conduct an CI(S)A against a judge of the Supreme Anti-Corruption Court may be filed (filed) only in criminal proceedings registered against him by the Prosecutor General or his acting and such a request subject to the requirements of Art. 482-1 of the CPC of Ukraine is subject to consideration by the investigating judge, specified in paragraph 18 of Part 1 of Article. 3 of the CPC of Ukraine.

For covert investigative (search) actions (CI(S)A) involving lawyers, additional safeguards are outlined in Paragraph 3 of Part 1 of Article 23 of the Law of Ukraine "On Advocacy." This provision specifies that such actions, including those involving lawyers whose right to practice is suspended, can only be conducted with court authorization. This authorization is granted based on a judicial decision made at the request of the Prosecutor General, their deputies, or prosecutors from the Autonomous Republic of Crimea, regions, Kyiv, or Sevastopol.

Although the Kyiv City Prosecutor's Office has been reorganized under the Law of Ukraine No. 5076-VI (2013), the terms "regional prosecutor's offices" and "oblast prosecutor's offices" are still used to refer to prosecutor's offices in different regions. Nevertheless, in line with the general principles of criminal proceedings and the protection of lawyers' rights, requests for authorization should be made to the Prosecutor General or their deputy, or to the head of the regional prosecutor's office or their deputy. Along with this has the right to exist and the legal position that before the relevant changes to paragraph 3 of Part 1 of Art. 23 of the Law of Ukraine "On Advocacy and Advocacy" with the replacement of "Regional Prosecutor", "Kyiv City Prosecutor" "their deputies" to "respectively the head of the regional (regional) prosecutor's office or his deputy", granting permission to conduct CI(S)A for the petition filed by the head of the regional prosecutor's office and his deputy is illegal. Controversial in this part is the presence of the authority to submit a request to conduct an emergency (S)A on special entities to the First Deputy Prosecutor General and the First Deputy Head of the Regional Prosecutor's Office.

This distinction arises because Paragraph 9 of Part 1 of Article 3 of the Criminal Procedure Code (CPC) of Ukraine defines the "head of the prosecutor's office" as including the Prosecutor General, the head of the regional prosecutor's office, the head of the district prosecutor's office, and their first deputies and deputies acting within their authority. This indicates that the roles of "Deputy Head of the Prosecutor's Office" and "First Deputy Head of the Prosecutor's Office" are separate and distinct. Similar distinctions are made in Articles 10, 11, 12, and 15 of the Law of Ukraine "On the Prosecutor's Office," which clearly delineate the administrative roles of "Deputy" and "First Deputy" Prosecutor General or Head of the Regional Prosecutor's Office. According to Part 3 of Article 9 of the CPC, which states that "Laws and other normative legal acts of Ukraine related to criminal proceedings must comply with this Code. Any law that contradicts this Code cannot be applied in criminal proceedings," this distinction is crucial for CI(S)A involving judges and lawyers.

Regarding requests for authorization to conduct covert investigative (search) actions (CI(S)A) involving a People's Deputy of Ukraine, Part 2 of Article 482-2 of the Criminal Procedure Code (CPC) stipulates that such requests must be approved by the Prosecutor General (or the Acting Prosecutor General). Additionally, this authorization is required only for criminal proceedings being investigated by NABU investigators or the central office of the State Bureau of Investigation. The analysis of the above wording identifies certain aspects that should be taken into account when exercising the following powers:

- in contrast to the established guarantees for lawyers and judges, the application for permission to conduct an CI(S)A in the NDU can be approved not only by a person who holds a certain position, but also performs duties in such a position;

- the Prosecutor General of Ukraine, the person acting as the Prosecutor General is authorized only to approve the petition.

It should be noted that among the powers of the prosecutor defined in paragraph 10 of Part 2 of Art. 36 of the CPC of Ukraine, the legislator clearly distinguishes between the concept of "agreeing or refusing to approve the requests of the investigator to the investigating judge to conduct an emergency CI(S)A and «independently submit such requests to the investigating judge." These circumstances give grounds to conclude that the Prosecutor General and the person acting in his capacity are not empowered to submit motions to the investigating judge to conduct an emergency CI(S)A, but only to approve such motions prepared and signed by investigators or prosecutors.

However, the question of the need in such cases to include the prosecutor who holds the administrative position of Prosecutor General, his first deputy and deputy, head of the regional (regional) prosecutor's office, his first deputy and deputy in the group of prosecutors in criminal proceedings - remains controversial.

Judicial practice also differs as to whether prosecutors authorized to approve and file motions to conduct CI(S)A on special entities for which the law provides additional guarantees for their activities should be part of the group of prosecutors. On similar issues, which by their legal nature can be correlated with the granting of permission to conduct an CI(S)A as a measure restricting human rights and freedoms, different approaches are used, and, as a result, we have different conclusions about the presence/absence of the prosecutor, holding the relevant administrative position, the right to approve petitions and other procedural actions or decisions. Thus, considering the legality of signing (approving) a notice of suspicion of a judge by the Prosecutor General or his deputy, who were not members of the group of prosecutors and were not procedural leaders, the Grand Chamber of the Supreme Court noted that this power of the Prosecutor General or his deputy is exclusive and may not be delegated to other prosecutors or investigators. In order to exercise this power, neither the Prosecutor General nor his Deputy is obliged to provide procedural guidance in the relevant criminal proceedings against a judge, as the current criminal procedure law does not require such a requirement (Resolution of the Supreme Court No 536/2475/14-k, 2019).

Another legal position is that:

- the burden of proof lies with the investigator, prosecutor, who provides procedural guidance in criminal proceedings;

- High-level prosecutors, including heads of prosecutor's offices, who are not part of the team Theoretical and modern approaches to the search for a suspect specific criminal cases, do not have full access to materials, documents, and other information related to the pre-trial investigation (as per Paragraph 2 of Part 2 of Article 36 of the CPC). They also lack the authority to evaluate the evidence collected during the pre-trial investigation or to substantiate the circumstances outlined in Article 91 of the CPC, which hampers their ability to properly justify a request for an emergency measure.

- in parts 4-6 of Article C of the CPC of Ukraine, which provides for the authority of prosecutors holding administrative positions, the authority to initiate, submit motions

to conduct an emergency (S)A or to approve them are absent;

- holding an administrative position does not give the prosecutor the right to interfere in the procedural activities of another prosecutor, including those who are under his authority, as this would be contrary to the requirements of Part 1 of Art. 36 of the CPC of Ukraine;

- the rules set out in Art. 482-2 of the CPC of Ukraine are special in relation to those set out in paragraph 15 of Part 1 of Art. 3 and item 10 part 2 of Art. 36 of the CPC of Ukraine only in terms of defining specific officials of the prosecutor's office as prosecutors who are procedural leaders in the relevant criminal proceedings, endowed with the authority to carry out the relevant procedural action;

- the adoption of procedural decisions in criminal proceedings by another prosecutor is not a procedural manager is possible only in cases expressly provided for in Part. 4-6 st. 36, part 3 of Art. 37, art. 313 of the CPC of Ukraine, is exclusive and is not subject to expanded interpretation.

In view of the above, the position is expressed that during the pre-trial investigation to perform procedural actions and make decisions in criminal proceedings are vested only prosecutors – procedural managers (except directly provided in Part 4-6 of Article 36 powers of heads of prosecutor's offices and complaints in the cases provided for in Articles 308 and 311 of the CPC of Ukraine), as the procedural management of the pre-trial investigation is primary and decisive in relation to departmental supervision. A prosecutor who does not exercise procedural guidance cannot be held procedurally responsible for the consequences of actions taken and decisions made, so the decision (approval of the petition) by the Prosecutor General (acting Prosecutor General), his deputy, the head of the regional prosecutor's office is not their determining right. but only by derivative powers of primary law arising from procedural guidance.

