CRIMINAL LAW AND CRIMINOLOGY. CRIMINAL AND PENAL LAW

DOI https://doi.org/10.30525/978-9934-26-372-9-41

LEGAL ADAPTATION OF UKRAINE TO EUROPEAN STANDARDS IN THE FIELD OF CYBERSECURITY

Batrachenko T. S.
Ph.D. in Law, Associate Professor of the Department of Law Enforcement and Criminal and Legal Disciplines, University of Customs and Finance Dnipro, Ukraine

Over the past decade, cybercrime has become an important factor threatening cybersecurity and national security in Ukraine, especially in a state of war. In order to ensure effective counteraction to cybercrime and compliance with European standards, Ukraine is actively adapting its legislation to the norms and requirements of the European Union in this area. This initiative is particularly relevant as cybersecurity in a country at war becomes an important component of national defense and a strategic lever in ensuring the security and sovereignty of Ukraine. Therefore, overcoming cyber threats in these conditions requires the improvement of legislation and strategies in this area to ensure effective protection of national interests.

Cybercrime is becoming an urgent issue for many countries, including Ukraine, which is actively fighting this threat to cybersecurity and national security. In the context of European standards and norms, Ukraine is taking measures to adapt its legislation in the field of cybersecurity and combating cybercrime. This study aims to analyze the legislation of Ukraine and the European Union in this area and identify key aspects [1, p. 51].

Ukrainian legislation in this area includes the Law "On Cybersecurity" and the Law "On Information Security". These laws define the basic concepts, requirements, and obligations for cybersecurity in the country. In addition, the Ukrainian government has established the National Cybersecurity Center to coordinate activities in this area. Therefore, the above-mentioned legal acts are key provisions that regulate aspects of cybersecurity and combating cybercrime.

These laws establish clear definitions of the basic concepts in the field of cybersecurity, which helps to unify the understanding of key terms. They necessarily impose requirements on entities that must ensure the cybersecurity of their information and infrastructure, contributing to the growth of cybersecurity levels. In addition, the legislation provides for liability for violations of established norms and obligations, which contributes to the introduction of discipline in the field of cybersecurity. The Laws also establish cybersecurity measures and standards that are applied by entities to ensure information security [2].

The formation of the National Cybersecurity Center demonstrates the importance of coordination and cooperation between government agencies and other stakeholders for the effective implementation of cybersecurity policy in Ukraine.

The EU effectively applies cybersecurity legislation in accordance with the Network and Information Security Directive (NIS Directive) and the General Data Protection Regulation (GDPR), which are important components of EU legislation on cybersecurity and privacy. The Directive sets out requirements for operators of critical infrastructure and providers of digital services to ensure an appropriate level of cybersecurity and to assist in the resolution of incidents in the field of network and information security. The Directive also establishes mechanisms for cooperation and information sharing between EU Member States in the event of cybersecurity threats. The GDPR, on the other hand, regulates the protection of personal data of EU citizens and requires organizations and businesses to ensure an appropriate level of protection of this data. An important aspect in the implementation of the EU's cybersecurity policy is the establishment of high standards of confidentiality and data protection, as well as the existence of appropriate penalties for non-compliance.

An important aspect is the study of the normative acts and practices of EU countries related to legislative regulation, national cybersecurity centers, public-private partnerships, standardization and certification, response to cybersecurity incidents, education and training, as well as international cooperation. This allows to identify best practices and recommendations that can be applied in Ukraine to improve the level of cybersecurity and compliance with international standards.

Therefore, the issue of cloud infrastructure certification (EUCS – European Cybersecurity Certification Scheme for Cloud Services) and its impact on strengthening resilience and cybersecurity, to which Ukraine also joined in September 2023, deserves attention. Thus, thanks to this step, global cloud service providers have committed to providing Ukraine with assistance

and placing state information systems in cloud environments. This made it possible to ensure the resilience of the infrastructure and the continuity of service delivery to citizens and businesses after the full-scale invasion of Russian troops into Ukraine. In addition, this step was the implementation of fruitful cooperation with the European Union Agency for Network and Information Security (ENISA), which brought Ukrainian legislation in this area closer to EU standards, as well as cooperation on the further adaptation of our legislation to the European one [3].

An analysis of the legislation of the European Union and Ukraine in the field of cybersecurity allows us to assert an analogy in the definition of key concepts and the establishment of regulatory requirements for cybersecurity. However, it is important to note that EU legislation is distinguished by a more developed system of cooperation and coordination between its members, which contributes to more effective information sharing and joint actions in the field of cybersecurity. This cooperation helps to ensure a higher level of resilience and responsibility in cyberspace at the level of the European Union, which could be a valuable experience for Ukraine in further improving its legislation and cybersecurity policies.

In addition, cybersecurity is becoming an increasingly important aspect of national and international security, especially in the context of cybercrime and transnational cyber threats. Ukraine is actively working to adapt its legislation to European cybersecurity standards in order to not only ensure its cybersecurity, but also to improve compliance with international norms and support cooperation with international partners, including the EU.

The analysis of the experience of EU countries shows that they are developing more developed systems of cooperation and coordination in the field of cybersecurity, which contributes to more effective response to cyber threats. Cooperation and exchange of experience with European partners can help improve cybersecurity in Ukraine, especially in the context of increasing cyber threats in a state of war.

It is important to emphasize the constant analysis and adaptation of cybersecurity legislation and policies to changes in cyber threats and international standards. Only such a striving for relevance and compliance with international norms can guarantee reliable cybersecurity and resilience of Ukraine's information systems in the context of the modern digital world.

References:

1. Батраченко Т.С. Міжнародне співробітництво у сфері протидії транснаціональній кіберзлочинності. Матеріали Всеукраїнської

науково-практичної конференції «Актуальні проблеми міжнародного права». ХНУ імені В. Н. Каразіна, Харків. 2023. С. 50–53.

2. Стратегія кібербезпеки України (2021–2025 роки) «Безпечний кіберпростір – запорука успішного розвитку країни» URL: https://www.rnbo.gov.ua/files/2021/STRATEGIYA%20KYBERBEZPEKI/proekt%20strategii_kyberbezpeki_Ukr.pdf

3. Державна служба спеціального зв'язку та захисту інформації України URL: https://cip.gov.ua/ua/news/ukrayina-ta-yes-pracyuyut-nad-posilennyam-kiberzakhistu-khmarnikh-servisiv

DOI https://doi.org/10.30525/978-9934-26-372-9-42

THE "LEGALIZATION" OF CANNABIS: SOME RISKS FOR UKRAINE

«ЛЕГАЛІЗАЦІЯ» КАНАБІСУ: ДЕЯКІ РИЗИКИ ДЛЯ УКРАЇНИ

Bakhurynska O. O.
PhD in Law, Associate Professor, Associate Professor at the Department of Criminal Law Politics and Criminal Law, Educational and Scientific Institute of Law, Taras Shevchenko National University of Kyiv Kyiv, Ukraine

Бахуринська О. О.
кандидат юридичних наук, доцент, доцент кафедри кримінально-правової політики та кримінального права, Навчально-науковий інститут права, Київський національний університет імені Тараса Шевченка м. Київ,Україна

Прийняття 13 липня 2023 року за основу проекту Закону № 7457 «Про регулювання обігу рослин роду коноплі (Cannabis) в медичних, промислових цілях, науковій та науково-технічній діяльності для створення умов щодо розширення доступу пацієнтів до необхідного лікування онкологічних захворювань та посттравматичних стресових розладів, отриманих внаслідок війни» [1] дало орієнтири вирішення давно обговорюваної проблеми забезпечення прав пацієнтів на необхідне лікування. У фаховому та громадському середовищі продовжується дискусія щодо незавершеності формування супровідного пакету законопроекту, у якому, зокрема, відсутій надважливий елемент – проект змін до Переліку наркотичних засобів, психотропних речовин і прекурсорів від 6 травня 2000 року; критикується рішення авторів даного законопроекту віддати питання визначення відсотка