Restrictions imposed by criminal procedural law on the possibility of conducting emergency situations in relation to certain special entities, due to their special status and guarantees of independence, require an increase in the status of the prosecutor, who may perform such actions against special entities, and, accordingly, , the head of the prosecutor's office, whose powers include the approval (submission) of a petition for an emergency (S)A, must be a member of the group of prosecutors – procedural heads. Summing up the issue related to the application for an emergency (S)A for a special entity, property and premises owned, owned or used, it should be noted the need to comply with the requirements for signing such an application by an authorized person, providing information in the application and / or confirming the relevant document of the fact that such a person holds a relevant administrative position or performing duties. At the same time, special attention should be paid to the requirements of the Law of Ukraine "On Temporary Acting of Officials Appointed with the Consent of the Verkhovna Rada of Ukraine, the President of Ukraine or the Verkhovna Rada of Ukraine on the Nomination of the President of Ukraine". appointed by the President of Ukraine with the consent of the Verkhovna Rada, his duties are temporarily, but not more than one month, performed by the first deputy (and in his absence - the deputy) of this person, appointed by a constitutionally legitimate person.

The status of such entities as the "Acting Prosecutor General" and the "Acting Prosecutor General", the grounds for its acquisition, the content and scope of powers are different. "Acting Attorney General" – the First Deputy, Deputy, to whom the Attorney General by his order entrusts the performance of the duties of the Attorney General for the period of business trip, vacation, etc. The specified subject of procedural activity is provided in the CPC of Ukraine. "Acting Prosecutor General" is a person who temporarily performs duties on the basis of an order of the person who appointed the Prosecutor General – the President of Ukraine. The reason for such a decision is the absence of the Prosecutor General (resignation, disappearance, etc.). The current CPC does not provide for such a subject of procedural activity. As the CPC does not provide

for the possibility of delegating procedural powers of the Prosecutor General to a person temporarily acting, the person with the status of "acting Prosecutor General" is not empowered to approve requests for an CI(S)A or perform other procedural actions, relating to the powers of the Attorney General or the person acting in his capacity. In addition, when deciding on the conduct of an emergency (S)A in relation to a lawyer (defense counsel) should be taken into account established by part 5 of Art. 258 of the CPC of Ukraine prohibits the conduct of emergency situations (S)A, related to interference in the communication of defense counsel with the suspect, accused, convicted, acquitted. In our opinion, the wording of the ban on interfering in private communication between the defense counsel and his client is unsuccessful and does not meet modern trends and standards established by international legal acts, which negatively affects the proper preservation of legal secrecy. confession.

Analyzing these provisions of the criminal procedure law, we can draw the following conclusions:

1. it is not prohibited to interfere in a lawyer's private communication with another client: a witness, a victim, a person whose property is being seized, a representative of a legal entity subject to criminal proceedings, a person whose property is being seized, an insane person, who committed a socially dangerous act, etc.

2. it is not prohibited to interfere in the private communication of one defense counsel with another defense counsel or a representative of a person, including a representative of a juvenile suspect, accused, convicted, acquitted.

When analyzing the guarantees of legal secrecy to determine the boundaries of lawful interference, it is essential to consider both national and international legal instruments, as well as relevant case law. For instance, Article 23 of the Law of Ukraine "On Advocacy" prohibits requiring a lawyer, their assistant, trainee, or anyone employed by a lawyer, law firm, or bar association, as well as individuals whose right to practice law has been suspended, to disclose information that constitutes a lawyer's secret. Such individuals cannot be questioned about these matters unless the person who entrusted the information has legally released them from the obligation of confidentiality. Similarly, Article 65 of the Criminal Procedure Code (CPC) of Ukraine stipulates that priests cannot be interrogated about information received during confession, and lawyers cannot be questioned about information that is legally protected. Additionally, Article 8.224 of the CPC provides that individuals have the right not to answer questions regarding the secrecy of confession and professional confidentiality of defense attorneys.

However, these provisions do not fully address the issue of interfering with legal secrecy during covert investigative (search) actions (CI(S)A). Paragraph 3 of Part 1 of Article 23 of the Law of Ukraine "On Advocacy" offers an additional safeguard by requiring that investigative measures or actions involving a lawyer can only be conducted with court authorization, based on a decision from the court or a prosecutor from the Autonomous Republic of Crimea, regions, Kyiv, or Sevastopol. Additionally, Paragraph 8 of this article prohibits involving a lawyer in confidential cooperation during such measures if it involves legal secrecy. Given the lack of clear definitions in national legislation regarding the boundaries of lawful interference with legal secrecy, the legal positions of the European Court of Human Rights (ECtHR) on this matter are crucial.

The key principles regarding the interpretation and application of Article 8 of the European Convention on Human Rights, particularly concerning interference with private communication during covert investigative (search) actions (CI(S) A), are outlined in the European Court of Human Rights judgment in the case of Misho v. France, delivered on December 6, 2012 (§§ 118-119): "While Article 8 protects correspondence between individuals, it also provides enhanced protection for the exchange of information between lawyers and their clients. This is due to the

fundamental role of lawyers in a democratic society – the role of protecting the parties to litigation. Lawyers will not be able to perform this important task if they cannot guarantee to those they protect that the exchange of information between them will remain confidential. In order to carry out this mission successfully, it is important that there is trust between the lawyer and his client, and that is why secrecy is necessary. The right to a fair trial, including the right of the accused not to testify against himself, is not directly related to this, but depends on compliance with this condition". In view of the additional protection afforded by Article 8 to maintain the confidentiality of the lawyer-client relationship and the grounds on which that confidentiality is based, the ECtHR considers that lawyers' professional secrecy, by imposing certain obligations on them, has special protection under this Article." (Judgment of the European Court of Human Right No 12323/11..., 2012).

Please note that the ECtHR does not differentiate between clients of lawyers and suspects, accused, convicted or other persons. There is no distinction between types of proceedings or forms of legal aid provided by lawyers. The main thing to focus on is the confidentiality of the lawyer-client relationship.

In other cases, the ECtHR found a violation of Art. 8 of the Convention:

- study of bank statements on the accounts of a lawyer during the investigation of tax fraud (Judgment of the European Court of Human Rights No 69436/10..., 2015);

- interception by a police officer of papers that a lawyer passed on to his clients, who were accompanied by police in the court lobby (Judgment of the European Court of Human Rights no. 28798/13..., 2018);

- wiretapping of the applicant's law firm by order of the Federal Prosecutor in connection with the investigation of a criminal case in which the applicant (lawyer) was a third party process, and issues related to activities other than the activities of a lawyer) (Judgment of the European Court of Human Rights No 23224/94..., 1998);

- The interception of a lawyer's telephone conversations, the inability of the lawyer to contest the legality of this measure, and the destruction of the records were noted by the court. The court emphasized that such wiretapping between a lawyer and their client constitutes a clear violation of professional secrecy, which is fundamental to the trust between them. (Judgment of the European Court of Human Right No 30181/05..., 2015).

In addition, for the objective perception of the criteria for distinguishing between lawful and excessive and unjustified interference with legal secrecy, we consider it necessary to cite a number of cases in which the ECtHR did not recognize a violation of Article 8 of the Convention and interference with legal secrecy.

For example, in Versini-Kampinci and Krasnyanski v. France, the Court found that the applicants' lawyer and his colleague had represented the interests of the director of a company suspected of violating an embargo on beef imports from the United Kingdom during the cow rabies crisis. Records of telephone conversations between the client and the lawyer, which contained information protected by legal secrecy, were used as evidence in the disciplinary proceedings against the lawyers. The Court considers that the violation of Article 8 of the Convention did not occur because the recording of the conversations between the lawyer and the client was made because the lawyer was suspected of having committed an offense and aimed at preventing mass riots.

In the case of Klass and Others v. Germany, five German lawyers complained about German law, which allows the authorities to monitor their correspondence and telephone conversations without the authorities having to inform them of the measures taken against them.

While not finding a violation of Article 8 of the Convention, the Court clarified that such interference with the right guaranteed by Article 8 § 1 was deemed necessary in a democratic society for national security and to prevent riots or crimes.

The Court observed that covert surveillance is permissible under the Convention only if it is essential for maintaining democratic institutions. It also acknowledged that modern democratic societies face advanced threats from espionage and terrorism, necessitating effective countermeasures, including secret monitoring of subversive activities. According to the Court, legislation that authorizes covert surveillance of emails, mail, and telecommunications is acceptable only when it is necessary to safeguard national interests and security, or to prevent unrest and criminal activities (Newsletter – Professional Secret Lawyer, 2021).

The ECtHR demonstrated a similar position in its judgment of 5 July 2001 in the case of Selahattin Erdem (Duran Kalkan). Assessing the legality of monitoring his correspondence with a lawyer while in custody, the ECtHR concluded that finding the accused's correspondence with a lawyer under the control of public authorities in this case did not violate Art. 8 of the Convention, because interference in correspondence between a lawyer and an applicant has a legal basis in national law (Pogoretsky & Pogoretsky, 2016).

In this case, the ECtHR actually preferred national law to international law, public danger (terrorism) to legal secrecy.

These legal positions of the ECtHR indicate that the presence of a person in the status of a lawyer can not be perceived as an unconditional circumstance that makes it impossible to interfere in his private communication, especially when it comes to committing a criminal offense by a lawyer. However, such interference must be justified, not violate the guaranteed secrecy of the lawyer's communication with the client and be proportionate to the threats that cause such interference, to exclude excessive interference with a person's private life.

However, in practice it is almost impossible to separate the lawyer's professional activity from his private life. Considering the issue of legal secrecy in this context, the ECtHR noted: Respect for privacy should also include, to some extent, the right to establish and develop relationships with others. Moreover, there seems to be no fundamental reason for such an understanding of "private life" to exclude professional and business activities, it is in their work that most people have a significant, if not the greatest, chance to develop relationships with the outside world. This view is confirmed by the fact that it is not always possible to clearly distinguish which activities of a person are part of his professional and business life. If a person has a humanitarian profession, his work in this context can become an integral part of his life to the point that it becomes impossible to separate who he is acting at this time." (Titova, 2011).

At the same time, when such a distinction can be made, the ECtHR points to the duty of a lawyer to report his suspicions of possible criminal acts of their clients, such as the legalization of criminally obtained property. However, in the Court's view, such a duty should apply to activities which, although practiced by a lawyer, are similar to other professions which are not protected by legal secrecy and are remote from the mission of protection. In particular, if the lawyer participates on behalf of and on behalf of the client in finance or real estate transactions, acts as a principal or assists the client in preparing or conducting transactions for certain financial transactions, which may include: buying and selling real estate or commercial enterprises; management of capital, shares or other assets owned by the client; opening bank, savings or investment accounts; organization of payment of contributions for the creation or management of legal entities; creation, management or administration of trust companies or similar entities - interference in such activities can be considered legitimate (Titova, 2011). Interference with the rights of a lawyer is also considered lawful if there is a suspicion that the lawyer himself has committed or is committing a crime.

Conclusions

Summing up, it is possible to determine the main criteria and limits of lawful

interference with legal secrecy during the CI(S)A:

1. the procedure for such interference and guarantees for the protection of individual rights must be provided for by national law;

2. Confidential exchange of information between a lawyer and his client is unconditionally protected only if the lawyer acts as a defense attorney and his client is a suspect, accused, convicted or acquitted, otherwise in order to assess the legality of such interference, the circumstances of his commission, the public danger, the role of the lawyer in his commission or concealment of its consequences, the guarantees of such intervention provided by national law;

3. Guarantees of protection of lawyer's secrecy apply not only to the conduct of emergency CI(S)A related to interference in private communication, but also others, during which access to information constituting a lawyer's secret may be obtained, in particular secret intrusion into the office lawyer, audio, video control of the place, secret sampling for expert research, etc .;

4. Violation of the inviolability of the lawyer's home, office (place of work), holding of an emergency meeting CI(S)A, including in public places, measures to involve a lawyer in covert cooperation, should be considered not only a violation of legal secrecy, but also a violation of the right to the reputation of a lawyer, which can negatively affect a wide range of his rights and opportunities;

5. Interference with legal secrecy must be carried out in accordance with the law, which provides for compliance with procedural issues: filing a petition by the relevant authorized person, timely involvement of a representative of the bar self-government body in the investigation, exclusion of third parties access to lawyers' files legal secrecy and access of authorized persons to materials directly related to the subject of pre-trial investigation in criminal proceedings and denial of access to other materials (dossier) of a lawyer, possibility to destroy or return materials containing legal secrecy and not related to the subject of investigation unjustified in terms of proportionality.

6. impossibility to differentiate the lawyer's communication with clients (primarily in telephone conversations); 8 of the Convention;

7. The commission by a lawyer of a crime, preparation or attempt to commit it, in the presence of other obligatory and sufficient conditions, may be considered as a legal ground for interfering in his private communication with other persons.

The current regulation of covert investigative (search) actions against specific entities—such as judges, judges of the Supreme Anti-Corruption Court, lawyers, and People's Deputies of Ukraine—within Ukrainian criminal procedure legislation is ambiguous and inconsistent. Several unresolved issues concerning the organization and execution of these proceedings compromise the protection of human and civil rights and freedoms and hinder the effective pursuit of criminal justice objectives.

In view of the above, the issue of granting permission to hold an emergency CI(S)A on judges, lawyers and deputies is subject to additional regulation in terms of determining the basic principles:

1. Exhaustive and unambiguous list of persons entitled to initiate (enter information into the unified register of pre-trial investigations) criminal proceedings against persons endowed with special status.

2. Specification of the requirements for registration of a criminal offense against special entities with the reflection of information about a particular person, whose position he holds (his status), the content of illegal actions on the application (notification) of the crime.

3. Expanding and specifying the range of persons whose interference in the communication of a lawyer with whom is prohibited.

4. Specification of the procedure and conditions for conducting other emergency situations, including inspections of publicly inaccessible places, during which documents containing legal secrecy and in fact related to interference in private

communication may be inspected.

5. Differentiation of the procedure and conditions of the CI(S)A in relation to a judge, lawyer, People's Deputy, depending on whether their illegal activities are related to the performance of duties of a judge, lawyer, deputy.

6. Establishment of a ban on tacit withdrawal of information in the deliberation room of a judge (court).

7. To specify the status of the prosecutor authorized to apply to the court with a request for permission to hold an emergency CI(S)A for persons with special status. This issue can be resolved by introducing the requirement to include such a prosecutor who holds an administrative position in the group of prosecutors – procedural managers in a particular criminal proceeding, assigning him the functions of the head of such a group.

References

Constitution of Ukraine. (1996). https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text

Babikov O.P. (2021). Expediency and threats of the use of covert measures to obtain information»: materials of the international scientific-practical conference. *Current issues of legal science and practice in the 21st century, September 23-24*, 2021.

Interception of telephones in the international law and legislation of eleven European countries (Great Britain, Germany, Finland, France, Switzerland, Sweden, Hungary, Poland, the Russian Federation, Romania Ukraine). (2014). https://khpg.org/1084719187

Universal Declaration of Human Rights. (1948). https://zakon.rada.gov.ua/laws/show/995_015#Text

Convention for the Protection of Human Rights and Fundamental Freedoms. (1950). https://zakon.rada.gov.ua/laws/show/995_004#Text

International Covenant on Civil and Political Rights. (1973). https://zakon.rada.gov.ua/laws/show/995_043#Text

Convention on Migrant Workers. (1975). https://zakon.rada.gov.ua/laws/show/993_159#Text

Criminal Procedure Code of Ukraine. (2022). https://zakon.rada.gov.ua/laws/main/4651-17#Text

European Court of Human Rights: The case of Yuvig v. France. (1990). Kharkiv Human Rights Group. Access mode: http://privacy.khpg.org/1604922590

Law of Ukraine No 2135-XII «On operational and investigative activities». (1992). https://zakon.rada.gov.ua/laws/show/2135-12#Text

Law of Ukraine No 3341-XII "On Organizational and Legal Basis of Combating Organized Crime". (1993). https://zakon.rada.gov.ua/laws/show/3341-12#Text

Law of Ukraine No 1402-VIII "On the Judiciary and the Status of Judges". (2016). https://zakon.rada.gov.ua/laws/show/1402-19#Text

Law of Ukraine No 5076-VI "On Advocacy". (2013). https://zakon.rada.gov.ua/laws/show/5076-17#Text

Resolution of the Supreme Court No 536/2475/14-k (2019). https://zib.com.ua/ua/141611-vp_vs_viznala_scho_genprokuror_ne_buv_zobovyazaniy_vruchati_.html

Judgment of the European Court of Human Right No 12323/11 "Misho v. France". (2012). https://hudoc.echr.coe.int/eng#%7B%22itemid%22:%5B%22001-115377%22%5D%7D

Judgment of the European Court of Human Rights No 69436/10 (Section IV) "Brito Ferrinho Bexiga Villa-Nova v. Portugal". (2015). Retrieved from: https://base.garant.ru/71414612/

Judgment of the European Court of Human Rights no. 28798/13 "Ordre des avocats de Brest and Laurent v. France" (2018). Retrieved from: http://aoskif.com.ua/ua/blog/perehoplennya-povidomlen-advokata-telefonnih-dzvinkiv-ta-tayemne-sposterezhennya-praktika-yespl

Judgment of the European Court of Human Rights No 23224/94 "Kopp v. Switzerland".

(1998). Retrieved from: https://europeancourt.ru/resheniya-evropejskogo-suda-na-russkom-yazyke/kopp-protiv-shvejcarii-postanovlenie-evropejskogo-suda/

Judgment of the European Court of Human Right No 30181/05 “Pruteanu v. Romania”. (2015). Retrieved from: https://pdpecho.com/tag/pruteanu-v-romania/

Newsletter – Professional Secret Lawyer. (2021). European Court of Human Rights: Ukrainian Aspect. Retrieved from: https://www.echr.com.ua/publication/profesijna-tayemnicya-advokata/

Pogoretsky, M.A., & Pogoretsky, M.M. (2016). Guarantees of legal secrecy in the decisions of the European Court of Human Rights and their implementation impact on the criminal procedure legislation of Ukraine and law enforcement practice. *Bulletin of criminal proceedings, 2,* 77-87

Titova, N.M. (2011). Influence of decisions of the European Court of Human Rights on the formation of the status of a lawyer. *Law Practice, 4*. Retrieved from: http://www.dom-prava.com/publications/titova-n.m.–vliyanie-resheniy-evropeyskogo-suda-po-pravam-cheloveka-na-formirovanie

STRENGTHENING CYBERSECURITY IN UKRAINE: LEGAL FRAMEWORKS AND TECHNICAL STRATEGIES FOR ENSURING CYBERSPACE INTEGRITY

Iryna Sopilko
National Aviation University
03058, 1 Lyubomir Huzar Ave., Kyiv, Ukraine
e-mail: sopilko8182@edu-knu.com
https://orcid.org/0000-0001-7670-3157

Abstract

Since 2014, Ukraine has been grappling with increasing cyberattacks linked to ongoing conflicts, notably with the Russian Federation. The study highlights the evolution of Ukraine's cyber defense strategies, including responses to significant incidents such as the 2017 Petya virus attack and the escalation of cyber hostilities following Russia's full-scale invasion in February 2022. The research provides an in-depth analysis of legal measures and technical infrastructure aimed at safeguarding Ukraine's cyberspace. It examines key legal frameworks adopted to enhance cybersecurity, the role of governmental and non-governmental entities, and the technical challenges faced in protecting critical infrastructure from cyber threats. The paper also reviews significant contributions from both Ukrainian and international scholars, offering a comprehensive understanding of cyberspace's multifaceted nature and its implications for national and global security. The paper concludes with strategic recommendations for advancing Ukraine's cybersecurity posture, including the continuous improvement of national security systems, balancing information openness with access restrictions, fostering digital innovation, and enhancing public cyber hygiene. The findings underscore the importance of a cohesive approach to cybersecurity that integrates legal, technical, and societal dimensions to effectively counter cyber threats and uphold national security. By addressing these critical areas, Ukraine aims to establish itself as a resilient participant in the global information and cyberspace community.

Keywords: Cyberspace; cybersecurity; legal frameworks; technical infrastructure; national security.

1. Introduction

Today, the information sphere became a platform for the development of a post-industrial society, it is a catalyst for the formation of an information society in Ukraine. And this sphere has a significant impact on the state of economic, political, defense, and other components of the national security of the Ukrainian state. That is why the formation and development of stable and open information space in the country are what will allow creating and developing an equally stable cybernetic space, where fast and mobile information flows efficiently and freely exist and interact.

As most of the world knows, since 2014, Ukraine has been battling against the aggression of the Russian Federation, defending its territorial integrity and sovereignty in every possible way. The enemy is waging war in all dimensions - on land, water, in the air, and even in a relatively new one - cybernetics. But the first attacks on the information and cybernetic systems of Ukrainian subjects (private enterprises and state institutions) were committed back in 2013, during the Euromaidan.

The Russian-Ukrainian cyber war, as K. Zetter points out, is the first conflict in the cybernetic domain, in which an attack was carried out on the energy system with its subsequent disabling (Inside the Cunning, Unprecedented Hack..., 2016). At the same time, as the head for the development of electronic services of the Ministry of Digital

Transformation M. Banik notes, this cyber war is generally the first in the world (This is the world's first cyber war..., 2022).

In 2017, Ukraine, in the face of its critical infrastructure facilities, was subjected to large-scale cyber-attacks in connection with the rampant Petya virus. Then the state authorities seriously thought about regulating the sphere of cyber security and threw a lot of effort into resolving this matter. Special legal acts were adopted to ensure the protection of Ukraine's national interests in cyberspace and the implementation of an appropriate state policy in the field of cybersecurity. Even more serious consequences were brought by the actions of an aggressively-minded neighboring state, which launched a hybrid war against Ukraine. Now this war waged by Russia is aimed not only at Ukraine, but at the whole world, and, therefore, the entire world community must fight the enemy.

As for Ukraine, with the start of a full-scale invasion of Russia on February 24, 2022, the number of cyber-attacks has increased significantly. Although this year they began against the Ukrainian state on the night of January 13-14, when, as a result of the actions of hackers, some government websites were hacked, in particular, web resources of the Ministry of Education, the Ministry of Foreign Affairs, as well as the Diya service. The attackers used WhisperGate software, which can destroy data.

A month later, on February 15, a huge DDoS attack took place against the websites of the Ministry of Defense, the Ministry of Internal Affairs, and several Ukrainian banks, including Oschadbank, the instigator of which was Russia, which the US presidential administration is sure of (Cyber-attacks on Ukrainian web resources..., 2022). There were several attacks between February 20-23, 2022, and already on February 27, the Ministry of Digital Transformation called on everyone to join the IT army to deter the enemy's attack on our state (This is the world's first cyber war..., 2022). And since then, the number of attacks has been growing - both cybernetic and «physical» - using missiles and weapons prohibited by the Geneva conventions.

In November 2022, the head of the Cybersecurity Department of the Security Service of Ukraine, I. Vityuk, reported that the Russian Federation was accompanying its missile strikes against Ukraine's energy facilities with the strongest cyber attacks to arrange the maximum «blackout» in the defending country. He also noted that the majority of cyber-attacks are not reported to the public, although the enemy carries out an average of more than 10 of them in the cybernetic domain of Ukraine per day. This can have a very serious negative impact since such cyber attacks can be more effective than rocket raids because a «simultaneous attack on all regional energy systems can turn off the power throughout the country.» Also, according to him, about 90% of all cyber-attacks come from Russia, and another part is carried out by the Belarusian special services for the benefit of the Russian Federation. I. Vityuk noted that about 800 cyber attacks were recorded 2 years ago, about 1,400 a year later, and in the current 2022, as of November, this number has increased to more than 3,500 (Russia daily carries out more than 10 cyber..., 2022).

All this confirms the need to maintain the high-quality functioning of cyberspace in the country. In connection with the above, it is important to understand the essence of this term, its features, technical structure, and how this issue is settled at the legal level today. A scientific understanding of the sense of cyberspace will allow for a deeper analysis of cyber incidents in it, manage it and ensure cybersecurity more carefully. This scientific work is dedicated to the issue mentioned. It should be noted that there are still few comprehensive studies on this subject matter since the topic is very new for our state. But there are detailed analyzes and studies on the topic of certain categories and issues of the information and cybernetic spheres.

So, V. M. Furashev explored the essence of cyberspace and information space and gave on their basis a definition of the concepts of "cybersecurity", "information security" and the differences between these spaces and concepts. Thus, he perceives the cybernetic

domain as a form of coexistence of a collection of material and non-material objects and methods aimed at developing, perceiving, processing, exchanging, remembering data (Furashev, 2012). T. S. Smovzhenko, Z. E. Skrynnyk, and others described in detail the features of the existence of an information-global social reality, functioning in real-time, as one that turns humanity into an integral system of worldwide communications. They analyzed and voiced the principles of information policy on the way of the development of the information society in Ukraine, and also studied in detail the information space, of which the cybernetic space is a part (Smovzhenko & Skrynnyk, 2015).

V. L. Girich and V. N. Chuprina studied the role of information and communication technologies in the life of the world community and the nature of the global information space as a bunch of information resources and infrastructures that make up state and interstate computer webs and other cross-border data transmission channels (Girich & Chuprina, 2007). The policy of the modern state, formed under the influence of the global information space, was analyzed by O. Proskurina, she also learned the main directions that state institutions and political organizations seek to comply with while integrating into the global information space. The scientist also focuses in her research on the features of the information strategy of Ukraine in the modern geopolitical space (Proskurina, 2009). I. M. Sopilko defined the concept of information security and gave a qualitative description of this phenomenon in the framework of information warfare.

As for foreign studies of this problem, Weiss M. and Biermann F. described in detail the phenomenon of protecting critical infrastructure from cyberattacks as the main political task of every government and at the same time a public one (Weiss & Biermann, 2021). C. Gao and others qualitatively and comprehensively studied the relationship between cyberspace and real space, assessed the situational state of cyberspace, pointed out the role of network event propagation and traceability analysis, and situational modeling of cyber events to predict risks in cyberspace. They also provided a very clear definition and understanding of cybernetic geography (Guo et al., 2019).

B. P. Medeiros and L. R. Goldoni consider cyberspace as a strategic area for international relations and offer their developments in the form of an analytical tool called «The Fundamental Conceptual Trinity of Cyberspace» in the face of such characteristics of the cybernetic domain as deterritoriality, a plurality of actors and uncertainty (Medeiros & Goldoni, 2020). D.B. Hollis pays special attention to the technical architecture that ensures the functioning of the global Internet and governance in cyberspace and also points to the role of international law in cyberspace (A brief primer on international law and cyberspace, 2021). T. C. Folsom defines cyberspace as an exemplified switched network for the movement of data traffic, further characterized by degrees of admission, navigation, information action, development (and trust), and also suggests improvements in legislation to better respond to new technological challenges (Folsom, 2007).

2. Materials and Methods

This scientific article was written by a group of authors taking into account the provisions of the current Ukrainian legislation and normative regulations of other countries, as well as technical standards adopted in the information technology field. The methodological basis in this study was the generally recognized criteria of scientific objectivity, as well as other general scientific research methods that provide a comprehensive analysis of cyberspace as an objective new, fourth domain in a range of air, water, and land spaces of Ukraine. Thus, the dialectical method of scientific knowledge of the phenomena of reality in their relationship and development became the basis for working on this scientific article. The authors applied the empirical method in the face of describing the essence of the cybernetic space (domain) and the theoretical method in the form of analysis, abstraction, deduction, generalization, explanation, and others. The system method was also used, which helped researchers to establish a connection

between cyberspace and information space, between cybersecurity and information security, and other related categories and concepts.

Special research methods made it possible to study the unique properties characteristic of cybernetic space. Thus, the formal-logical method made it achievable to significantly deepen the conceptual apparatus of the study. The usage of the comparative legal method used by the authors made it possible to clarify the problematic issues of law enforcement in the field of ensuring the normative regulation of the functioning of cyberspace in Ukraine and providing cybersecurity and information security in the country. The method of classification and grouping was useful in the process of determining the subject-object composition of the concept of cybernetic space and related categories. The modeling method has become the basis for the development of recommendations and suggestions for improving legislation in the field of ensuring an appropriate level of cybersecurity and information security, as well as the functioning of cyberspace in Ukraine.

3. Results and Discussion

The term «cyberspace» came to us from science fiction and has become common today among technical workers, security professionals, military, state authorities, and other information subjects. It usually refers to some sort of global information technology environment where people communicate, do business, work, exchange information, and otherwise interact. This concept, for the most part, has become generally accepted in connection with the use of the World Wide Web. And if for some researchers cyberspace is a part of the national critical infrastructure (Weiss & Biermann, 2021), then for others it is a phenomenon determined not so much by technical implementation, but by social interaction (Morningstar & Farmer, 2003). Despite there are much more approaches to understanding and implementing cyberspace, which will be discussed further.

But first, it is worth noting that at the arch of the present and past centuries, both in the social and technical sciences, the term “global information space” arose and took root, which is directly related to the cybernetic space. This is the result of the widespread and intensive involvement and the use of the latest achievements of the information technology revolution in the world in everyday life. Furthermore, in connection with this term, the more narrowly focused term «global cyberspace» is often used.

So, there are several approaches to defining and understanding cyberspace. And we will directly consider them together with related categories and phenomena.

The very name of such a concept was formed from two words - «cybernetics» and «space». For the first time the term «cyberspace» «lit up» in 1984 in the book «Neuromancer» by W. Gibson. The author himself strongly criticized this concept, considering it to be somewhat «meaningless», nevertheless, the term has taken hold and is now used in all corners of the globe to describe objects and functions related to the worldwide global network. Gibson understood cyberspace as a kind of concerted illusion that a huge number of users on earth experience every day (Gibson, 2004).

From a technical point of view, it is worth paying attention to the approach of D. Hollis, who understands the concept under discussion as the technical architecture that assures the functioning of the Internet as a worldwide global network (A brief primer on international law and cyberspace, 2021). The identification of cyberspace with the global Internet network is also observed in Duhem’s legal dictionary, where it is called decentralized, but at the same time interconnected by a set of data and an autonomous telecommunications network (Cyberspace Definition, 2022). Also, the legal dictionary Farlex, when trying to find out the essence of the concept of «cyberspace,» redirects the user to a webpage dedicated to the term «Internet», by which is comprehended the worldwide telecommunications network including computers connected to it related to state, commercial and private entities (Definition of cyberspace, 2022).

As Techopedia points out, any system that has a substantial user base or even a

well-designed interface can be understood as cyberspace. At the same time, its main feature is an interactive and virtual environment for a wide spectrum of parties (What Does Cyberspace Mean, 2022). T. Folsom understands cyberspace as a switched network for moving information traffic, which is characterized by different levels of access, information activity, navigation, and trust in it. The author mentioned does not identify this concept with the Internet, which, in his interpretation, is a special tool that creates and opens the gateway to cyberspace. At the same time, the set of actions that make up cyberspace on the other side of the gateway and the gateway itself together constitute an objective cybernetic space with matters that can arise from its goals (Folsom, 2007).

B.P. Medeiros and L.R. Goldoni understand the concept of cyberspace as a unique area of artificial interaction between people, existing in the combination of technological, technical, and personal layers, without which traditional areas are no longer represented, although it is partially divorced from physical components. The uniqueness of cyberspace as a domain lies in the fact that, unlike the three «physical» ones, it was created by people (Medeiros & Goldoni, 2020).

From the point of view of this scientific research, it is also important to know the definition of cybernetic space given by V.M. Furashev, as a form of coexistence of a special bunch of material and non-material objects, phenomena, methods, strategies the objective of which is interaction with information, that is, the creation, braining, processing of such information and knowledge, their mutual exchange (Furashev, 2012).

Accordingly, we can conclude that there is no single unified and standardized definition of the term «cyberspace». One thing is clear that in all approaches to its understanding, we are necessarily talking about a system of connected computers, digital networks, and other communication and information technologies. Thus, cyberspace is a kind of interactive domain in which data (information, facts, knowledge) is stored, used, processed, operated as an object of exchange and transfer, and the like. Looking ahead, we note that cyberspace also includes the worldwide Internet, which we will discuss further.

The possibility of using the term «cyberspace» in a purely practical plane is evidenced both by its mention in many sources of scientific literature and by its official fixing in the legislation of numerous countries. So, concerning international legal documents, this term is mentioned in paragraph 8 of the Okinawa Charter of the Global Information Society, which states that the international community should direct its forces and resources to coordinated activity to create not only a secure but also crime-free cyberspace. And it is essential to do this for the development of the World Information Society (Virchow & Braun, 2000). Cyberspace is also mentioned in the 2015 United States–China Cybersecurity Agreement, in the draft Cyberspace Electronic Security Act of 1999, S.3480 – Protecting Cyberspace as a National Asset Act of 2010. In the latest regulatory document, the concept in question was represented as an interconnected network information infrastructure, the components of which are telecommunication networks, as well as various systems and embedded processors and controllers used in critical industries (Lieberman, 2010). But this is local regulation.

It is also worth considering the standards for software solutions of the National Institute of Standards and Technology (also NIST) and the American National Standards Institute (also ANSI) (Supplemental Information for the Interagency Report..., 2015). For example, NIST SP 800-30 Rev. 1, NIST SP 800-39, and NIST SP 800-53 Rev. 4 define cyberspace as a global area in the information environment with an interconnected network of information system infrastructures in its structure, that is, computer systems, embedded processors and controllers in critical industries, as well as telecommunications networks and the Internet directly (Guide for Conducting Risk Assessments, 2011; Managing Information Security Risk. Organization, Mission, and Information System View, 2011; Security and Privacy Controls for Federal Information Systems and Organizations, 2021). But NIST SP 800-160 considers this term as an interconnected network of information

technology infrastructures, which includes not only the already mentioned computer systems, embedded processors, and controllers, but also telecommunications networks along with the world wide web (Developing Cyber-Resilient Systems..., 2021).

Summing up the information on the issue of international legal support of cyberspace, we can say that current international law does not contain special norms and rules for regulating relations in it. In this regard, D. Hollis points to some understatement and insufficient regulation regarding the application of the norms of the current international law to cyberspace, although some international actors such as the Group of Twenty, the First Committee of the UN General Assembly on Disarmament and International Security, the EU and others have already revealed their agreement with the applicability of international law in interaction with information and communication technologies. That is, the question rather concerns not the possibility of applying international law, but how this will be done (A brief primer on international law and cyberspace, 2021).

It should be understood that cyberspace today is a unique and not fully explored channel for the creation and dissemination of all kinds of information. It has become the main catalyst for world economic growth, an effective way for international dialogue and cooperation, as well as a completely new area of state sovereignty. But such advantages come with some challenges. Accordingly, the special intangible nature of the studied space significantly complicated not only the definition of such a phenomenon itself but also the substantiation of its legal foundations with their subsequent normative consolidation in official state sources. In this regard, we note that the national legislation of Ukraine concerning cyberspace is represented, first of all, by Law 2163-VIII On the Basic Principles for Ensuring Cybersecurity of Ukraine dated October 05, 2017. This normative act regulates the basis for ensuring the protection of the country's national interests in cyberspace, as well as the vital interests of the main subjects of the relevant relations - an individual and a citizen, society and the state. Its action also extends to the key goals and directions of state policy, the powers, and principles of coordination of the activities of state bodies, institutions, and other entities to ensure cybersecurity. Article 1 (paragraph 11) of Law 2163-VIII defines cyberspace as a virtual domain created as a result of the operation of connected, compatible communication systems and electronic communications using the World Wide Web, as well as, if necessary, other global information transmission networks. Such a space allows everyone to communicate and execute social relations in it (On the main principles of ensuring the cybersecurity of Ukraine, 2022). Cyberspace is thus an ever-evolving environment that changes as technology advances and adapts to new emerging user needs. We are talking about a unique domain, because, unlike the already existing land, water, and air spaces, the cybernetic was created by people. And, due to the ongoing technological research and increasing user experience, it is characterized by constant variability. We also should mention the important «information» component of cyberspace. So, it is distinguished by the absence of geographic reference, as well as the boundaries of physical space. This shows its transboundary character. But also the cybernetic domain does not exist on its own, it is inextricably linked with the information sphere (environment). For this scientific study, it is also important to understand the essence of the last concept. For this, we turn to Section I of Law No. 537-V On the Basic Principles for the Development of the Information Society in Ukraine for 2007-2015 dated January 9, 2007, which says of one of the main priorities of the Ukrainian state - the desire to form an information society that will be open to everyone and focused on the interests and development of individuals. In such a society, each person will not only receive knowledge, but also produce it, transfer it to other people and social groups, freely access such information, and the like. Through this, every Ukrainian will be able to fully realize his potential, which will not only improve the quality of human life but will allow him to develop, as well as the society as a whole (On the Basic principles for the development..., 2007). The organizational

and legal foundations for the development of the information society in Ukraine are considered in paragraph 3 of Section IV of Law No. 537-V, which include resource, institutional, and integration. To achieve the latter, namely, to integrate the Ukrainian state into the global information space, it is important that Ukraine actively participate in the latter, as well as to conduct active international cooperation on reducing the digital and information divide between subjects and implementing a universal general active approach. To achieve these objectives, in addition to expanding the sphere of influence and cooperation with major international actors, the Law under consideration prescribes the integration of Ukrainian science and culture into the global scientific, technological and cultural information space, as well as encouraging partnerships between all sectors of the economy to develop the information society, as required by the UN Millennium Declaration (On the Basic principles for the development..., 2007). Also, the entry of the Ukrainian state into the world information space and information-oriented interstate cooperation is indicated as one of the main directions and priorities of state policy in paragraph 8 of part 1 of article 3 of the Law No. 2657-XII «On Information» dated October 02, 1992 (On information, 2022).

If we recall the previously mentioned global information space, we can consider it as an important element of the social space, even as a kind of special «social information space». As O. Proskurina comments, in the course of implementing the information strategy, an important direction for Ukraine should be precisely the active participation in the work of international actors aimed at the political and legal regulation of the global information space. In this regard, Ukraine should join international treaties on the procedure for the activities of official and non-official bodies in information networks (Proskurina, 2009). Some scientists proceed from the fact that the global information space should be regarded as a set of information resources and infrastructures with interstate and state computer networks in their composition. This set also includes public networks, telecommunications systems, and other cross-border data communication channels. The mentioned resources, in turn, are websites, various texts, databases, and other content. It is these resources in their totality that form a single information space through the information and communication infrastructure (Girich & Chuprina, 2007).

There is another point of view that combines several equivalent approaches to the definition of the information environment (space, field) regarding it as:

- a sphere of subjective activity where data are produced, consumed, altered;
- a similar sphere of subject activity within the framework of public life, which, in addition to the already indicated actions, also includes the preservation of information, its dissemination, and processing;
- the plurality of the knowledge and information themselves, the information infrastructure, and the subjects carrying out information activities;
- a set of systems of information resources, the interaction of information, as well as information infrastructure (Smovzhenko & Skrynnyk, 2015).

In the field of standardization, CNSSI 4009-2015 of the Committee on National Security Systems was adopted (Committee on National Security Systems..., 2022), which defines the information environment as a set of people, organizations, and systems that manage, process, disseminate information, or affect it (Girich & Chuprina, 2007). At the same time, it is important to pay attention to the fact that the information space is not static, it is also clearly structured with the help of information fields and flows. But, as in the case of cyberspace, information has no physical boundaries but has an objective virtual component.

To summarize the above, we can say that the terms «cyberspace» and «information space» are not identical, although they are very similar. So, they differ primarily in their focus. Accordingly, if we mean cybernetic space, then it is an inseparable element of the information space, covering only living beings that perceive, process, recall data, and exchange acquired knowledge. And the information space (information environment)

applies to all sources of information in general, while the subjects of interaction are not required to appropriately perceive data, exchange them, process them, and so on.

At the same time, according to V. M. Furashev, both of the categories under consideration are characterized by such signs as the reality of a generally acting impact, the simultaneous combination of material and non-material, discrete and constant, abstract and real (Furashev, 2012). And yet, cyberspace and information space are different concepts. And, in our opinion, the first should be considered as an element of the system of the second, and not just as an element, but as an important segment in which global flows of both an economic and political character and social relationships are concentrated.

Now let's discuss the important characteristics of cyberspace - deterritoriality, multiple actors, and uncertainty. As sure B.P. Medeiros and L.R. Goldoni, each of these characteristics do not pose a problem, but when they work together, and when operated by users for their purposes, issues can arise. In this regard, we note that, unlike traditional spaces, cybernetic, as mentioned earlier, is not limited by territorial boundaries. It is essentially intangible, yet dependent on mobile devices operating in traditional spaces. It is possible to conclude the simultaneous «presence» of cybernetic space in the other three through the information flows of the electromagnetic spectrum. The deterritorializing nature of the phenomenon under consideration is manifested in its partial non-materiality, but such a space is both an object and a means of power relations. And when the relevant subjects use it and the opportunities provided by it, for their selfish purposes, the territorialization of cyberspace occurs. In this regard, some difficulties arise in the form of challenges to the zonal logic of the territory as a geographical contour in which the state exerts its dominant influence by controlling border flows. The multiplicity of actors in cyberspace is manifested in the fact that it has become a platform for power relations, and the number of actors able to access and interact with this new seat of power is constantly growing. To it undoubtedly contribute wide prevalence and low costs of use (Medeiros & Goldoni, 2020).

This multiplicity resulted in an opportunity for intelligence agencies to track the conversations of the tops of state power, businessmen, and researchers in all corners of the planet, and now terrorists can recruit dissidents from other lands without any problems; hackers can cause significant physical damage to the critical infrastructure of the state and the like. The low cost of use allows cybercriminals to easily and at minimal cost commit sabotage in the cybernetic domain, for example, against a specific airport, as was the case with Ukraine in 2017 due to the Petya virus, than to train people, acquire and operate special equipment to destabilize the work of the airport. Everything is aggravated by the fact that the more complex the state infrastructure, the higher the level of its vulnerability to cyber threats.

Uncertainty as a special quality of cyberspace is manifested in the complexity of the process of identifying and recognizing the ownership of actions by specific actors, and this undermines accountability processes. As a result, there is a lack of indicators of success and anonymity and the very uncertainty of cyberspace. Concerning the issue of accountability, note that such a theing results in the form of speculation in an international context. In this case, there is contextual responsibility, which means that the responsible person is the subject who benefits from the action. As a result, obstacles to the process of attribution and subsequent accountability can lead to an escalation of the war or the prosecution of the innocent (Medeiros & Goldoni, 2020).

Further, we will analyze in more detail the main sources of Ukrainian legislation related to the topic of this study. Earlier, the main Ukrainian legal document that regulates issues related to cyberspace has already been mentioned, this is Law No. 2163-VIII, better known as the Law on Cybersecurity. It has not only defined cyberspace, but also cybersecurity itself. The latter, according to paragraph 5 of Article 1 of this Law, represents the protection of the vital interests of the state of Ukraine, Ukrainian society,

and directly each inhabitant of Ukrainian territory when operating in cyberspace. It is under this condition that not only the sustainable development of the Ukrainian information society, but also the digital communication environment is ensured, and it also provides the identification, precluding, and elimination of possible or real threats to the national security of the Ukrainian state in cybernetic space (On the main principles of ensuring the cybersecurity of Ukraine, 2022). It should be noted that state security in the generalized sense usually implies a condition of protection of the state from internal and external threats. It organically combined military, social, economic, and information security. The latter is of particular interest in the context of this scientific study.

Information security can be defined as a special state of protection of the information environment of the Ukrainian society, in which information subjects represented by the mentioned society, its members, and the state as a whole can freely develop information, and also have complete confidence in the protection of their information rights from internal and external cyber threats (Sopilko, 2021). Paragraph 13 of section 2 of Law No. 537-V gives an official definition of information security as a special state of protection of the interests of Ukraine, every Ukrainian, upon reaching which there will be no harm due to the untimeliness, incompleteness, and inaccuracy of the info provided, as well as no its integrity, confidentiality and availability are violated (On the Basic principles for the development..., 2007). Because of the foregoing, we conclude that cybersecurity is an important element of information security, which in turn is a pivotal segment of national security.

In addition to Law No. 2163-VIII on Cybersecurity, the regulation of the cyber domain in Ukraine is governed by several other legal instruments, including:

- The Ukrainian Constitution of 1996;
- Various laws, such as the «On Information» Law (dated October 2, 1992, No. 2657-XII), the «On the Fundamentals of Domestic and Foreign Policy» Law (dated July 1, 2010, No. 2017), the «On the National Security of Ukraine» Law (dated June 21, 2018, No. 2469-VIII), and the «On Electronic Communications» Law (dated December 16, 2020, No. 1089-IX);
- International treaties ratified by Ukraine, in accordance with Article 9 of the Constitution, and approved by the Verkhovna Rada;
- Decrees issued by the President of Ukraine;
- Regulations established by the Cabinet of Ministers of Ukraine;
- Other relevant regulatory legal acts.

Consequently, the legal support for the functioning of cyberspace in Ukraine is represented by program and regulatory acts containing tasks, objectives, and arrows for solving tasks mentioned to achieve a suitable level of protection of the cyberspace of the state. In addition to the noted legal instruments, a bunch of principles should also be suggested, without which, in our opinion, it will be challenging to achieve these objectives using only the application of the norms of the existing legal framework. These are the principles of:

·respect for human rights and freedoms. After all, as O. Mironets appropriately notes, the prevention of human rights violations is an essential element of the defensive policy of each state (Myronets et al., 2019). According to this fundamental, all activities of the authorities in cybernetic space should be aimed at providing the observance of such rights and interests, and any limitations imposed should not violate them;

·responsibility. Each player in a cybernetic domain must be responsible for preserving stability in it;

·rationality and cognition. Each participant of relations in the space mentioned must assume before acting in such a way that it could threaten the stability of cyberspace;

·appropriate intervention. In case of non-observance of the previous principle, appropriate measures are needed on the part of the bodies ensuring the functioning of the cybernetic space in Ukraine.

Equally noteworthy, we consider the development and undertaking of guides and standards aimed at preventing destabilizing actions, as well as at stimulating the implementation of steps to intensify the stability of cyberspace.

4. Conclusions

With the help of a bibliographic review and legal analysis in this scientific paper, an attempt was made to define cyberspace, conceptualize it, and determine its distinctive technical, social, legal components. This, first of all, will help develop new and improve existing local legislation, as well as promote a holistic and strategically oriented understanding of the role of the cybernetic domain in the life of the international community.

The analysis of various definitions of cyberspace suggests that its understanding is based on the functional essence of the digital domain under consideration. Although cyberspace is, nonetheless, a more multifaceted phenomenon that harmoniously combines resource, technical, intellectual elements, whose essence, features, and content can be the subject of further scientific research with an eye to processing and improving legal regulation on this issue.

It can be concluded that today, to build a full-fledged and comprehensive legal support for the functioning of cyberspace in Ukraine, as well as maintaining the national information security at the proper level in the country, the following is required:

·strengthening and continuous improvement of the national cyber and information security system with the involvement of not only government agencies, but also the active public, representatives of the commercial and academic spheres;

·providing an official interpretation and definition of the legal status and position of information resources, taking into account ownership rights to them, the level of protection and access to information;

·ensuring a balance between the principle of openness of information and the restriction of access to it. Our society is an information one, and, therefore, the protection of data with limited access in the conditions of its existence is impossible without the development and implementation of a flexible legal framework and a balanced state policy in the infosphere;

·all favoring digitalization and the outgrowth of information technology potential, the development of a competitive Ukrainian information product;

·formation and provision of information and psychological safety of information subjects. In connection with the development of information technology, today we are witnessing the dominance of fake data and other misinformation. Consequently, it is important to protect the consciousness of both individuals and the entire society from negative information impact, for which, among other things, it is important to teach Ukrainians cyber and information hygiene;

·providing worthy counteraction to cybercriminals and cyberterrorists. For the work of almost every sector of the economy and other areas of social interaction, information and telecommunication technologies cannot be dispensed with, and therefore they must be reliably protected from the actions of intruders;

·formation and promotion of a positive image of our state on the Internet as one that in every possible way supports and helps to develop the information society.

We are confident that by ensuring the achievement of these objectives, Ukraine will be able to become a worthy member of the global information space, and directly cyberspace based on equality and independence.

References

A brief primer on international law and cyberspace (2021). *Carnegie Endowment for International Peace*. Retrieved from: https://carnegieendowment.org/2021/06/14/brief-primer-on-international-law-and-cyberspace-pub-84763

Committee on National Security Systems (CNSS) Glossary (2022). CNSSI 4009. Retrieved from: https://www.serdp-estcp.org/content/download/47576/453617/file/CNSSI%204009%20Glossary%202015.pdf

Cyber-attacks on Ukrainian web resources are possible on February 22 – CERT-UA (2022). *Ukrainska Pravda*. Retrieved from: https://www.epravda.com.ua/rus/news/2022/02/21/682554/

Cyberspace Definition (2022). *Duhaime Legal Dictionary*. Retrieved from: https://www.duhaime.org/legal-dictionary/term/cyberspace

Definition of cyberspace (2022). *TheFreeDictionary*. Retrieved from: https://legal-dictionary.thefreedictionary.com/cyberspace

Developing Cyber-Resilient Systems: A Systems Security Engineering Approach (2021). *NIST Special Publication 800-160. Revision 1*. Retrieved from: https://doi.org/10.6028/NIST.SP.800-160v2r1

Folsom, T. C. (2007). Defining Cyberspace (Finding Real Virtue in the Place of Virtual Reality). *Tulane Journal of Technology & Intellectual Property, 9*, 75. Retrieved from: https://ssrn.com/abstract=1350999

Furashev, V. M. (2012). Cyberspace and information space, cybersecurity and information security: essence, definition, differences. *Information and Law, 2*(5), 162–175.

Gibson, W. (2004). *Neuromancer: 20th anniversary edition*. New York: Ace Books.

Girich, V. L. & Chuprina, V. N. (2007). *Global information space and the problem of access to world information resources*. Retrieved from: http://marc21.rsl.ru/upload/mba2007/mba2007_05.pdf

Guide for Conducting Risk Assessments (2011). *NIST Special Publication 800-30. Revision 1. Gaithersburg: National Institute of Standards and Technology*. Retrieved from: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-30r1.pdf

Guo, Q., Gao, C., Jiang, D., Wang, Z., Fang, C. & Hao, M. (2019). Theoretical basis and technical methods of cyberspace geography. *Journal of Geographical Sciences, 29(*12), 1949–1964. Retrieved from: https://doi.org/10.1007/s11442-019-1698-7

Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid (2016). *WIRED*. Retrieved from: https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/

Lieberman, J. (2010). S.3480 - Protecting Cyberspace as a National Asset Act of 2010. *111th Congress. Homeland Security and Governmental Affairs*. Retrieved from: https://www.congress.gov/bill/111th-congress/senate-bill/3480/text

Managing Information Security Risk. Organization, Mission, and Information System View (2011). *NIST Special Publication 800-39*. Gaithersburg: National Institute of Standards and Technology. Retrieved from: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-39.pdf

Medeiros, B. P. & Goldoni, L. R. F. (2020). The fundamental conceptual trinity of cyberspace. *Contexto internacional, 42*(1), 31–54. Retrieved from: https://doi.org/10.1590/s0102-8529.2019420100002

Morningstar, C. & Farmer, F. R. (2003). The Lessons of Lucasfilm's Habitat. In: *The New Media Reader* (pp. 664-667). London: The MIT Press. Retrieved from: https://monoskop.org/images/4/4c/Wardrip-Fruin_Noah_Montfort_Nick_eds_The_New_Media_Reader.pdf

Myronets, O.M., Burdin, M., Tsukan, O. & Nesteriak, Y. (2019). Prevention of human rights violation. *Asia Life Sciences, 21(*2), 577–591.

On information (2022). *Law of Ukraine No. 2657-XII*. Retrieved from: https://zakon.rada.gov.ua/laws/show/2657-12#text

On the Basic principles for the development of the information society in Ukraine for 2007-2015 (2007). Law of Ukraine No. 537-V. Retrieved from: https://zakon.rada.gov.ua/laws/show/537-16#text

On the main principles of ensuring the cybersecurity of Ukraine (2022). Law of Ukraine

of No. 2163-VIII. Retrieved from: https://zakon.rada.gov.ua/laws/show/2163-19#text

Proskurina, O. (2009). Information strategy of Ukraine in the modern geopolitical space. *Information Society, 3,* 1–8. Retrieved from: https://ipiend.gov.ua/wp-content/uploads/2018/07/proskurina_informatsina.pdf

Russia daily carries out more than 10 cyber-attacks on strategic objects of Ukraine – SSU (2022). *Ukrainska Pravda*. Retrieved from: https://www.pravda.com.ua/rus/news/2022/11/9/7375609/

Security and Privacy Controls for Federal Information Systems and Organizations (2021). *NIST Special Publication 800-53 Revision. 5*. Retrieved from: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-53r4.pdf

Smovzhenko, T. S. & Skrynnyk, Z. E. (2015). *Ukrainian people in the European world: the dimension of identity*. Kyiv: UBD NBU. 609 p.

Sopilko, I. M. (2021). Information security as an object of regulation in the law of Ukraine. *Journal of International Legal Communication, 1*(1), 11–22. Retrieved from: https://doi.org/10.32612/uw.27201643.2021.1.

Supplemental Information for the Interagency Report on Strategic U. S. Government Engagement in International Standardization to Achieve U. S. (2015). *NISTIR 8074*. Retrieved from: https://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.8074v2.pdf

This is the world's first cyber war. The Ministry of Digital told about the Ukrainian IT army (2022). *Suspilne News*. Retrieved from: https://suspilne.media/222186-ce-persa-u-sviti-kibervijna-u-mincifri-rozpovili-pro-ukrainsku-it-armiu/

Virchow, D. & Braun, J. (2000). Okinawa Charter for the Global Information Society. Geology. Retrieved from: https://www.semanticscholar.org/paper/Okinawa-Charter-on-Global-Information-Society-Virchow-Braun/3eae8bc9b7564b4dd0840d744fad1280038d9131

Weiss, M. & Biermann, F. (2021). Cyberspace and the protection of critical national infrastructure. *Journal of Economic Policy Reform,* 1–18. Retrieved from: https://doi.org/10.1080/17487870.2021.1905530

What Does Cyberspace Mean? (2022) *Techopedia*. Retrieved from: https://www.techopedia.com/definition/2493/cyberspace

Journal

«LEGAL HORIZONS»

Volume 21, No. 2
2024

Editing English-language texts: O. Lapka

Literary editor: A. Shcherbak

Editing bibliographic lists: O. Yatsun

Desktop publishing: K. Tiazhkorob

Signed to the print with the original layout 28.05.2024

Conventional Printed Sheet 9
Circulation 300 copies

Publisher: Sumy State University
40007, 2 Rymskyi-Korsakov Str., Sumy, Ukraine

E-mail: info@legalhorizons.com.ua